

ایجاد برنامه مدیریت ریسک سایبری

امنیت در حال تکامل برای عصر دیجیتال

برایان آلن، براندون باپست و تری آلن هیکس

ترجمه:

سید نعمت اله حسینی اصیل، اعظم السادات میرحاج محمدآبادی



انتشارات اشجع

- سرشناسه : آلن، برایان، ۱۹۵۲ - م.
- Allen, Brian
- عنوان و نام پدیدآور : ایجاد برنامه مدیریت ریسک سایبری : امنیت در حال تکامل برای عصر دیجیتال / نویسندگان برایان آلن، براندون باپست، تری آلن هیکس ؛ ترجمه سید نعمت‌اله حسینی اصل، اعظم‌السادات میرحاج محمدآبادی.
- مشخصات نشر : تهران : اشجع، ۱۴۰۳.
- مشخصات ظاهری : ۳۵۵ ص. : جدول (بخشی رنگی).
- شابک : ۹۷۸-۶۲۲-۶۴۶۱-۵۲-۸
- وضعیت فهرست نویسی : یادداشت
- یادداشت : Building a cyber risk management program : عنوان
evolving security for the digital age ,2023.
- عنوان دیگر : امنیت در حال تکامل برای عصر دیجیتال.
- موضوع : شرکت‌های اقتصادی -- شبکه‌های کامپیوتری -- تدابیر ایمنی
- Business enterprises -- Computer networks -- Security measures
- کامپیوترها -- ایمنی اطلاعات -- مدیریت ریسک
- Computer security -- Risk management
- شناسه افزوده : باپست، براندن
- شناسه افزوده : Bapst, Brandon
- شناسه افزوده : هیکس، تری آلن
- شناسه افزوده : Hicks, Terry Allan
- شناسه افزوده : حسینی اصیل، سید نعمت‌اله، ۱۳۵۶ - مترجم
- شناسه افزوده : میرحاج محمدآبادی، اعظم‌السادات، ۱۳۵۹ - مترجم
- رده بندی کنگره : HF۵۵۴۸/۳۷
- رده بندی دیویی : ۶۵۸/۶۷۸
- شماره کتابشناسی ملی : ۹۶۹۹۷۲۵



ایجاد برنامه مدیریت ریسک سایبری

برایان آلن، براندون باپست و نری الیکس

سید نعمت اله حسینی اصیل، اعظم السادات میرحاج محمدآبادی

انتشارات اشجع

چاپ: اول - ۱۴۰۳

قیمت: ۳۵۰,۰۰۰ تومان

شمارگان: ۵۰۰ نسخه

شابک: ۹۷۸-۶۲۲-۶۴۶۱-۵۲-۸

تهران، مجیدیه شمالی، خیابان برادران محمودی شرقی، کوچه امید، پلاک ۱

تلفن: ۲۲۵۲۰۷۰۲ www.ashja.com

شرکت مشاوره مدیریت مشیر محاسب:

همراه شما در مسیر ارتقای مدیریت ریسک

معرفی

شرکت مشاوره مدیریت مشیر محاسب با نام تجاری «4M» با گرد هم آوردن جمعی از متخصصان، صاحب نظران و کارشناسان مجرب و با سابقه در حوزه مدیریت ریسک سازمانی، متعهد به ارائه خدمات نوین و تخصصی مدیریت ریسک به فعالان در فضای کسب و کار، به ویژه شرکت های بزرگ تولیدی و خدماتی در حیطه های مختلف از جمله: صنعت نفت و گاز و پتروشیمی، صنعت معدنی و فولادی، صنعت بانک و بیمه، حمل و نقل، صنعت دارویی و ... است.

خدمات ما:

مشیر محاسب طیف گسترده ای از خدمات را در زمینه مدیریت ریسک ارائه می دهد که شامل موارد زیر است:

- آموزش: برگزاری دوره های آموزشی تخصصی بلندمدت و کوتاه مدت داخلی و خارجی در زمینه های مختلف مدیریت ریسک، از جمله مفاهیم پایه مدیریت ریسک، شناسایی و ارزیابی ریسک، مدیریت ریسک عملیاتی، مدیریت ریسک اعتباری، مدیریت ریسک بازار، مدیریت ریسک نقدینگی، مدیریت ریسک تطبیق، مدیریت ریسک فن آوری اطلاعات، حاکمیت شرکتی و مدیریت ریسک.

