تلخیص وتحلیل کتاب

مدیریت و تحلیل ریسک امنیتی[1]

حسین عصاریان نژاد[2]

اشاره:

آنالیز ریسک، تکنیکی است که برای شناسایی و ارزیابی مولفه ها و عواملی که ممکن است موفقیت یک سازمان یا دستیابی به یک هدف را به مخاطره بیاندازند، مورد استفاده قرار می گیرد. نام دیگر این فرآیند، « آنالیز حوادث سازمانی» است. این فرآیند نیازمند انجام یک تجزیه و تحلیل هزینه- منفعت است. فرآیند هزینه- منفعت می بایست در بازنگری ویژگی ها و مزایای یک سرمایه یا کارکرد یا فرآیند دخیل باشد.

بخشی از بازنگری یک موفقیت، تعیین هزینه های آن است. این هزینه ها عبارتند از هزینه های تامین و توسعه؛ یعنی هزینه های عملیاتی و نگهداری و ...، هزینه های مستندسازی، هزینه های آموزش نیروی انسانی، هزینه زیرساخت ها، هزینه به روزآوری، هزینه های جابه جایی وتولید خدمات و محصول و مانند آن. تمامی این هزینه ها مستلزم جنبه های مادی و معنوی است .

اگرچه توجه به تمامی مولفه های هزینه ای برای تصمیم گیری در زمینه اجرای فعالیت سازمانی بسیار مهم است، ولی این هزینه های اجرایی تنها یک متغیر است. هزینه عدم اجرای یک ماموریت نیز متغیر دیگری است که می بایست در فرآیند تجزیه و تحلیل مورد توجه قرار گیرد. چنانچه اجرای ماموریت با تاخیر مواجه شده یا مورد اقبال قرار نگیرد، چه اثراتی بر سازمان خواهد داشت؟ عدم پیشرفت ماموریت چه تاثیراتی بر مزیت های رقابتی سازمان دارد؟ چگونه می تواند توانایی شرکت در دستیابی به اهداف و ماموریت ها را تحت تاثیر قرار دهد؟

در حالت کلی، هر جا که ثروت یا منابعی صرف می شود، می بایست ارزیابی ریسک انجام شود. این امر سبب می شود که اجرا یا عدم اجرای ماموریت با دلایل موجه همراه بوده ونشان می دهد که مدیر

---

[1]-Security Risk Assessment and Management,By Betty E. Biringer Rudolph V. Matalucci Sharon O'Connor Published by John Wiley & Sons, Lnc,۲۰۰۷– ۳۵۸ p.

۲.استادیار وعضو هیأت علمی دانشگاه عالی دفاع ملی

تلاش خود را جهت اتخاذ تصمیم درست انجام داده است. خروجی فرآیند تحلیل ریسک دو بار مورد استفاده قرار می گیرد. بار نخست در زمان اتخاذ تصمیم است. مورد دوم در زمان ارائه نتایج تصمیم به شخص ثالث یا شریک بیرونی است و مدیر ناچار است تا فرآیند تصمیم گیری خود را به وی ارائه دهد. در مجموع باید گفت که اجرای فرآیندهای تحلیل و ارزیابی ریسک، درک و تجسم مناسبی از ماموریت به دست می دهد.

مقدمه نویسنده

نویسنده کتاب مدیریت و تحلیل ریسک امنیتی در ابتدای کتاب به اهمیت مدیریت ریسک اشاره نموده و می‌نویسد:

رقابت در محیط امروزین مستلزم توانمندی فزآینده برای جذب بهینه منابع محدود محیطی اعم از کالا، نیروی انسانی شایسته و منابع بهینه است. مصرف بهینه این منابع، دومین عاملی است که از نقش موثری در کسب مزیت رقابتی برای سازمان ها برخوردار است. در این راستا، با وجود تمام برنامه‌ریزی ها و دقت‌نظرهایی که توسط مدیران و کارشناسان شرکت ها در این زمینه صورت می‌گیرد، اماهنوز برخی عوامل خارج از کنترل نهادها و سازمان ها وجود دارد که با درجات مختلفی از احتمال، امکان دست نیافتن سازمانها به هریک از اهداف عملیاتی را می‌تواند افزایش دهد. در این راستا، احتمال عدم دسترسی به اهداف از پیش تعیین شده، تحت عنوان ریسک مطرح است. بر مبنای اهدافی که تحت تاثیر ریسک قرار می‌گیرد و همچنین از نظر عوامل موثر بر احتمال دستیابی به هدف، ریسک حاکم بر فعالیت سازمان‌ها را به دسته‌های مختلفی تقسیم می‌کنند. از آن جمله می‌توان به ریسک امنیتی، ریسک سرمایه‌ای، ریسک سیستماتیک، و... اشاره کرد. در این کتاب سعی بر این است تا ابتدا، طبقه‌بندی اولیه‌ای از انواع ریسک را مطرح و سپس ابعاد مدیریت ریسک به طور مشروح مورد بررسی قرار گیرند . در مرحله بعد سعی بر آن است تا شاخص های لازم برای ارزیابی و تحلیل ریسک در سطوح راهبردی شناسایی و معرفی شود.

فصل اول: ریسک چیست ؟

دراین فصل نویسنده به مفاهیم وتعاریف ریسک پرداخته و می نویسد:

با مراجعه به منابع مختلف علمی، تعاریف متعددی از ریسک می‌توان یافت. که البته هر کدام از این تعاریف بسته به بُعد یا زاویه دید خود، تعریف متفاوتی از ریسک ارائه کرده‌اند وستون و بریگام در تعریف ریسک می‌نویسند :

ریسک عبارت است از تغییر احتمالی بازده آتی ناشی از شکست و یا تهدید سازمان.

«نیکلز» مفهوم ریسک را از ابعاد مختلف مد نظر قرار داده و آن را از نظر مفهومی به دو دسته تقسیم می‌کند. وی معتقد است واژه ریسک به احتمال ضرر، درجه احتمال ضرر، و میزان احتمال ضرر اشاره دارد. در این راستا ریسک احتمال خطر هم احتمال سود و هم احتمال زیان را دربر می‌گیرد. در حالی که ریسک خالص صرفاً احتمال زیان را در بر می‌گیرد و شامل احتمال سود نمی‌شود، مانند احتمال وقوع آتش.

لذا، با توجه به مجموعه تعاریف فوق، می‌توان ریسک را به صورت زیر تعریف کرد:

«ریسک عبارت است از احتمال تغییر در مزایا و منافع پیش‌بینی شده برای یک تصمیم، یک واقعه و یا یک حالت در آینده»

منظور از احتمال این است که اطمینانی به تغییرات نیست. در صورتی که اطمینان کافی نسبت به تغییرات وجود داشت، تغییرات مطمئن در چارچوب منافع و مزایای پیش‌بینی شده پوشش پیدا می‌کرد، در حالی که عدم امکان پیش‌بینی ناشی از احتمالی بودن تغییرات، آن را به ریسک حاکم بر منافع و مزایا تبدیل کرده است.

تغییر، اشاره به هرگونه کاهش یا افزایش در منافع دارد به این معنا که صرفاً تغییرات نامطلوب نیست که در چارچوب ریسک پوشش پیدا می‌کند. بلکه تغییرات مطلوب نیز در این معنا در چارچوب ریسک قرار دارد.

تصمیم، واقعه یا حالت، اشاره به ارادی و غیر ارادی بودن شرایطی دارد که ریسک بر آن حاکم می‌شود. ممکن است تصمیمی به صورت ارادی گرفته شود، مزایا و منافع آن ارزیابی شود، و بر مزایا و منافع آن ریسک خاصی حاکم باشد. از طرف دیگر ممکن است واقعه یا حالتی در آینده به صورت غیر ارادی پیش‌آید و پیش‌بینی‌های مزایا و منافع آن تحت لوای احتمال تغییر قرار گیرد.

فصل دوم: مفاهیم مدیریت ریسک

نویسنده در آغاز این فصل، ضمن اشاره به مفهوم مدیریت،به مفهوم مدیریت ریسک اشاره می‌کند. از این منظر مدیریت ریسک، فرآیندی سیستماتیک است که با تعیین، تحلیل و اعمال کنترل لازم برای غلبه بر ریسک، کنترل می شود. این امر به‌منظور حداکثر کردن نتایج مثبت و حداقل کردن پیامدهای منفی صورت می‌پذیرد.

ریسک و عدم اطمینان، هر دو برای بیان وجود خطر به‌کار رفته‌اند ولی با یکدیگر متفاوتند. ریسک بیانگر شرایطی از احتمال وجود خطر است که احتمال و آثار ناشی از آن قابل برآورد بوده و در صورت مدیریت به موقع قابل پیشگیری است، در حالی که

شرایط عدم اطمینان به زمانی اطلاق می‌شود که هیچ نوع اطلاعاتی از مقدار و احتمال وقوع ریسک در دسترس نباشد. عدم اطمینان بدترین حالت برای مدیریت و درک ضرورت های شرایط مدیریت ریسک است

از طرف موسسه مدیریت پروژه، مدیریت ریسک به عنوان یکی از نه سطح اصلی «کلیات دانش مدیریت پروژه» معرفی شده‌است. در تعریف این موسسه، مدیریت ریسک پروژه به فازهای‌شناسایی ریسک، اندازه گیری ریسک، ارائه پاسخ (عکس‌العمل در مقابل ریسک) و کنترل ریسک تقسیم شده‌است. در این تعریف، مدیریت ریسک پروژه عبارت است از«کلیه فرایندهای مرتبط با شناسایی، تحلیل و پاسخگویی به هرگونه عدم اطمینان که شامل حداکثرسازی نتایج رخدادهای مطلوب و به حداقل رساندن نتایج وقایع نامطلوب می‌باشد.»

در منابع مختلف، تعاریف دیگری نیز ارائه شده‌است. بنا بر نظر بوهم، مدیریت ریسک فرایندی شامل دو فاز اصلی است؛ فاز تخمین ریسک (شامل شناسایی، تحلیل و اولویت بندی) و فاز کنترل ریسک (شامل مراحل برنامه ریزی مدیریت ریسک، برنامه ریزی نظارت ریسک و اقدامات اصلاحی) می‌باشد. بنا به اعتقاد فیرلی مدیریت ریسک دارای هفت فاز است:

۱) شناسایی فاکتورهای ریسک؛
۲) تخمین احتمال رخداد ریسک و میزان تاثیر آن؛
۳) ارائه راهکارهایی جهت تعدیل ریسک‌های شناسایی شده؛
۴) نظارت بر فاکتورهای ریسک؛
۵) ارائه یک طرح احتمالی؛
۶) مدیریت بحران؛
۷) احیای سازمان بعد از بحران.

موسسه مدیریت پروژه، در راهنمای خود در مورد کلیات دانش مدیریت پروژه (نسخه سال ۲۰۰۰)، برای فرایند مدیریت ریسک پروژه، شش فاز را معرفی کرده‌است:

۱) برنامه ریزی مدیریت ریسک،
۲) شناسایی،
۳) تحلیل کیفی ریسک،
۴) تحلیل کمّی ریسک،

۵) برنامه ریزی پاسخ ریسک
۶) نظارت و کنترل ریسک .

انواع مختلف ریسک

در این کتاب در مورد انواع مختلف ریسک آمده است که شیوه ارتباط ریسک با فرصت به شرایط تلقی ریسک بستگی دارد. بعضی اوقات، یک وضعیت، هم فرصت سودآوری و هم امکان بالقوه زیان را فراهم می سازد، ولی در موارد دیگر، فرصت بازسازی محیطی وجود ندارد، تنها امکان بالقوه زیان و تهدید موجود است. بنابراین ریسک می تواند دارای دو نوع تقسیم فرعی دیگر باشد:

ریسک سوداگرانه؛
ریسک خطرناک.

در ریسک سودا گرانه، شما می توانید یک موفقیت تحقق یافته یا بهبودی در روال شرایط نسبت به وضع موجودتان داشته باشید. و به‌طور همزمان نیز امکان بالقوه ای برای تجربه یک زیان یا بدتر شدن شرایط نسبت به وضع موجود را داشته باشید.

در مقابل، ریسک خطرناک فقط یک امکان بالقوه بروز تهدید و زیان به همراه دارد و هیچ فرصتی برای بهبود روال شرایط فراهم نمی سازد. برای مثال، به‌چگونگی در نظر گرفتن امنیت، به‌عنوان یک ریسک خطرناک توجه شود.

بنابراین،ریسک به‌صورت کاملاً مشخص و روشنی قابل طبقه بندی با عنوان سوداگرانه و خطرناک بر مبنای نوع آن نیست، بلکه بر اساس شرایطی که آن ادراک می شود، قابل دسته بندی است.

تمامی اشکال ریسک، چه آنهایی که به‌عنوان ریسک سوداگرانه طبقه بندی شده باشندو یا به‌عنوان ریسک خطرناک، شامل عناصر مشترکی به شرح ذیل است:

۱ -محتوا ؛ ۲ – فعالیت؛ ۳ – شرایط؛ ۴ – پیامدها.

محتوا یعنی زمینه، وضعیت، یا محیطی که ریسک در آن منظور شده و مشخص کننده فعالیت ها و شرایط مرتبط با آن وضعیت است. به‌عبارت دیگر، محتوا نمایی از تمامی پیامدهای سنجیده شده فراهم می‌سازد. بدون تعیین یک محتوای مناسب، به‌طور قطع نمی‌توان تعیین نمود، کدامین فعالیت ها، شرایط و پیامدها می‌بایست در تجزیه و تحلیل ریسک و فعالیت های مدیریتی درنظرگرفته شوند. بنابراین، محتوا، مبنایی برای تمامی فعالیتهای بعدی مدیریت ریسک فراهم می کند.

بعد از ایجاد یک محتوا، عناصر باقی مانده در ریسک به‌طور مناسبی قابل بررسی هستند. عنصر فعالیت یعنی عمل یا اتفاقی که باعث ریسک می شود. فعالیت، عنصر فعال ریسک است و می بایست با یک یا چندین شرط ویژه برای ظهور ریسک ترکیب شود. تمامی اشکال ریسک با یک فعالیت به‌وجود می آیند؛ بدون فعالیت، امکان ریسک وجود ندارد.

در حالی‌که فعالیت، عنصر فعال ریسک است، شرایط تشکیل دهنده، عنصر منفعل ریسک است. این شرایط تعیین کننده وضعیت جاری یا یک مجموعه از اوضاع و احوال است که می‌تواند به ریسک منجر شود. شرایط، وقتی با یک فعالیت آغازگر خاص ترکیب می شود، می تواند یک مجموعه از پیامدها یا خروجی ها را تولید کند. پیامدها، به‌عنوان آخرین عنصر ریسک، نتایج یا اثرات بالقوه یک فعالیت در ترکیب با یک شرط یا شرایط خاص است.

فصل سوم: مدیریت ریسک و مهندسی ارزش

در این فصل نویسنده به کاربرد مدیریت ریسک در مهندسی ارزش می‌پردازد. از نظر او چون ریسک معرف یک رویداد غیرمنتظره است که در رخداد آن عدم اطمینان وجود دارد. لذا هر چه عدم اطمینان بیشتر باشد، شناخت ریسک مشکل‌تر خواهد شد. در یک طبقه‌بندی کلی، مدیریت ریسک از نظر نویسنده کتاب شامل شش مرحله زیر است: برنامه‌ریزی مدیریت ریسک، شناسایی ریسک، تجزیه‌وتحلیل کیفی ریسک، تجزیه‌وتحلیل کمی ریسک، برنامه‌ریزی واکنش به ریسک و کنترل و پیگیری ریسک.

کاربرد مدیریت ریسک در مهندسی ارزش و مدیریت ریسک دو جزء جدایی‌ناپذیر از یکدیگرند. مدیریت ریسک برای همه شرکت‌ها ارزش می‌آفریند. هدف مهندسی ارزش، انتخاب و اجرای بهترین گزینه‌های عملکردی است که البته همواره نسبت به گزینه‌های انتخابی تا حدی عدم اطمینان وجود دارد. هدف از مدیریت ریسک نیز شناخت و مدیریت همین عدم اطمینان است.

بدیهی است که مدیریت ریسک نمی‌تواند عدم اطمینان موجود را در جهت رسیدن به اهداف به‌طور کامل حذف کند، اما روش‌هایی برای تعیین عناصری که باعث این عدم اطمینان می‌شوند را ارائه می‌کند تا مدیریت بتواند به‌جای غافل‌گیر شدن (Reactive Management)، آنها را به نحو احسن شناسایی و مدیریت (pro-active

Management) کند. با این روش مدیر متوجه ارزش عناصر عملکردی کالا شده و در حد امکان خواهد توانست احتمال، شدت و نوع پدیده‌های ریسکی را شناسایی کند.

برنامه یکپارچه مدیریت ریسک و مهندسی ارزش باعث می‌شود هزینه قطعی موضوعات کیفی که کمی کردن آنها مشکل است نیز محاسبه شده و مساله دقیق‌تر تحلیل شود. تحلیل ریسک، مکانیزمی عالی برای مقایسه دقیق طراحی اولیه و گزینه‌های طراحی شده در فرآیند مهندسی ارزش دارد.

طی سال‌های اخیر یکی از موارد مهم در مدل‌سازی، فاکتورهای انسانی برای قابلیت اطمینان و ارزیابی ریسک است.

مهندسی ارزش نیز به‌عنوان یکی از روش‌های کارآمد بهینه‌سازی طرح‌های بزرگ ، سال‌هاست که مطرح شده است. در مهندسی ارزش صدها جایگزین برای یک مساله ایجاد می‌شود، ولی این که آیا به نتایج مورد نظر خواهد رسید یا نه، سوال دیگری است. بنابراین تحلیل ریسک نیز به‌عنوان یکی از اجزای تفکیک‌ناپذیر مهندسی ارزش محسوب می‌شود. ضمن آن که مهندسی ارزش نیز هیچ مغایرتی با ابزارهای مدیریتی از جمله مدیریت ریسک ندارد.

فصل چهارم: ریسک های امنیتی

در این فصل نویسنده سخن خود را با این کلام آغاز می کند:کسب چه مهارت های امنیتی، سطح ریسک در فعالیت های من را کاهش می دهد.

واقعا این سوال بسیار مهمی در زندگی یک شخص است که چگونه می تواند مهارت های خود را ارتقاء دهد. تقریباً در تمامی کسانی که با کامپیوتر سر و کار دارند، یک نقطه مشترک وجود دارد. در حقیقت این گونه نیست که ما فقط در زمینه حرفه خود باید اطلاعات کسب کنیم و آموخته شویم؛ ما نیاز داریم که از حرفه ها و تخصص های دیگر نیز در زمینه های مربوط به حرفه و شغل خود با خبر باشیم.

همه ما می دانیم که برخی حرفه ها از جمله مدیران سیستم (System Administrator)، و مدیران پایگاه های داده ای (Database Administrator)، تخصص های اصلی و مشترکی با هم دارند که بسیار مورد هجوم و تهدید اطلاعاتی قرار دارند.

داشتن دانش لازم در زمینه پروتکل های امنیتی مورد استفاده از شبکه یکی از تخصص های مورد نیاز برای هر مدیر سیستم است. در ضمن یک مدیر سیستم کسی

است که سرویس دهنده های وب (Web Server) را راه اندازی و پیکربندی می کند.

دانش و تخصص لازم در زمینه خطاهای پروتکلHTTP ، چیزی است که علاوه بر یک مدیر سیستم، یک تحلیلگر امنیتی نیز آن را می داند. همچنین دانستن پروسه های مورد نیاز جهت محکم سازی یک سرویس دهنده وب جهت حفظ امنیت آن، دانش مورد نیاز هر دو آنها است. این موضوع در زمینه پروتکل FTP نیز صادق است.

معماری یک شبکه جزو بخش هایی است که معمولاً در شبکه های بزرگ مورد غفلت قرار می گیرند و باز هم یک مدیر سیستم تنها کسی است که در این زمینه بیشترین نگرانی را دارد. با کمی پیچیدگی، یک شبکه می تواند هم از داخل و هم از بیرون در معرض خطر باشد. داشتن DMZ امروزه در برابر تکنیک های حفاظتی دیگر، بسیار معمول و پیش پا افتاده است. همه این مسایل که درباره معماری و طراحی یک شبکه است، نیاز به دانشی دارد که مدیران سیستم ها و تحلیلگران امنیتی هر دو به اندازه کافی از آن بهره مند باشند.

هر شبکه بزرگ و امروزی دارای ابزارهای مختلف امنیتی است. این ابزارها شامل فایروال، راه حل های آنتی ویروس ها، فیلترکنندگان محتوا و پروکسی سرور ها می باشد که معمولا تمامی آنها توسط مدیران سیستم ها، مدیریت می شود. تنها تفاوت یک مدیر سیستم و یک تحلیلگر امنیتی عمق دانش آنها درباره خروجی های این ابزارها می باشد. برای نمونه یک تحلیلگر سیستم، کلیه ترافیک خروجی یک فایروال را تجزیه و تحلیل می کند و می گوید آیا هشدار های این سیستم معتبر هستند یا خیر. شاید فقط تعداد محدودی از مدیران سیستم هستند که با خواندن جزییات بسته های شبکه راحتند. این کار نیاز به زمان زیادی دارد، در حالی که تنها چیزهایی که مدیران سیستم نیاز دارند راه اندازی سیستم ، پیکربندی و نگهداری از این ابزارهاست، این همان دانشی است که یک تحلیلگر امنیتی نیز آن را دارا می باشد.

یک مدیر سیستم نه تنها در زمینه عملکرد سرویس های ارائه شده در شبکه مهارت دارد، همچنین نگران وضعیت امنیتی آنها نیز است. شما نمی توانید یک سیستم یا سرویس را بدون داشتن تخصص و دانش لازم درباره آن، امن کنید. یک تحلیلگر امنیتی شخصی است که دانش گسترده ای دارد. شما می توانید یکی از تخصص های دیگر همچون "تست نفوذگری (Penetration Testing) "و یا متخصص "امنیت

برنامه های کاربردی (Web Application Security) "را نیز به عنوان حرفه آینده خود انتخاب کنید.

فصل پنجم : سیاست های امنیتی و مدیریت ریسک

در این فصل نویسنده کتاب بر این اعتقاد است که هر سازمانی نیاز به سیاست های امنیتی که مدبرانه تدوین شده باشند دارد. در هر لحظه خطرات مختلفی از بیرون و درون سازمان مثل نفوذگران، رقبا و یا کشورهای خارجی، منافع سازمان را تهدید می کند. هدف سیاست های امنیتی تعریف روال ها، راهنماها و تمریناتی است که امنیت را در محیط سازمان برقرار و مدیریت می نماید. با اجرای دقیق سیاست های امنیتی، سازمان ها می توانند تهدیدات را کاهش دهند.