- **مشاوره:** ارائه مشاوره تخصصی در زمینه مدیریت ریسک به سازمان‌ها در سطوح مختلف، شامل طراحی و پیاده‌سازی ساختار مدیریت ریسک، ارزیابی و بهینه‌سازی فرآیندهای مدیریت ریسک موجود، تدوین و استقرار سیاست‌ها و رویه‌های مدیریت ریسک، ارائه راهکارهای عملی برای مدیریت انواع ریسک.
- **توسعه نرم‌افزار:** ارائه نرم‌افزارهای تخصصی مدیریت ریسک متناسب با نیازهای مختلف سازمان‌ها، استقرار و پشتیبانی نرم‌افزارهای مدیریت ریسک، آموزش و توانمندسازی کارکنان در زمینه استفاده از نرم‌افزارهای مدیریت ریسک.

مزایای انتخاب مشیر محاسب

انتخاب مشیر محاسب به‌عنوان مشاور مدیریت ریسک سازمان شما مزایای متعددی را همراه دارد، از جمله:

- **تخصص و تجربه:** بهره‌مندی از تخصص و تجربه کارشناسان مجرب و با سابقه در حوزه مدیریت ریسک
- **پوشش زنجیره کامل خدمات مدیریت ریسک:** شامل آموزش، مشاوره و توسعه نرم‌افزار
- **ارائه راهکارهای جامع:** ارائه راهکارهای جامع و یکپارچه متناسب با نیازها و الزامات هر سازمان
- **تعهد به کیفیت:** ارائه خدمات با بالاترین سطح کیفیت و مطابق با استانداردهای بین‌المللی
- **مشتری محور:** تمرکز بر نیازها و خواسته‌های مشتریان و ارائه خدمات با رویکردی مشتری محور

• استفاده از فن آوری های نوین: استفاده از جدیدترین فن آوری ها و ابزارها در ارائه

خدمات

ما در مشیر محاسب معتقدیم که مدیریت ریسک، امری ضروری برای موفقیت هر سازمان در دنیای پر چالش امروز است. با انتخاب مشیر محاسب به عنوان مشاور خود، می توانید از تخصص و تجربه ما برای ارتقای سطح مدیریت ریسک در سازمان خود و دستیابی به اهداف بلندمدتان بهره مند شوید و گامی بلند در جهت ارتقای سطح مدیریت ریسک و افزایش تاب آوری سازمان خود در برابر چالش ها و مخاطرات مختلف بردارید.

با توجه به نوپا بودن دانش ریسک در کشور و فقر متون تخصصی فارسی، این شرکت یکی از مسئولیت های اجتماعی خویش را توسعه فرهنگ و اشاعه این دانش نوپا در سطح جامعه می داند، برخی از متون برجسته این حوزه را انتخاب و اقدام به انتشار آن کرده است. کتاب حاضر نیز حاصل تلاش تیم کارشناسی مشیر محاسب برای استفاده علاقه مندان و فعالان این حوزه است.

امید است که این تلاش ها گام مؤثری در گسترش فرهنگ مدیریت ریسک در سطح سازمانی و فردی باشد.