به تعبیر این کتاب سیاست امنیتی یک سازمان سندی است که برنامه های سازمان برای محافظت سرمایه های فیزیکی و مرتبط با فناوری ارتباطات را بیان می نماید.

هر سیاست امنیتی مشخص کننده اهداف امنیتی و ماموریتی سازمان است ولی در مورد معماری و پیاده سازی این اهداف، بحثی نمی کند. سند سیاست امنیتی سازمان باید قابل فهم، واقع بینانه و غیر متناقض باشد، علاوه بر این از نظر اقتصادی امکان پذیر، از نظر عملی قابل انعطاف و متناسب با اهداف سازمان و نظرات مدیریت آن، سطح حفاظتی قابل قبولی را ارائه نماید.

اغلب ریسک های امنیتی توسط محققان امنیتی شناخته و فاش می شوند .

در حال حاضر چنان به نظر می رسد که به صورت کلی صنعت امنیت خواستار تایید و بر ملا شدن نواقص و ریسک های امنیتی درزمان نیاز به اثربخشی سیستم می باشد. در حالی که این وضعیت های امنیتی در بعضی موارد بعد از هفته ها ، ماه ها و یا حتی سال ها به تولید کنندگان نرم افزار ختم و برای آن راهکار یافت می‌شود.

با گذشت زمان ریسک های امنیتی کم کم تبدیل به متاع با ارزشی برای کسب درآمد برخی از شرکت های امنیتی می‌شوند. اخیرا" شایعاتی پیرامون حفره امنیتی جدید WMF منتشر شدکه پیش از آن که این حفره پرآسیب به اطلاع عموم برسد، به مبلغ ۴۰۰۰ دلار فروخته شد .

در حالی که وجوه پرداختی از طرف شرکت های iDefense و ۳ Comبرای موسسات راهبردی یا تیم های امنیتی بسیار قوی چیز چشم گیری به حساب نمی آید، اما این مبالغ برای محققان امنیتی مستقل چنان قابل توجه است که تمام وقت خود را

وقف این موضوع نمایند. این افراد می توانند با تسلط بر راه‌های کشف و یافتن ضعف های امنیتی و آسیب پذیری ها هزینه زندگی خود را به خوبی از این راه تامین نمایند. این نوع فعالیت می تواند تبدیل به یک تلاش تمام وقت برای این افراد شود.

سر انجام باید به این نکتهٔ اذعان داشت که محققان امنیتی به همه لطف بزرگی می کنند و این چیزی است که آنها به خاطرش سزاوار پاداش هستند. در حالی که پذیرفتن متعهدانه و آشکار سازی آسیب پذیری ها امری بسیار مهم است ،

بی‌گمان، هیچ چیزی به اندازه داشتن احساس امنیت برای انسان اهمیت ندارد. به دیگر سخن، نیاز به امنیت یکی از نیازهای مهم جامعه بشری است. علل و عوامل زیادی در ایجاد امنیت افراد تأثیر دارد. یکی از این عوامل، برخورد افراد از حداقل امکانات زندگی است که می‌تواند در شرایط رویاروئی با ریسک به وی کمک کند .

تصمیم‌گیرندگان، برنامه‌ریزان، سیاستگذاران و کارشناسان بخش‌های راهبردی، باید در فکر باشند تا هنگام رویاروئی با خطر، متناسب با نوع خطرهائی که حوزه‌های راهبردی را تهدید می‌کند، امکانات و لوازم ضروری را پیش‌بینی کنند و در اختیار بهره‌برداران راهبرد قرار دهند تا هنگام پدید آمدن حادثه، امنیت سیستم را تا حدودی فراهم آید .

به‌طور کلی، دسترسی آسان و بدون واسطه مدیران به این‌گونه امکانات، می‌تواند یکی ازعوامل مهم و کارآمد در کاهش پدیده ریسک به‌شمار رود. در این راستا، حمایت آموزشی و خدماتی از نهادهای راهبردی در دولت از اهمیت ویژه‌ای برخوردار است . زیرا این عده به دلیل در معرض فشار و تهدید و ضرورت رویارویی با خطر در شرایط هرمراه با ریسک را ندارند

یکی دیگر از راه‌های به حداقل رساندن ریسک، افزایش سطح سرعت واکنش راهبران نسبت به دامنه و گستره خطر و آشنائی با راه‌های رویاروئی با آن است. در این زمینه، نقش‌آموزش به‌عنوان اهرم مؤثری که می‌تواند شناخت انسان را نسبت به پدیده‌های مختلف افزایش دهد، اهمیت ویژه‌ای دارد .

مدیران راهبردی باید از نعمت "آموزش‌های رویاروئی با ریسک" برخوردار باشند تا بتوانند در هنگام رویاروئی با خطر و برآمدن حادثه، به‌خوبی با شرایط ایجاد شده رویاروئی کنند .

بی‌گمان آموزش، زمانی مؤثر و کارساز خواهد بود که تمام عناصر تصمیم‌ساز محیط نیز از سودمندی‌های آن بهره‌مند شوند. از این‌رو، تدوین یک برنامه آموزشی مناسب و تصمیم‌گیری در مورد طراحی راهبردهای مناسب رویاروئی با ریسک ضرورت پیدا می‌کند .

بنابراین، تصمیم‌گیرندگان بخش های راهبردی همواره باید یک "طرح مدیریت کاهش و تسلط بر ریسک" را برای خود طراحی کنند و آن را به‌کار گیرند .

فصل ششم: استانداردهای ارزیابی ریسک

استاندارد های ارزیابی ریسک گسترده ترین شکل و مجموعه از استاندارد های جدیدی است که در بیست سال اخیر منتشر شده است . این استاندارد ها بسیاری از اجزای ساختاری و اساسی کنترل از قبیل اهمیت، ماهیت شواهد کنترل، برنامه ریزی کنترل، درک کنترل داخلی و ارزیابی ریسک را بازنویسی می کنند. به کارگیری این استاندارد ها به دلیل ماهیت گسترده ی آنها (در ذات خویش) یک فرایند مدیریت تغییر محسوب می شود. عامل ابتذال مدیریت تغییر آن است که رهبران تغییر،گرایش به برقراری ارتباط کم (بیش از حد اندک) با افرادی که تحت تأثیر واقع می شوند دارند .

دو گروهی که بیشترین تأثیر را به واسطه ی استاندارد های جدید معطوف خود می سازند، کارکنان بخش کنترل و نظارت کیفیت هستند. رهبران به کارگیری نیاز به ارتباط فوری و همیشگی با این دو گروه برای هرچه بهتر آماده کردن آنان برای تغییراتی که توسط استاندارد های جدید لازم دانسته شده، دارند. این ارتباط یک رویداد واحد نیست بلکه بیشتر مجموعه ای از رویداد های همیشگی در سازمان است. شما برای به کارگیری یکنواخت استاندارد های ارزیابی ریسک نیاز به راهنمایی کارکنان خود از راه فرایند ارتباطات معین دارید که برای هر اقدامی به وسعت و جامعیت استاندارد های ارزیابی ریسک، جابه جا کردن کارکنان از راه هر یک از این مراحل وقت زیادی را به خود اختصاص خواهد داد از این رو باید این فرایند را از هم اکنون آغاز کنید .

انتقال استاندارد های ارزیابی ریسک یک رویداد واحد نیست بلکه بیشتر مجموعه-ای از رویداد های همیشگی زیر است

۱- آگاهی: باید کارکنان را از استانداردهای جدید با خبر ساخته و(به روش متداولی) با قابلیت و مفهومی که به کارگیری آن استاندارد ها برای آنان دارد آشنا سازید

۲- تشویق و ترغیب: به محض آن که مخاطبانتان از استاندارد های جدید مطلع شدند، می توانید عقاید آنان را در مورد این استاندارد ها تحت تأثیر قرار دهید.

۳- دعوت به عمل: هدف نهایی ارتباط شما این است که اعتقاد و رفتار خاصی را در کارمندان و مشتریان خود به کار بیندازید. ممکن است از مشتریان خود بخواهید که کنترل داخلیشان را تقویت کرده و یا رویکرد ها و سیاست های کنترلی خود را به ثبت برسانند.

۴- عمل: سرانجام کارکنان شما قادر به اجرای اقداماتی خواهند بود که از آنان در خواست کرده اید، خواه آن اقدام مشتریان را مجبور به ثبت کنترل داخلی خود کند یا این که کارکنان شما بررسی سیستم را در تمام عملیات های خود به اجرا بگذارند.

فصل هفتم: استاندار های امنیتی

این فصل اختصاص به ضرورت رعایت استانداردها و روال های امنیتی به منظور مدیریت ریسک در محیط اطلاعاتی سازمان است. از نگاه نویسنده سیاست های امنیتی دربردارنده کلیه انتظارات، برنامه ها و اهداف عملیاتی مدیریت سازمان می باشد. برای عملیاتی و قابل اجرا بودن سیاست امنیتی، باید با استفاده از استانداردها، راهنماها و رویه های شناخته شده تعریف شود که اطمینان از سازگاری کلیه عملیات اجرایی با سیاست‌های امنیتی حاصل گردد. از نظر نویسنده استانداردها، راهنما ها و روال ها تفسیر خاصی از سیاست را ارائه می کنند و کاربران، مشتریان و مدیران سازمان را برای پیاده سازی سیاست آماده می نمایند. از این منظر ساختار سیاست امنیتی مرکب از اجزاء زیر می باشد:

عبارتی در رابطه با موضوع سیاست
چگونگی اجرای سیاست در محیط سازمان
نقش و مسؤولیت افراد مختلف تاثیر گذار در سیاست
سیاست به چه میزان انعطاف پذیر است؟
اعمال، فعالیت ها و فرایندهای مجاز و غیر مجاز
موارد سخت گیری و عدم انعطاف سیاست

فصل هشتم: کنترل ریسک های امنیتی

در این فصل نویسنده ضمن اشاره به فصول قبلی در کنترل سطح در ریسک‌های امنیتی به مراحل ایجاد سیستم مدیریت امنیت اطلاعات در محیط فعالیت پرداخته و

ابتداء با ایجاد و تعریف سیاست ها آغاز نموده و می‌نویسد در این مرحله ایجاد سیاست های کلی سازمان مدنظر قراردارد. روالها از درون فعالیت سازمان استخراج شده و در قالب سند و سیاست امنیتی به مدیران ابلاغ می شود. مدیران ارشد نقش کلیدی در گردآوری این سند خواهند داشت. هر چند یک سازمان ممکن است دارای چندین زیرمجموعه و شاخه های کاری باشد لذا شروع پیاده سازی سیستم امنیت اطلاعات کاری بس دشوار است. برای جلوگیری از پیچیدگی پیاده سازی، ابتدا بایدتعریف محدوده و Scope صورت پذیرد. Scope می تواند ساختمان مرکزی یک سازمان یا بخش اداری و یا حتی بخش کنترل شبکه سازمان باشد.

به دنبال آن برای این که بتوان کنترل های مناسب را برای قسمت های مختلف سازمان اعمال کرد ابتدا نیاز به تعیین دارایی ها می باشد. در واقع ابتدا باید تعیین کرد چه داریم و سپس اقدام به ایمن سازی آن نماییم. در این مرحله لیست کلیه تجهیزات و دارایی های سازمان تهیه شده و باتوجه به درجه اهمیت آن طبقه بندی خواهند شد. با داشتن لیست دارایی ها و اهمیت آن ها برای سازمان ، نسبت به پیش بینی خطرات اقدام کنید. پس از تعیین کلیه خطرات برای هر دارایی اقدام به تشخیص نقاط ضعف امنیتی و دلایل به وجود آمدن تهدیدها نمایید و سپس با داشتن اطلاعات نقاط ضعف را برطرف سازید و خطرات و تهدیدها و نقاط ضعف را مستند نمایید.

سپس با انتخاب استانداردهای کنترل مناسب می‌توان به۱۰ گروه کنترلی رسید که هرگروه شامل چندین کنترل زیرمجموعه است. بنابراین در کل ۱۲۷ کنترل برای داشتن سیستم مدیریت امنیت اطلاعات مدنظر قراردارد. با انجام مراحل بالا شرکت یا سازمان شما پتانسیل پیاده سازی کنترل های مذکور را خواهد داشت.

این ده گروه کنترلی عبارتند از:

۱. سیاست های امنیتی
۲. امنیت سازمان
۳. کنترل و طبقه بندی سرمایه و دارایی ها
۴. امنیت کارکنان
۵. امنیت فیزیکی و زیرساختی سازمان
۶. مدیریت ارتباط ها
۷. کنترل دسترسی ها

۸. روش ها و تکنیک های نگهداری و بهبود اطلاعات
۹. مدیریت تداوم کار سازمان
۱۰. سازگاری با موارد قانونی

شناخت دقیق مزیت ها، تعیین تهدیدها ، نقاط ضعف امنیتی و در نهایت ایجاد مکانیز کنترلی، سیستم را در به دست آوردن جدولی موسوم به SOA یا Statement Of Applicability یاری می رساند. این جدول لیستی نهایی از کلیه کنترل های سطح ریسک برای پیاده سازی ارائه می دهد.

فصل نهم: راهکارهای به حداقل رساندن ریسک

نویسنده کتاب معتقد است مراحل اصلی پیاده‌سازی مدیریت ریسک بسیاری از فعالیت هایی که سازمان ها که فرض می‌کنند تحت کنترل دارند، با ریسک به عنوان رخدادی شناخته‌نشده روبرو کرده که سازمان ها کوشش می‌کنند آن را کنترل کنند. اکثر عملکردها چنین رخدادهایی را به خوبی از سر رد می‌کنند ولی با یک تلاش جامع مدیریت ریسک ، رویدادهای ریسک قبل از وقوع شناسایی و کنترل می‌گردند و یا برنامه‌ای تهیه می‌شود که در زمان وقوع این رویدادها با آنها مقابله کند.

با درنظر گرفتن این مفاهیم پایه‌ای، امکان مقابله با ریسک به وجود می‌آید . لذا ابتدا باید نسبت به شناسایی ریسک‌های محتمل پروژه اقدام کرد.این کار با دسته‌بندی ساختار کارها و با پرسش چند سوال از خود و یا اعضای گروه پروژه، امکان‌پذیر است. مثلا : درموقع نیاز به منبعی یا منابعی که در دسترس نیستند چه اتفاقی خواهد افتاد ؟ اگر کنترلی در مورد مولفه‌ای که بر پروژه اثرگذار است نداشته باشیم چه اتفاقی می‌افتد ؟ بدترین سناریو چیست ؟ چه چیزی باعث آن می‌گردد ؟ چه قدر وقوع این اتفاق محتمل است ؟ عواقب آن چیست ؟

امروز براساس این تعریف احتمال وقوع هر ریسک قابل محاسبه‌است . اما مشکل اصلی در تالیف کتاب های مربوط به ریسک آن است که همواره داده‌های تجربی به اندازه کافی در دسترس نیستند تا این کار به دقت انجام گیرد . در این روش معمولا افراد باتجربه‌ای مبادرت به این کار می‌کنند که تجارب جامعی از انواع رویدادها در سازمان های مختلف کسب کرده‌اند .

ما در دنیای مخاطرات ریسک زندگی می‌کنیم . باید ریسک‌ها را تحلیل کنیم ؛ اگر با آنها برخورد داریم باید آنها را شناسایی و در مجموع تمام ریسک‌ها و عواید آنها را باید

ارزیابی کنیم . منافع حاصل از مدیریت ریسک ممکن است تا غلبه پروژه بر آن ملموس نباشد اما به خاطر داشته باشید که کسی که از برنامه‌ریزی اجتناب کند به طور حتم برنامه شکست عملکرد خود را طرح‌ریزی نموده‌است!

فصل دهم: تحلیل ریسک

از منظر نویسنده اولین فاز از فرآیند مدیریت ریسک با عنوان تحلیل مخاطرات (Risk Analysis) شناخته می شود که عبارت است از فرآیندی سیستماتیک که در آن تهدیدهای فرآروی دارایی های اطلاعاتی (Threats to Information Assets) تعیین شده و تاثیر هر یک (Threat Impact) بر کسب و کار سازمان محاسبه می شود. ارائه impact ها به خصوص به شکل عددی می تواند به تصمیم گیری مدیران برای اولویت بندی ریسک ها کمک کند. تحلیل ریسک برای پاسخ به سوالات زیر انجام می شود:

اگر یک ریسک واقعا اتفاق بیافتد، چقدر زیانبار خواهد بود؟

رخداد یک ریسک معمولا (احتمالاً) هر چند وقت یکبار خواهد بود؟

آیا کنترل کردن ریسک مربوط مقرون به صرفه است؟

نکته ای که در پاسخ به سوال سوم باید توجه داشت این است که بر اساس معیارهایی، می توان برخی از ریسک ها را کنترل نموده و کاهش داد (Risk Mitigation) ، برخی را پذیرفت (Risk Acceptance) و یا برخی را به بخش یا سازمان دیگری ارجاع داد (Risk Transferring) .

یک ارائه مناسب در این موضوع ...

قدرت بالا در شبیه سازی ریسک

نرم افزار Pertmaster Project Risk, ابزار پیشرفته پیچیده ترین ریسک های پروژه را در اختیار دارد که انجام شبیه سازی های زیر را برای کاربران میسر می سازد :

مصرف منابع احتمالی

Cash Flow احتمالی

پنجره ریسک

فعالیت های احتمالی

ساختار شکست احتمالی

ارتباط زمان و هزینه

انجام محاسبات و اتخاذ تصمیمات
نمودار شبکه پروژه و ارتباطات تک تک فعالیت ها
نمایش مدت، شروع، پایان و مصرف منابع
کپی مستقیم نمودارها به برنامه Word و PowerPoint و غیره
نمایش برنامه جاری و برنامه مبنا (Baseline)
ایجاد و نمایش نمودار ریسک
محاسبات بحرانیت، حساسیت و قطعیت
مرتب سازی و فیلتر فعالیت ها بر اساس بحرانیت حساسیت و قطعیت
نمایش اطلاعات فعالیت در جدول و نمودار میله ای فعالیت
محاسبه خودکارکمترین، بیشترین،نما، میانه، انحراف معیار برای زمان، هزینه و منابع

امکان انتقال (Export) اطلاعات تحلیل ریسک به برنامه های صفحه گسترده برای محاسبه یا رسم نمودار های دلخواه تحلیل ریسک Monte-carloعلیرغم نرم افزارهای دیگر که محاسبات آنها صرفاً به روش مسیر بحرانی بودن و تنها یک برآورد قطعی برای زمان و هزینه فعالیت ها ارائه می دهند. پرتمستر با استفاده از شبیه سازی مونت کارلو ، زمان و هزینه فعالیت ها را برای حالت های مختلف پروژه محاسبه می کند.

نمای کاربر پسند و قدرت محاسبه (Schedule) پرتمستر سرعت و سهولت کار بسیار خوبی را در اختیار کاربران قرار می دهد که قابل مقایسه با سیستم های دیگر مدیریت ریسک نمی باشد.

در پرتمستر امکان تخصیص احتمال به آیتم های زیر وجود دارد :
مدت فعالیت، هزینه فعالیت، تخصیص منابع، هزینه منابع، وقایع احتمالی

فصل دوازدهم: ریسک راهبردی و عملیاتی

از منظر نویسنده، ریسک استراتژیک، ریسکی است که یک سازمان برای تحقق اهداف تجاری اش می پذیرد. در مضمون این تعریف امکان بالقوه سودآوری و زیاندهی هر دو وجود دارد، که ریسک استراتژیک را طبیعتاً سوداگرانه می سازد. توجه کنید که چگونه چهار عنصر ریسک برای ریسک استراتژیک به‌کار برده می شود. برای مثال، شرایطی را فرض کنید که مدیریت ارشد در یک سازمان راهبردی در حال بررسی ورود

به یک حوزه جدید، است. از آنجایی که این امر به‌واسطه فرایند تصمیم گیری به اجرا گذاشته می شود، مدیر راهبردی می بایست فرصت ها و تهدیدهای بالقوه موجود درآن حوزه را بررسی کند.

تمامی فعالیت ها، شرایط و پیامدها می‌بایست در داخل این محتوای خاص در نظر گرفته شوند. فعالیت ها در این مثال طیفی از انتخابهای استراتژیک سنجیده شده است. مدیریت تعدادی از انتخابهای قابل پیگیری، شامل چهار مورد زیر را پیش روی دارد

۱ - تصمیم گرفتن برای ورود فوری به حوزه جدید؛

۲ - انجام اقدام احتیاطی از طریق ارائه خدمات آزمایشی اندک؛

۳ - در حال حاضر توقف عمل و محفوظ نگهداشتن حقوق راهبردی خود در اقدامات آتی؛

۴ - تصمیم گرفتن برای عدم ورود به حوزه مورد هدف.

شرایط در این مثال، شامل روندهای جاری و عدم اطمینان نسبت به انتظار نتایج راهبردی و آنچه که رقبا ممکن است انجام بدهند، و شایستگی های اصلی سازمان در حال حاضر است. ترکیب هر فعالیت استراتژیک با روندهای جاری و عدم اطمینان، یک طیفی از پیامدها، یا مجموعه ای از فرصت‌ها و تهدیدات بالقوه برای سازمان تولید می کند. مدیریت درجه نسبی هر فرصت و ریسک ناشی از هر فعالیت استراتژیک را مورد بررسی قرار می دهد. آنها بهترین انتخاب را بر مبنای میزان تحمل ریسک درمقابل میزان تمایل برای به‌دست آوردن مزایایی از فرصت های آن، انجام می دهند .

بنابراین، چهار عنصر اصلی ریسک یک ابزار مفید برای تجزیه و درک یک ریسک تجاری استراتژیک فراهم می‌سازد. این عناصر همچنین در زمان بررسی یک ریسک خطرناک، مثل ریسک عملیاتی، مفید واقع می شوند .