ارتباط با ما

• وب سایت: <https://4mco.ir/>

• تلفن: ۰۲۱-۲۲۲۲۸۷۷۰

• ایمیل: info@4mco.ir

فهرست مطالب

موضوع

صفحه

این کتاب برای چه افرادی مناسب است؟.....	۱۷
فصل اول: امنیت سایبری در عصر تحول دیجیتال.....	۲۳
انقلاب صنعتی چهارم.....	۲۸
امنیت سایبری اساساً یک شیوه ریسک است.....	۳۵
نظارت و پاسخگویی مدیریت ریسک سایبری.....	۳۸
تحول دیجیتال و بلوغ برنامه مدیریت ریسک سایبری.....	۴۰
امنیت سایبری فقط یک نگرانی "امنیتی" نیست.....	۴۱
برنامه مدیریت ریسک سایبری: یک نگرانی فوری سازمانی.....	۴۵
نقشه راه کتاب.....	۴۷
نکته نهایی.....	۴۸
فصل دوم: برنامه مدیریت ریسک سایبری.....	۴۹
کمسیون بورس و اوراق بهادار آمریکا صحبت می کند - و جهان را شگوش می دهد.....	۴۹
افشای رویداد ("افشای زمان حال").....	۵۱
افشای مدیریت، راهبرد و حکمرانی ریسک ("افشای دوره‌ای").....	۵۲
چارچوب برنامه مدیریت ریسک سایبری.....	۵۴
برنامه مدیریت ریسک سایبری: پيشران‌های کلیدی.....	۵۷
برآوردن تعهدات و مسئولیت‌ها.....	۶۰
وقتی مدیریت ریسک به طور کامل شکست می خورد: فاجعه بوئینگ ۷۳۷ مکس.....	۶۴
برنامه مدیریت ریسک در فاجعه‌های بوئینگ.....	۶۷
مأموریت ضروری و حیاتی: پرونده بوئینگ.....	۷۱
مزایای برنامه ریسک امنیتی.....	۷۳
مزیت ۱- به رسمیت شناختن راهبردی عملکرد ریسک امنیتی.....	۷۶
مزیت ۲- اطمینان از اینکه عملکرد ریسک سایبری بودجه مؤثر دارد.....	۷۸
مزیت ۳- حمایت از تصمیم‌گیرندگان ریسک.....	۷۹

۸۰	برنامه مدیریت ریسک سایبری: سیستماتیک اما نه ریسک صفر
۸۲	پاسخگویی و مسئولیت قانونی هیئت‌مدیره
۸۷	حکم بوئینگ و مسئولیت نظارت بر ریسک سایبری
۹۰	مدیران ارشد امنیت اطلاعات در خط مقدم مسئولیت
۹۲	نکته نهایی

۹۵	فصل سوم: حکمرانی چابک
۹۸	پنهان سازی هک شرکت اوپر
۱۰۱	حکمرانی خوب چگونه است؟
۱۰۳	همسویی با راهبرد حکمرانی سازمانی
۱۰۸	هفت اصل حکمرانی چابک
۱۰۸	اصل ۱- ایجاد سیاست‌ها و فرآیندها
۱۱۰	اصل ۲- حاکمیت، نقش‌ها و مسئولیت‌ها را در سراسر مدل سه خطی ایجاد کنید
۱۱۴	اصل ۳- همسو کردن مجموعه‌های حکمرانی چابک با چارچوب‌های موجود مدیریت ریسک
۱۱۷	اصل ۴- دامنه توسط هیئت‌مدیره و مدیران ارشد تعریف می‌شود
۱۲۰	اصل ۵- هیئت‌مدیره و مدیران ارشد تعریف می‌شود
۱۲۲	اصل ۶- فرآیندهای حاکمیت حسابرسی
۱۲۴	اصل ۷- همسویی منابع با نقش‌های و مسئولیت‌های تعریف شده
۱۲۵	نکته نهایی

۱۲۷	فصل چهارم: سیستم آگاه به ریسک
۱۳۰	چرا اطلاعات ریسک در سطوح بالا اهمیت دارند
۱۳۱	ریسک و اطلاعات ریسک تعریف شده
۱۳۵	پنج اصل سیستم آگاه به ریسک
۱۳۶	اصل ۱- تعریف چارچوب و روش ارزیابی ریسک
۱۴۰	اصل ۲- ایجاد یک روش برای آستانه ریسک
۱۴۴	اصل ۳- برقراری درک مشترک از نیازهای مبتنی بر ریسک
۱۴۶	اصل ۴- توافق بر بازه زمانی ارزیابی ریسک
۱۵۰	اصل ۵- فعال سازی فرآیندهای گزارش‌دهی