نقد شکلی کتاب

امروزه در موضوع مدیریت و تحلیل ریسک، کتاب و سمینارهای متعددی مطرح و درج شده است و فرآیندها و مراحل مختلفی را ذکر کرده‌اند که بر خلاف نویسنده در این کتاب، نگارنده اصرار دارد که در ابتدا ریسک را از منظر خود مطرح و سپس نقد شکلی کتاب را آغاز کند، به نظر می رسد برای نقد این کتاب در مرحله نخست باید فرایند مدیریت ریسک را شامل نه فاز می‌داند که عبارتند از:

۱) شناسایی جنبه‌های کلیدی فعالیت سازمان؛

۲)تمرکز بر یک رویکرد استراتژیک در مدیریت ریسک؛
۳) شناسایی زمان بروز ریسک ها؛
۴) تخمین ریسک ها و بررسی روابط میان آنها؛
۵) تخصیص مالکیت ریسک ها و ارائه پاسخ مناسب؛
۶) تخمین میزان عدم اطمینان؛
۷) تخمین اهمیت رابطه میان ریسک های مختلف؛
۸) طراحی پاسخ ها و نظارت بر وضعیت ریسک
۹) کنترل مراحل اجرا.

در تکمیل این فرآیندها مدیریت ریسک را به صورت فرایند مقابله با ریسک نیز می‌توان در قالب مراحل چهارگانه زیر تعریف کرد.

۱) برنامه ریزی ریسک،
۲) ارزیابی (شناسایی و تحلیل) ریسک،
۳) توسعه روش های مقابله با ریسک
۴) نظارت بر وضعیت ریسک ها.

در مطالعات نظری صورت گرفته از سوی نویسنده، طبقه‌بندی های مختلفی از ریسک ارائه شده است. اما به ریسک حاکم بر پروژه‌های اقتصادی بیش از دیگر حوزه‌ها توجه شده است. در این طبقه‌بندی، تجزیه و تحلیل ارائه شده، تنها به تصمیم‌گیرندگان و مشاوران اقتصادی کمک می‌کند تا فاکتورهای موثر بر پذیرش یا عدم پذیرش گزینه‌های تصمیم‌گیری را رتبه‌بندی کنند. نویسنده در این کتاب فاکتورهای موثر بر طبقه‌بندی را تحت عنوان فاکتورهای ریسک ، مورد اشاره قرار داده است و با تکنیک رتبه‌بندی ریسک در مدل خود به منظور کمک به تصمیم‌گیرنده سبب تولید یک دید تک بعدی می شود، در حالی که می‌توانست با یک نگاه جامع ابعاد فنی، اقتصادی و اجتماعی سیاسی ریسک حاکم بر فعالیت یک سازمان را ارزیابی کند.

نقد روشی کتاب

اساسی ترین نکته‌ای که در این کتاب نویسنده می بایست در روشمند نمودن داده‌ها و حوزه‌های مورد توجه،بر آن تاکید می‌نمود،دقت در تبیین فرآیندهای مدیریت ریسک و تعریف آن است. در واقع مدیریت ریسک فرایند سنجش یا ارزیابی ریسک و سپس طرح استراتژی‌هایی برای اداره ریسک است. در مجموع، باید استراتژی‌های به‌کار

رفته شامل: انتقال ریسک به بخش های دیگر، اجتناب از ریسک، کاهش اثرات منفی ریسک و پذیرش قسمتی یا تمامی پیامدهای یک ریسک خاص هستند. که در روش تحقیق این کتاب کمتر به آن توجه شده است. باید به این نکته اذعان داشت که مدیریت ریسک سنتی، تمرکزش روی ریسک‌های جلوگیری کننده از علل قانونی و فیزیکی بود (مثل حوادث و بحران هاست). مدیریت مخاطرات و بحران ها، از سوی دیگر، تمرکزش روی ریسک‌هایی بود که می تواند استفاده از ابزار قدرت را اداره کند. مدیریت ریسک ناملموس، تمرکزش روی ریسک‌های مربوط به سرمایه انسانی، مثل ریسک دانش، ریسک روابط و ریسک فرایندهای عملیاتی است. بدون توجه به نوع مدیریت ریسک، تمامی سازمانهای بزرگ دارای تیم‌های مدیریت ریسک هستند و انجمن‌ها و گروه‌های کوچک به‌صورت غیر رسمی- در صورت عدم وجود نوع رسمی آن- مدیریت ریسک را مورد استفاده قرار می دهند .

نویسنده کتاب در نگارشهای خود به این نکته اساسی بی تفاوت بوده است که در مدیریت ریسک مطلوب، یک فرایند اولویت بندی منظور گردیده که بدان طریق ریسک‌هایی با بیشترین زیاندهی و بالاترین احتمال وقوع در ابتدا و ریسک هایی با احتمال وقوع کمتر و زیاندهی پایین تر در ادامه مورد رسیدگی قرار می‌گیرند. در عمل، این فرایند ممکن است خیلی مشکل باشد و همچنین در اغلب اوقات ایجاد توازن میان ریسک‌هایی که احتمال وقوع شان بالا و زیاندهی شان پایین و ریسک‌هایی که احتمال وقوع شان پایین و زیاندهی شان بالاست، ممکن است به‌طور مناسبی مورد رسیدگی قرار نگیرند. درنتیجه می توان ریسک‌های موجود در سازمان را از این دو بعُد نیزطبقه بندی کرد

در دنیای پرتحول امروز، مدیریت ریسک از اهمیت روزافزونی برخوردار شده است که از جمله نکاتی که در این کتاب از آن غفلت صریحی شده است مدیریت ریسک‌های پنهانی است.

ریسک پنهانی، یک نوع جدید از ریسک است یعنی که احتمال وقوع آن ۱۰۰ درصد است، ولی در سازمان ها به‌خاطر فقدان توانایی تشخیص، نادیده گرفته می شود. برای مثال ریسک دانش، زمانی رخ می دهد که دانش با ضعف و نقص به‌کار برده شود.

ریسک روابط هم که در این کتاب ذکر نشده است، زمانی رخ می دهد که همکاری بی‌اثر و نتیجه ای اتفاق افتد. ریسک فرایند عملیاتی، که در ص۴۹ به صورت کمرنگی

ذکر شده است زمانی رخ می دهد که عملیات بی‌ثمری اتفاق افتد. این ریسک ها به‌صورت مستقیم بهره وری عملکردی کارکنان را کاهش داده، و باعث نزول مقرون به صرفه بودن خدمات، محصول، توانمندیمنابع، ارزش و کیفیت فرآیند تولید می‌شود. در واقع مدیریت ریسک پنهان باعث می‌شود در مدیریت ریسک به‌واسطه شناسایی و کاهش ریسک‌هایی که عامل نزول بهره وری می باشند، ارزش های آنی و مستقیمی خلق شود .

در کتاب و در موضوع روش‌شناسی خود باید به این اهمیت دست می‌یافت که می توان مدیریت ریسک را یک وظیفه ای شامل فرایندها، روش ها، و ابزاری برای اداره ریسک در فعالیت های سازمانی دانست. که یک محیط منضبط را برای تصمیم گیری های پیشتازانه و غیر منفعل در موارد زیر فراهم می آورد:

ارزیابی پیوسته در مورد آنچه که ایجاد اشکال می کند (ریسک)

شناسایی ریسک‌های مهم در راستای برخورد با آنها

اجرای استراتژی‌های مناسب به‌منظور اداره نمودن آن ریسک‌ها

فصل سوم کتاب در مورد پارادایم مدیریت ریسک بحث کرده و نویسنده در مقدمه این فصل بر این باور است که پارادایم یا الگوی مدیریت ریسک، مجموعه ای از وظایف به‌صورت یک سری فعالیت های پیوسته در سرتاسر چرخه عمر یک مأموریت می باشند و عبارتنداز:

شناسایی ریسک ها؛ تحلیل؛ برنامه ریزی؛ پیگیری؛ کنترل .

از نظر نویسنده وظایف پیوسته در مدیریت ریسک عبارتند از: هر ریسکی که به طور طبیعی این وظایف را به‌طور متوالی طی می‌کند، ولی فعالیت ها به‌صورت پیوسته، همزمان(مثلاً ریسک‌هایی پیگیری می شوند در حالی‌که به موازاتش ریسک‌های جدیدی شناسایی و تحلیل می شوند)و تکراری (مثلاً برنامه کاهنده ای برای یک ریسک ممکن است برای ریسک دیگری مفید باشد) در سرتا سر چرخه حیات یک مأموریت اتفاق می افتند.این وظایف پیوسته عبارتند از:

شناسایی: جستجو و مکان یابی ریسک‌ها، قبل از مشکل ساز شدن آنها.

تحلیل: تبدیل داده های ریسک به اطلاعات تصمیم گیری. ارزیابی میزان اثر، احتمال وقوع ومحدوده زمانی ریسک‌ها و طبقه بندی و اولویت بندی ریسک‌ها .

برنامه ریزی: ترجمه اطلاعات ریسک به تصمیم ها و فعالیت ها (هم حال و هم آینده) و به‌کارگیری آن فعالیت ها.

پیگیری: بررسی شاخص های ریسک و فعالیت های کاهنده.

کنترل: اصلاح انحرافات نسبت به برنامه های کاهنده ریسک.

ارتباطات: اطلاعات و بازخورهای بیرونی و درونی از فعالیت های ریسک، ریسک‌های موجود و ریسک‌های پدید آمده فراهم می‌سازد.

در موضوع استانداردها و سیاست های امنیتی که نویسنده از آن سخن به میان آورده است، باید به پیشرفت علوم کامپیوتری و همچنین به وجود آمدن ابزارهای جدید Hackو Crack و همچنین وجود صدها مشکل ناخواسته در طراحی نرم افزارهای مختلف و روال های امنیتی سازمان ها و خطر حمله و دسترسی افراد غیرمجاز که همیشه وجود دارد، اشاره می‌شد. امروزه حتی قوی ترین سایت های موجود در دنیا در معرض خطر افراد غیرمجاز و سودجو قرار دارند. و نمی توان به امنیت ۱۰۰٪ اطمینان داشت، البته باید به نکات امنیتی و ایجاد سیاست های مختلف امنیتی توجه کرد.

برخی استانداردهای مقابله با ریسک، قالبی مطمئن برای داشتن یک سیستم مورد اطمینان امنیتی می باشد. که می‌تواند سبب شود تا فوائد زیر حادث گردد:

اطمینان از تداوم تجارت و کاهش صدمات توسط ایمن ساختن اطلاعات و کاهش تهدیدها

اطمینان از سازگاری با استاندارد امنیت اطلاعات و محافظت از داده ها

قابل اطمینان کردن تصمیم گیری ها و محک زدن سیستم مدیریت امنیت اطلاعات

ایجاد اطمینان نزد کاربران و مصرف کنندگان اطلاعات

امکان حیات و رقابت بهتر با سایر محیط‌های جانبی

ایجاد مدیریت فعال و پویا در پیاده سازی امنیت داده ها و اطلاعات

نویسنده کتاب در موضوع سیاست امنیتی مباحث جالبی را مطرح نموده است اما از این نکته اساسی غافل مانده است که بهترین روش برای دستیابی به امنیت اطلاعات، فرموله نمودن سیاست امنیتی است. مشخص نمودن سرمایه های اصلی که باید امن شوند و تعیین سطح دسترسی افراد (به عبارت دیگر این که چه افرادی به چه سرمایه هایی دسترسی دارند) در اولین گام باید انجام شود. هدف اصلی در کتاب در مورد سیاست امنیتی باید بردن باشد که کاربران بدانند مجاز به چه کارهایی هستند و از

سوی دیگر، مدیران سیستم و سازمان را در تصمیم گیری برای پیکربندی و استفاده از سیستم ها یاری رسانند.

نکته مهم دیگر که به هیچ عنوان در تحلیل ریسک های امنیتی به آن اشاره نشده و برای تدوین سیاست امنیتی پس از تحلیل ریسک های سازمان لازم است به آن توجه شود این است که باید به روش هایی که دیگران برگزیده اند متوسل شد.

سازمان های بزرگ و متوسط برای تعریف سیاست امنیتی خود ناچار به پیروی روش بالا به پایین می باشند. ولی برای سازمان های کوچک انجام این کار به روش پایین به بالا نیز امکان پذیر است. در این حالت از قابلیت های ابزارهای موجود بهره گرفته می شود. بدین معنی که بهترین سیاست امنیتی در شرایطی تدوین می شود که مدیریت سازمان سیاست کلی را ارائه نموده و یا دستور پیاده سازی اصول امنیتی را در سازمان صادر کند. تدوین کنندگان سیاست سازمان باید فعالیت خود را بر پایه اصول و استانداردهای صنعتی انجام دهند. رویه ها،راهنماها و تجربیات پایه ای برای ایجاد و توسعه فناوری امنیتی در سازمان ها مختلف هستند. محصولاتی مانند ESM سازگاری و انعطاف سیاست را با سیاست ها و روال های امنیتی سیستم عامل ها، پایگاه داده ها و برنامه های کاربردی ارزیابی می نمایند.

اصولاً روش‌های ارزیابی قابلیت اطمینان بر ارزیابی «احتمال خطر» استوار است، البته در گذشته قابلیت اطمینان بر مبنای تحلیل‌های کیفی از سوابق و تجربیات در طراحی و بهره‌برداری ارزیابی می‌شد که این روش به‌عنوان یک قضاوت حرفه‌ای غیرقابل اتکاء بوده است.

قابلیت اطمینان یکی از مشخصه‌های ذاتی تلاش مدیران است که بدین صورت تعریف شده است: «احتمال عملکرد رضایت‌بخش بودن یک سیستم تحت شرایط کاری مشخص و برای مدت زمان معین».

احتمال، اولین شاخص ارزیابی اطمینان و ورش مناسبی برای تحلیل ریسک است که در بیان روش‌ها جا مانده است. سه بخش دیگر تعریف یعنی عملکرد رضایت‌بخش، زمان و شرایط کار مشخص، پارامترهای حرفه‌ای هستند که تئوری احتمال هیچ کمکی به تعیین آنها نمی‌کند. فقط متخصصین می‌توانند با استفاده از تئوری‌های مربوطه بحث قابلیت اطمینان را ارزیابی کنند که انتخاب آنها نیز به نوع مساله بستگی ندارد. با توجه به این که برای هر مساله، شاخص مناسبی در بیان قابلیت اطمینان سیستم منطبق بر

مفاهیم کاربردی و کارآیی آن باید به‌کار رود، روش‌های ارزیابی مختلف دیگری در ارتباط با شاخص‌های کنترل ریسک نیز مطرح است.

هدف اصلی ارزیابی ریسک، تعیین میزان عدم قطعیت، هزینه‌های ناشی از آن و ارائه راهکارهای کاهش این هزینه‌ها است. بنابراین برای ارزیابی ریسک باید نگرش سیستمی داشت، به این معنی که باید نتیجه عملکرد اجزاء پس از اثرات متقابل آنها بر یکدیگر مورد تجزیه و تحلیل قرار گیرند. یکی از مهم‌ترین اجزاء تاثیرگذار بر خروجی هر سیستم متغیرهای تصادفی هستند که شناسایی و تجزیه و تحلیل آنها باعث شناخت منابع خطاها خواهد شد.

ریسک به دو روش سنتی و استفاده از تکنولوژی قابل ارزیابی است. امروزه با توجه به پیچیده‌تر شدن سیستم‌ها و توزیع شدت و مقدار عدم قطعیت بین متغیرهای مختلف، استفاده از روش تکنولوژیکی از اهمیت ویژه‌ای برخوردار است.

روش‌های دیگری نیز برای ارزیابی ریسک وجود دارد که درکتاب ذکری از آن به میان نیامده است.

الف- روش ماتریس ارزیابی خطر

در روش ماتریس ارزیابی خطر، ماتریسی تشکیل می‌شود که ردیف‌های آن نشان‌دهنده احتمال وقوع خطر در پنج سطح (مکرر، احتمالاً، گاهی اوقات، با احتمال کم و با احتمال خیلی کم یا غیرممکن) بوده و ستون‌ها معرف شدت خطر در چهار سطح (فاجعه‌آمیز یا خیلی خطرناک، بحرانی، حوادث جزئی و بی‌خطر) است.

ازتجزیه‌وتحلیل ماتریس مزبور، سطوح زیر مشخص می‌شود: غیر قابل قبول، نامطلوب (تایید مدیریت ضروری است)، قابل‌قبول (ولی با توجه به تصمیم مدیریت) و قابل‌قبول بدون نیاز به بررسی است.

ب- روش تعریف سناریو

در روش فوق با بهره‌گیری از نظرات متخصصان امر، سناریوهای مختلف تعریف و با استفاده از تکنیک‌های خاص اثرات و نتایج آنها مورد تجزیه و تحلیل (تحلیل حساسیت) قرار می‌گیرد. به‌عنوان یکی از تکنیک‌های مورد استفاده در این روش می‌توان به تکنیک «What if» اشاره کرد.

نقد محتوایی

متأسفانه، تعریف همه شمولی درباره اصطلاح ریسک و مدیریت و حوزه و دسته بندی آن وجود ندارد. کمیته سرپرستی بانکداری بَسِل (Basel) یک چارچوب کاملاً مناسب منتشر کرده است که به‌عنوان Basel II مشهور است و شامل یک تعریف از مفهوم و بایسته های ریسک به شمار می‌شود که به طور گسترده ای توسط انجمن مدیریت مورد استفاده قرار می گیرد. ریسک طبق تعریف چارچوب Basel II ، ریسک زیان ناشی از عدم کفایت یا نقص فرایندهای سازمانی افراد و سیستم ها یا از وقایع خارجی تعریف می شود .

تعریف دیگری از ریسک نیز موجود است که ریسک، یعنی امکان بالقوه عدم توفیق در دسترسی به اهداف مأموریت. این تعریف شامل زیان (ناکامی در رسیدن به اهداف مأموریت) و عدم اطمینان (احتمال وقوع یا عدم وقوع ناکامی) است. به‌طور همزمان، این تعریف مناسب برای استفاده در اکثر زمینه های متفاوت است و اگرچه اشکال مختلفی از ریسک (از جمله، ریسک تجاری، عملیاتی، پروژه ای و امنیتی) وجود دارد، ولی تمامی آنها مبنای مفهومی یکسانی دارند. در عین حال، می توان تفاوت های قابل ملاحظه و ملموسی از انواع مختلف ریسک بر مبنای محتوای درک شده، قائل شد. برای مثال، یک ریسک سوداگرانه،خصلت های منحصر به فردی دارد که آن را از یک ریسک خطرناک، از جمله ریسک عملیاتی، متمایز می‌سازد. طبیعت سوداگرانه یک ریسک تجاری هم سودآوری و هم زیان را در پی خواهد داشت، درحالی‌که ریسک عملیاتی هیچ فرصتی برای سودآوری ایجاد نمی کند. همان گونه که قبلاً گفته شد، تعریف ریسک به کار رفته در این متن چنین می رساند که ریسک، یعنی امکان بالقوه عدم توفیق در دسترسی به اهداف مأموریت . عبارت موجود منعکس کننده اصطلاحات رایج و مرسوم در توصیف ریسک است. توجه به این نکته ضروری است که مأموریت یک فرایند کار و یا همان محتوایی است که ریسک در آن منظور گردیده است. تعریف مأموریت، نخستین مرحله حیاتی در توصیف ریسک است، زیرا این مرحله اساس تشخیص، شرح و تفسیر ریسک را تشکیل می دهد. تمامی دیگر عناصر مشخص شده در ارتباط با مأموریت یک فرایند کاری بررسی شده است به تعبیری دیگر که در این کتاب کمتر به آن توجه شده است تعریف موجود ریسک همان عمل یا اتفاقی است که وقتی با آسیب پذیریهای موجود ترکیب شود، به یک طیفی از زیانهای بالقوه منجر می شود. آسیب پذیریها یعنی عیب و

نقص هایی که فرایند را در معرض زیان هایی قرار می دهد؛ ضربه ها به‌عنوان زیان های بالقوه ناشی از یک ریسک درک شده، تعریف می شوند. در ریسک تمامی زیان ها از پیگیری مأموریت حادث شده اند. از آنجایی که این یک ریسک خطرناک است، سبب می‌شود تا امکان بالقوه ای برای زیاندهی فراهم سازد و هیچ امکان بالقوه ای برای سودآوری ارائه نمی دهد .

یک نوع از شرایط اضافی که می بایست به‌عنوان عامل برای معادله ریسک این کتاب در نظر گرفته می‌شد؛ کنترل ریسک است که به آن توجه کامل نشده است.کنترل‌ها شرایط و وضعیت هایی هستند که محرک یک فرایند به‌سوی تحقق مأموریت است و شامل خط‌مشی‌ها، رویه ها، روال کارها، وضعیت ها و ساختارهای سازمانی هستند که به منظور ایجاد یک تضمین معقول و منطقی برای دستیابی به مأموریت ها و حذف ،کشف و اصلاح حوادث ناخواسته طراحی گردیده اند. به تعبیری دیگر نویسنده باید به این ضرورت توجه می‌داشت که کنترل‌ها می توانند به‌روش های زیر، ریسک را کاهش دهند :

حذف یک اتفاق آغازگر یا جرقه زا؛

کنترل میزان وقوع یک جرقه یا آغازگر و اجرای برنامه های اقتضایی در زمان مناسب؛

کاهش آسیب پذیریها؛

کاهش ضربه ها یا زیانهای بالقوه.

بنابراین، یک سنجش صحیح از ریسک می بایست شامل اثرات کنترل‌ها علاوه بر چهار عنصر موجود باشد. البته باید در این کتاب به این نکته نیز توجه می‌شد که معمولا، افراد راجع به ریسک از اصطلاح تهدید استفاده می‌کنند. یک تهدید یعنی وضعیت یا اتفاقی که باعث ریسک می شود. یک تهدید ترکیبی از یک جرقه و یک یا چند آسیب پذیری می باشد، زیرا مجموع این دو عنصرمشخص کننده اوضاع و احوالی است که باعث خلق ضرر و زیان بالقوه‌ای می‌شود .

نکته دیگری که نویسنده کتاب کمتر به آن توجه نموده است راهبردهای لازم در مدیریت ریسک است یعنی وقتی که ریسک‌ها شناسایی و ارزیابی شدند، تمامی تکنیک‌های اداره ریسک در یک یا چند طبقه از چهار طبقه اصلی زیر قرار می گیرند :

انتقال
اجتناب
کاهش (یا تسکین)
پذیرش (یا نگهداری)

استفاده مطلوب از این استراتژی‌ها شاید امکان پذیر نباشد. بعضی از آنها ممکن است مستلزم رفتارهای تعاملی باشد که برای فرد یا سازمانی که در زمینه مدیریت ریسک تصمیم گیری می کند، قابل قبول نباشد. در لایه مربوط به اجتناب از ریسک: باید به استراتژی اجتناب روی آورد، یعنی انجام ندادن فعالیتی که باعث ریسک می‌شود به عنوان نمونه در این زمینه، پرواز نکردن هواپیماست، تا از ریسک سرقت آن اجتناب شود. استراتژی اجتناب به‌نظر می رسد راه حلی برای تمامی ریسک ها است، ولی اجتناب از ریسک همچنین به معنی زیاندهی در مورد فرصت های بالقوه ای است که امکان دارد به‌واسطه پذیرش آن ریسک حاصل شود. داخل نشدن به یک حوزه به منظور اجتناب از ریسک، همچنین احتمال کسب موفقیت ها را ضایع می کند.