نکته نهایی.....	۱۵۲
فصل پنجم: راهبرد و اجرای مبتنی بر ریسک.....	۱۵۵
چت جی پی تی دنیای کسب و کار را تکان داد.....	۱۶۰
ریسک های هوش مصنوعی: دو غول فن آوری، دو مسیر انتخاب می کنند.....	۱۶۲
وال استریت: سریع حرکت کنید، در غیر این صورت جایگزین می شوید.....	۱۶۶
پیشگامان دنیای دیجیتال، بدون توقف در حال نوآوری.....	۱۶۷
تعریف راهبرد و اجرای مبتنی بر ریسک.....	۱۷۰
شش اصل راهبرد و اجرای مبتنی بر ریسک.....	۱۷۲
اصل ۱- تعیین آستانه های قابل قبول ریسک.....	۱۷۲
اصل ۲- هم راستا کردن راهبرد و بودجه با آستانه های ریسک تایید شده.....	۱۷۶
اصل ۳- اجرا برای رسیدن به آستانه های ریسک تایید شده.....	۱۸۰
اصل ۴- پایش مستمر.....	۱۸۲
اصل ۵- حسابرسی بر اساس ریسک.....	۱۸۴
اصل ۶- لحاظ کردن طرف های ثالث در مواجهه با ریسک.....	۱۸۵
نکته نهایی.....	۱۸۸
فصل ششم: تشدید و افشای ریسک.....	۱۸۹
کمیسیون بورس و اوراق بهادار و افشای ریسک.....	۱۹۲
نهادهای نظارتی در سراسر جهان نیازمند افشای ریسک هستند.....	۱۹۳
تشدید ریسک.....	۱۹۷
طبقه بندی ریسک سایبری.....	۲۰۰
تشدید و افشا: فراتر از حوادث امنیتی.....	۲۰۴
افشا: یک نگرانی اجباری برای سازمان ها.....	۲۰۵
رسوایی اکویفکس.....	۲۰۷
ملاحظات کمیسیون بورس و اوراق بهادار در خصوص اهمیت مالی.....	۲۱۲
برنامه ی مدیریت ریسک سایبری و هم سویی با مدیریت ریسک سازمانی.....	۲۱۵
پنج اصل تشدید و افشای ریسک.....	۲۱۶
اصل ۱- ایجاد فرایند تشدید ریسک.....	۲۱۷
اصل ۲- ایجاد فرآیندهای افشاء - همه ی سازمان ها.....	۲۲۱

اصل ۳- ایجاد فرآیندهای افشاء - شرکت‌های سهامی عام	۲۲۳
اصل ۴- بررسی فرآیند تشدید و افشاء	۲۲۹
اصل ۵- حسابرسی فرآیند تشدید و افشاء	۲۳۱
نکته نهایی	۲۳۲

فصل هفتم: اجرا (پیاده سازی) برنامه مدیریت ریسک سایبری

سفر مدیریت ریسک سایبری	۲۳۷
آغاز سفر مدیریت ریسک سایبری	۲۳۹
اجرای برنامه مدیریت ریسک سایبری	۲۴۳
حکمرانی چابک	۲۴۳
سیستم آگاه به ریسک	۲۵۱
راهبرد و اجرای مبتنی بر ریسک	۲۶۷
تشدید و افشای ریسک	۲۷۴
جلب حمایت برای پیاده سازی برنامه مدیریت ریسک سایبری	۲۸۰
نکته نهایی	۲۸۸

فصل هشتم: کاربرد برنامه مدیریت ریسک سایبری در مدیریت ریسک عملیاتی و

تاب آوری	۲۸۹
کارکردهای سازمانی که با تاب آوری عملیاتی در ارتباط هستند و به آن کمک می کنند	۲۹۴
حمله بدافزار سیستم های مرسک را در سراسر جهان تعطیل می کند	۲۹۸
راهبری تاب آوری عملیاتی با استفاده از چهار مؤلفه اصلی برنامه مدیریت ریسک سایبری	۳۰۳
حکمرانی چابک	۳۰۳
سیستم آگاه به ریسک	۳۰۵
راهبرد و اجرای مبتنی بر ریسک	۳۰۶
تشدید و افشای ریسک	۳۰۷
نکته نهایی	۳۰۸