کاهش ریسک: در استراتژی کاهش، یعنی به‌کارگیری شیوه هایی که باعث کاهش شدت زیان می شود. به‌عنوان مثال می توان به کپسول های آتش نشانی که برای فرونشاندن آتش طراحی گردیده اند، اشاره کرد که ریسک زیان ناشی از آتش را کاهش می دهد. این شیوه ممکن است باعث زیان های بیشتری به واسطه خسارات ناشی از آب شود و در نتیجه امکان دارد که مناسب نباشد. سیستم هالوژنی جلوگیری کننده از آتش ممکن است آن ریسک را کاهش دهد، ولی هزینه آن امکان دارد به‌عنوان یک عامل بازدارنده، از انتخاب آن استراتژی جلوگیری کند.

پذیرش ریسک: در استراتژی پذیرش، یعنی قبول زیان وقتی که آن رخ می دهد. در واقع خود - تضمینی یا تضمین شخصی در این طبقه جای می گیرد. پذیرش ریسک یک استراتژی قابل قبول برای ریسک‌های کوچک است که هزینه حفاظت در مقابل ریسک ممکن است از نظر زمانی بیشتر از تمامی زیان های حاصله باشد.تمامی ریسک‌هایی که قابل اجتناب و انتقال نیستند، ضرورتاً قابل پذیرش هستند. این ها شامل ریسک‌هایی می شود که خیلی بزرگ هستند که یا محافظت در مقابل آن امکان پذیر نیست یا پرداخت هزینه بیمه آن شاید عملی نباشد. در این زمینه، جنگ به‌خاطر ویژگی هایش و عدم وجود تضمین نسبت به ریسک‌هایش، مثالی مناسبی است. همچنین هر

مقداری از زیاندهی بالقوه علاوه بر مقدار تضمین شده، ریسک پذیرفته شده محسوب می شود. همچنین، ممکن است این حالت قابل قبول باشد در صورتی که امکان تحقق زیان های سنگین، کم باشد یا هزینه بیمه کردن برای مقدار پوشش بیشتر، خیلی زیاد باشد، به‌طوری که مانع بزرگی برای اهداف سازمانی ایجاد کند.

انتقال ریسک: استراتژی انتقال، یعنی موجب شدن این که بخش دیگری ریسک را قبول کند که، معمولاً به وسیله بستن قرارداد یا انجام اقدامات احتیاطی امکان پذیر است. بیمه کردن، یک نوع از استراتژی های انتقال ریسک با استفاده از بستن قرار داد است. در موارد دیگر این امر به واسطه قراردادهای کلامی انجام می گیرد که ریسک را به بخش های دیگر بدون پرداختی بابت حق بیمه، انتقال می دهد

بنابراین نویسنده محترم ضرورت داشت که به این نکات توجه می کند، زیرا که دنیای امروزین با تحولات و دگرگونی های متعددی همچون جهانی شدن، برون سپاری و ایجاد ائتلاف های استراتژیک مواجه است، مدیریت ریسک در فعالیت های سازمان ها اعم از دفاعی- نظامی- تجاری و خدمات انتفاعی اهمیت روزافزونی یافته است.که ضرورت دارد تا کتبی که در این رابطه به رشته تحریر در می‌آید، نیم نگاهی نسبت به انواع مختلف ریسک در سطوح سازمانی و استراتژی های مدیریت آن داشته باشند.

اما در حوزه بحث و بررسی سیاست های امنیتی با توجه به پیشرفت های اخیر، در آینده ای نه چندان دور، باید منتظر گسترده‌گی هرچه بیش تر استفاده از شبکه های بی سیم باشیم. این گسترده گی، با توجه به مشکلاتی که از نظر ریسک امنیتی در این قبیل شبکه ها وجود دارد نگرانی هایی را نیز به همراه دارد. این نگرانی ها که نشان دهنده ی ریسک بالای استفاده از این بستر برای سازمان های راهبردی و بزرگ است، توسعه ی این استاندارد را در ابهام فرو برده است که حتی از مهمترین آنها در کتاب شنود ساده یا آنالیز ترافیک یاد نشده است. در این نوع حمله، امکان ریسک پذیری ناشی از ضعف امنیتی در این است که نفوذگران تنها به پایش اطلاعات رد و بدل شده می پردازد. برای مثال شنود ترافیک بر روی یک شبکه، نمونه هایی از این نوع حمله به شمار می آیند و یا در قالب آنالیز ترافیک می‌توان با کپی برداشتن از اطلاعات پایش شده، به تحلیل جمعی داده ها پرداخت.

درتخصصی ترین شکستن حصار امنیتی می‌توان به تغییر هویت اطلاعات شبکه اقدام کرد، که با این روش می‌توان با تغییر هویت اصلی یکی از طرف های ارتباط یا

قلب هویت و یا تغییر جریان واقعی، فرایند پردازش اطلاعات را مختل نمود و یا با پاسخ های جعلی بسته هایی که طرف گیرنده ی اطلاعات در یک ارتباط دریافت و پالایش می کند و نفوذگر با ارسال مجدد این بسته ها خود را به جای گیرنده جازده و از سطح دسترسی مورد نظر برخوردار می گردد و در برخی از موارد که مرسوم ترین و متنوع ترین نوع حملات فعال است، تغییر پیام است. نفوذگران می‌توانند با اعمال تغییرات خاصی، دو طرف ارتباط را گمراه و مشکلاتی را برای سطح مورد نظر دسترسی – که می تواند یک کاربر عادی باشد – فراهم کنند.

بنابراین در نقد محتوایی این کتاب بایدبه صورت جدی به آسیب پذیری های محیطی به منظور پیشگیری از بروز آسیب پذیری هاتوجه فراوانی نمود. هنوز بسیاری از مدیران معتقدند که آسیب پذیری‌هارا نباید با ریسک درون محیط مرتبط بدانند ولیکن نتیجه حیاتی آن است که به همراه آسیب پذیری ها همواره طیف گسترده ای از اطلاعات منتقل می شود. در یک دید ابتدایی و سطحی این اطلاعات می تواند در مورد تکنولوژی هایی که تحت تاثیر قرار گرفته و نیز نتایج سوء استفاده از آنها باشد. در مقابل، اگر از عمیق ترین سطوح و یک دید حرفه ای به موضوع نگاه کنیم، به عنوان محقق می توان آسیب پذیری ها را در جزئیات مهیب و مخرب مشاهده کرد که یک بخش آسیب پذیر می‌تواند حساس شده و مورد سوء استفاده قرار گیرد.

یکی دیگر از راهبردهای اساسی "مدیریت ریسک" که بسیار ساده و آسان به‌نظر می‌رسید و انتظار بود در این کتاب به آن توجه می‌شد و از کنار آن عبور شده است استفاده از تجربه‌های سودمند مدیران راهبردی است. مدیران راهبردی طی سال‌ها تجربه‌اندوزی در شغل خود، به‌خوبی از تأثیر ناگوار شرایط محیطی بر محیط عملیاتی خویش آگاهی دارند و راه‌های مختلف مبارزه با شرایط سخت و دشوار را طی سال‌های پیاپی کار آموخته‌اند. اندوخته گرانبهائی که مدیران راهبردی، در توشه دارند، گنجینه با ارزشی است که هیچگاه نباید نادیده یا بی‌اهمیت انگاشته شود؛ بلکه باید چراغ راه هدایت تصمیم‌گیرندگان و برنامه‌ریزان توسعه ملی برای تدوین برنامه‌های رویاروئی با خطر در شرایط ریسک باشد؛ بدین‌معنا که موفقیت برنامه‌های تدوین‌شده برای کاهش ریسک در سطوح ملی بستگی به این دارد که تا چه اندازه به تجربه‌ها و نیازهای راهبردی و ملی توجه کرده و آن را به‌کار بسته‌ایم، در واقع باید به مدیران سطوح ملی توصیه کرد از تجربه‌های خود بیشتر استفاده کنند .

باور نگارنده این است که استفاده از تجربه‌ها زمانی کارساز و سودمند خواهد بود که مبتنی بر ارائه یک طرح متناسب با شرایط بومی و ملی برای رویاروئی با خطر باشد و لذا دستیابی به سازوکارهای مؤثر برای تخمین زمان وقوع یک پیشامد منفی و خسارت‌زا ریسک را قابل مدیریت نموده است. به دیگر سخن، آماده‌باش برای رویاروئی با وضعیت‌های نامعین و خطرزا به‌شمار می‌آید.

البته گفتنی است این نگاه مدیریتی تنها به پیش‌بینی صرف نمی‌پردازد، بلکه گزینه‌های مختلف احتمالاتی را نیز که برای پدید آمدن خطر در آینده وجود دارد، موردنظر قرار می‌دهد. بدیهی است در صورت طراحی و برنامه‌ریزی برای آینده، امکان رویاروئی با خطرها و در نتیجه کاهش ضریب زیان‌ها، بیشترمی شود .

یکی از اهرم‌های مهم،کارا و مؤثر در مدیریت ریسک، انتقال مسؤولیت ریسک به سازمان‌ها و مؤسسه‌های دیگر است. آینده نگری، سازوکار مهمی در این راستا به‌شمار می‌رود. طبیعی است که برای انجام این‌کار باید هزینه‌ای بپردازند .

آنچه در این میان اهمیت فراوانی دارد، این است که مدیران راهبردی باید بتوانند، برای حوادثی که هنوز روی نداده است، به آموزش بهای زیادی داده و زمان واطلاعات را موردتوجه قرار دهند که در پناه آن است که می توان بستر را برای گسترش آینده نگری و توجه به پیش بینی ، فراهم آورد .

نتیجه گیری علمی و پایانی نقد کتاب «مدیریت و تحلیل ریسک امنیتی» این است که عدم اطمینان محیطی و شدت رقابت فیما بین نهادها و مدیران، آنها را با چالش های متعدد مواجه می سازد که برای مدیریت مؤثر این چالش ها، رویکردهای نوین مدیریت و شایستگی های خاصی طرح و توصیه شده است. شناسایی و مدیریت ریسک یکی از رویکردهای جدید است که برای تقویت و ارتقای اثربخشی سازمان ها مورد استفاده قرار می گیرد. به طورکلی، ریسک با مفهوم احتمال متحمل زیان و یا عدم اطمینان شناخته می شود که انواع مختلف و طبقه بندی های متنوع دارد. یکی از این طبقه‌بندی ها ریسک سوداگرانه و ریسک خطرناک است. تمامی اشکال ریسک شامل عناصر مشترکی چون محتوا، فعالیت، شرایط و پیامدها هستند. طبقه بندی دیگر ریسک استراتژیک و ریسک عملیاتی است. مدیریت ریسک به مفهوم سنجش ریسک و سپس اتخاذ راهبردهایی برای مدیریت ریسک دلالت دارد. انواع ریسک ها برحسب احتمال وقوع و

تأثیر آنها قابل تقسیم است که نتیجه آن پورتفوی ریسک و اعمال استراتژی‌های مناسب (انتقال، اجتناب، کاهش و پذیرش) است .

تحولات عمده در محیط مدیریت، مثل جهانی شدن وظایف برخی از نهادها و سرعت بالای تغییرات در فناوری، باعث افزایش رقابت و دشواری مدیریت در سازمان ها گردیده است. در محیط فعالیت سازمانی، مدیریت و کارکنان می بایست توانایی برخورد با روابط درونی و وابستگی های مبهم و بغرنج میان فناوری، داده ها، وظایف، فعالیت ها، فرایندها و افراد را دارا باشند. در چنین محیط های پیچیده ای سازمان ها نیازمند مدیرانی هستند که این پیچیدگی های ذاتی را در زمان تصمیم گیری های مهمشان لحاظ و تفکیک کنند. مدیریت ریسک مؤثر که بر مبنای یک اصول مفهومی معتبر قرار دارد، بخش مهمی از این فرایند تصمیم‌گیری را تشکیل می دهد. در این نقد و بررسی این اصول به وسیله شناسایی عناصر اصلی ریسک و بررسی چگونگی تأثیر بالقوه این عناصر در موفقیت سازمان ها و چگونگی مقابله و مدیریت ریسک ها مورد بحث قرارگرفت .

از سوی دیگر در فصول کتاب به نکات اساسی و مهمی دیگری هم در کنار فصول دیگر باید اشاره می‌داشت،

۱. حساسیت یک سازمان به ریسک که تابع سه متغیر است: درجه آسیب پذیری از تاثیرات یک ریسک، اهمیت آسیب، توانایی سازمان در مهار آسیب

۲. تاثیر ریسک در طی زمان تغییر می کند و به همین دلیل فرآیند تصمیم گیری در مورد ریسک و مدیریت آن هم ثابت نیست (به عبارتی عکس العمل در برابر ریسک واحد در زمان های مختلف ممکن است متفاوت باشد)

۳. جهان ما جهانی متغیر است! در چنین جهانی، نتیجه هر گونه سرمایه گذاری بر هر موضوعی تا درجاتی مبهم و درنتیجه همراه با ریسک است و به همین خاطر مدیریت ریسک یک عنصرکلیدی در هر گونه سرمایه گذاری برای اخذ نتیجه است.

۴. ریسک و فرصت دست در دست هم دارند. هر کسی در زندگی به دنبال فرصت است و به خاطر عدم قطعیت در اموردنیا است که فرصت ها دست می دهند. ریسک های مرتبط با فرصت ها باید به نحو موثری مدیریت شوند، اگر قرار است فرصتی مد نظر قرار بگیرد.

۵. ریسک رقبا را می ترساند. ریسک آنها را از این که از فرصت ها بهره برداری کنند باز می دارد و باعث می شود تا سطحی بیشتر پیش نروند.

۶. برای پیشرفت باید ریسک پذیر بود.

۷. ریسک هم خوب است و هم بد. ریسک نیروی موثر پشت نوآوری است و در همان حال تهدیدی بزرگ است، اگر به درستی ارزیابی و مدیریت نشود. به خصوص در جایی که با موضوعات پیچیده سرو کار داریم که معمولا تکرار کارهای قبلی نیستند درجه ریسک به شدت بالا می رود.

۸. تصمیم گیری و ریسک عناصر بنیادی در فرآیند شناخت هستند.

۹. مردم بر اساس ریسک و پاداش حاصل از آن تصمیم می گیرند.

۱۰. میزان ریسک پذیری از فرد به فرد متغیر است و معمولاً بر اساس تاثیرات احتمالی شکست یا موفقیت در ریسک پذیرفته می شود.

۱۱.فرآیند شناخت در انسان بر اساس یک برداشت ذهنی ریسک را ارزیابی می کند و نه محاسبات دقیق. اما این توانایی انسان یکی از عوامل اصلی در پیشرفت بشر بوده است.

۱۲.مغز انسان به طور خودکار بر اساس اطلاعاتی که از قبل به دست آورده است و تطابق آنها با اطلاعات جدید، با به کارگیری روش های پردازش الگو (Pattern Recognition) ریسک را ارزیابی می کند.

۱۳.رفتارهای محتمل بر اساس نتایج مورد قبول به دست می آیند و نتایج به دست آمده لزوما نتایج دلخواه نیستند.

۱۴.بیشتر محققین بر این باورند که فرآیند بالا در چهار مرحله صورت می پذیرد: تنظیم کردن، قاعده سازی، بررسی و ارزیابی.

۱۵.در کنترل ریسک، مونیتورینگ و فهم تحول ریسک مهم هستند.

۱۶.ریسک ممکن است توسط عوامل درونی یا بیرونی ایجاد شود.

۱۷.ریسک بر دو نوع است: پیش بینی پذیر و غیر قابل پیش بینی

۱۸.ریسک قابل پیش بینی ریسک های شناخته شده و ناشناخته هستندا یعنی ریسک هایی که انتظار وقوع آنها می رود ولی معلوم نیست کی اتفاق بیافتند، مثل تغییر نرخ ارز.

۱۹.ریسک های غیرقابل پیش بینی، ریسک های ناشناخته و غیرقابل شناخت هستند، مثل وقوع ناگهانی یک جنگ یا ورشکستگی یک شرکت عظیم.

۲۰.به طور کلی سه شرایط مختلف وجود دارد که تحت آنها تصمیم گیری می شود: شرایط قطعی، شرایط مبهم، و شرایط ریسکی

۲۱.در شرایط قطعی تصمیم گیرنده می داند که صد درصد نتیجه مورد انتظار حاصل می شود. اما بین شرایط مبهم و شرایط ریسکی تفاوت وجود دارد.

۲۲.در شرایط ریسکی، احتمال وقوع حوادث مختلف قابل محاسبه است، اما در شرایط مبهم امکان محاسبه احتمال هم وجود ندارد.

۲۳.اغلب تلاش می شود تا شرایط مبهم به شرایط ریسکی تبدیل شود.

۲۴.در تبدیل شرایط مبهم به شرایط ریسکی چهار نوع تصمیم گیری وجود دارد:

۱. تصمیم گیرنده خوشبین است و سعی می کند با رویکرد «همه یا هیچ» نفعش را چند برابر کند و به این که ممکن است همه چیز را از دست دهد زیاد فکر نمی کند.

۲. تصمیم گیرنده بدبین است و در نظر می گیرد که چقدر خسارت را می تواند تحمل کند و به همین خاطر به حداقل منفعت قانع می شود تا جلوی ضرر را بگیرد.

۳. تصمیم گیرنده معمولا پاکباخته است و تلاش می کند تا میزان پشیمانی اش را تا حد امکان کم کند و همواره به اختلاف از دست دادن همه چیز یا به دست آوردن چیزی فکر می کند.

۴. تصمیم گیرنده تا نتواند از شرایط مبهم به شرایط ریسکی برسد تصمیمی نمی گیرد.

۲۵.در مدیریت ریسک، پنج عامل مهم وجود دارند: تعیین ریسک، طبقه بندی ریسک، تحلیل ریسک، رفتار ریسک، نتیجه ریسک.

۲۶.ریسک همواره با سه شاخص نوع ریسک، دامنه ریسک و تاثیر ریسک اندازه گیری می شود.

۲۷.در مدیریت ریسک، نقشه ریسک باید تعریف شود که شامل چهار نوع ریسک می شود:

الف- ریسک قرمز: ریسک با احتمال بالا و تاثیر زیاد،

ب- ریسک زرد بالا: ریسک با تاثیر زیاد ولی احتمال وقوع کم

ج- ریسک زرد پایین: ریسک با تاثیر کم ولی احتمال وقوع بالا،

د- ریسک سبز: ریسک با احتمال کم و تاثیر کم.

۲۸.مدیریت ریسک لزوما به معنی حذف ریسک نیست. بلکه در حد امکان تغییر ریسک قرمز به ریسک سبز است.

۲۹.نادیده گرفتن ریسک خود یک عمل ریسکی محسوب می شود.

۳۰.حذف بعضی ریسک ها اقتصادی نیست

۳۱.عقد قرارداد یک راه سنتی برای مدیریت ریسک است.

۳۲.قرارداد همچنین امکان کنترل ریسک را فراهم می کند.

پژوهشگاه علوم انسانی و مطالعات فرهنگی
پرتال جامع علوم انسانی

منابع مورد استفاده در نقد و تحلیل :

۱- ن-ک زاهدی شمس‌السادات، الوانی مهدی، فقیهی ابوالحسن، فرهنگ جامع مدیریت، چاپ اول، تهران: انتشارات دانشگاه علامه طباطبایی، ۱۳۷۶.

۲- ن-ک ویلیامز، سی آرتور – مدیریت ریسک، توسط دکتر داور ونوس، نشر نگاه دانش - ۱۳۸۲

۳- ن-ک مهندس نجف قراچورلو، ارزیابی و مدیریت ریسک، انتشارات علوم و فنون، چاپ اول، ۱۳۸۴.

۴.Dorfman, Mark S. (۱۹۹۷). Introduction to Risk Management and Insurance (۶th ed.), Prentice Hall

۵.Stulz, René M. (۲۰۰۳). Risk Management & Derivatives (۱st ed.), Mason, Ohio: Thomson South-Western

۶.Alijoyo, Antonius (۲۰۰۴). Focused Enterprise Risk Management (۱st ed.), PT Ray Indonesia, Jakarta

۷.Alberts, Christopher & Dorofee, Audrey. Managing Information Security Risks: The OCTAVESM Approach Boston, MA:Addison-Wesley, ۲۰۰۲

۸.Kloman, H. F. "Risk Management Agonists." Risk Analysis (June ۱۹۹۰)

۹.Project Management Institute (PMI), USA (۲۰۰۴),Project Management Body of Knowledge (PMBOK).

۱۰.Jae Ha Leea, Embedded options and Interest Rate Risk for Insurance companies, banks and other financial Institutions, The Quarterly Review of Economics and Finance ۴۰ (۲۰۰۰) ۱۶۹–۱۸۷.

۱۱.Zuckerman, Moving Towards a Holistic Approach to Risk Management Education-Teaching Business Security Management, Security Journal ۱۱ ۱۹۹۸, PP. ۸۱-۸۹

۱۲.Hennie Van Greuning, Sonja Brajovic Bratanovic, Analizing Banking Risk: A Framework..., World Bank, ۱۹۹۹

۱۳.John C. Choicken, Managing Risks and Decisions in Major Projects, Chapman & Hall, ۱۹۹۴.

۱۴.Michael Doumpos, Constantin Zopounidis, Assessing Financial Risks using a Multicriteria sorting procedure: the case of country Risk Assessment, Omega ۲۹ (۲۰۰۱) ۹۷-۱۰۹.

۱۵.Kay Mitusch, Dieter Nautz, Interest Rate and Liquidity Risk Mangement and the European Money Supply Process, Journal of Banking and Finance, ۲۵ (۲۰۰۱), ۲۰۸۹-۲۱۰۱.

۱۶.Jacob Lemming, Financial Rrisks for Green Electricity Investors and producers in a Tradable Green certificate Market, Energy Policy ۳۱ (۲۰۰۳) ۲۱–۳۲.

۱۷.J.-Ph. Bouchauda, Elements for a Theory of _Nancial Risks, Physica A ۲۸۵ (۲۰۰۰) ۱۸-۲۸.

پژوهشگاه علوم انسانی و مطالعات فرهنگی
پرتال جامع علوم انسانی

پژوهشگاه علوم انسانی و مطالعات فرهنگی
پرتال جامع علوم انسانی