فصل نهم: هوش مصنوعی و فراتر از آن؛ آینده ی مدیریت ریسک در دنیای دیجیتالی

تعریف هوش مصنوعی	۳۱۱
هوش مصنوعی: دنیایی کاملاً جدید از ریسک	۳۱۵

- هوش مصنوعی: هم ریسک و هم فرصت، سازمانی که آن را نادیده بگیرد، بازنده است..... ۳۱۹
- طبقه‌بندی و اصطلاحات یادگیری ماشین خصمانه براساس مؤسسه ملی استانداردها و فن‌آوری ۳۲۰
- چارچوب‌های مدیریت ریسک با پیامدهای هوش مصنوعی..... ۳۲۳
- مفاهیم کلیدی پیاده‌سازی هوش مصنوعی و چارچوب‌های مرتبط..... ۳۲۹
- فراتر از هوش مصنوعی: مرزهای دیجیتال، در حرکتی دائمی..... ۳۳۷
- نکته نهایی..... ۳۴۱
- پیوست: چارچوب برنامه مدیریت ریسک سایبری ویرایش اول..... ۳۴۳**
- هدف و زمینه..... ۳۴۳
- ساختار چارچوب برنامه مدیریت ریسک سایبری..... ۳۴۴
- توجه: افشای چارچوب..... ۳۴۹

www.ketab.ir

این کتاب برای چه افرادی مناسب است؟

کتاب به گونه‌ای طراحی شده است که ارزش واقعی را به طیف گسترده‌ای از خوانندگان ارائه کند. در عین حال در هر مرحله مشخص کرده‌ایم که کدام خوانندگان بیشتر از کدام محتوا متأثر خواهند شد. نقش‌های کلیدی که در این کتاب دیده‌ایم عبارتند از:

• کارشناسان امنیت در هر سطحی

مدیریت ریسک، بدون شک، به عنوان یک رویکردی با سابقه طولانی و کارآزموده شناخته می‌شود. طی چندین دهه، روش تکامل یافته، در میدان عمل به کار گرفته شده و به طور مداوم ارتقاء یافته است. با این وجود، علیرغم اثربخشی اثبات شده، مدیریت ریسک اغلب به عنوان یک برنامه جامع و رسمی برای امنیت در نظر گرفته نمی‌شود.

توسعه یک برنامه مدون برای مدیریت ریسک سایبری، مزایای متعددی را به همراه دارد که به نوبه خود به بلوغ، هدفمندی و اثربخشی هر چه بیشتر این رویکرد کمک می‌کند.

• کارشناسان امنیت در هر وظیفه‌ای

همان‌طور که در این کتاب به طور خاص بر امنیت سایبری تمرکز شده است، لازم به ذکر است که اصول و چارچوب‌های بنیادی ارائه شده در زمینه مدیریت ریسک، فراتر از این حوزه عمل کرده و در سایر سطوح و بخش‌های مختلف نیز قابل انطباق و اجرا هستند. با حذف کلمه "سایبر" از عنوان، می‌توان عناصر اساسی این رویکرد را در زمینه‌های دیگری

همچون: مدیریت ریسک‌های برنامه‌نویسی، "مدیریت کلاهبرداری (تقلب)"^۱، "مدیریت تداوم کسب‌وکار" و "تاب‌آوری عملیاتی"^۲ به کار گرفت.

• هیئت‌مدیره

این کتاب با هدف ارائه درک جامع از نقش و مسئولیت‌های خطیر مدیران در نظارت بر برنامه مدیریت ریسک سایبری طراحی شده است. در این کتاب، بینش‌هایی در مورد انتظارات نقش مدیریت در ایجاد و هدایت این برنامه ارائه می‌شود. اصول بنیادی این کتاب بر اهمیت نگاه به امنیت سایبری به عنوان یک ریسک کسب‌وکار تأکید می‌کند و دیدگاهی را به مدیران ارائه می‌دهد که آنها را قادر می‌سازد تا سؤالات مرتبط‌تری بپرسند و راهنمایی‌های بهتری برای مدیریت ریسک سایبری ارائه دهند. با انتقال تمرکز از جزئیات فنی تاکتیک‌ها و عملیات امنیت سایبری به نقش نظارت راهبردی بر ریسک‌های گسترده‌تر، مدیران می‌توانند اثربخشی برنامه مدیریت ریسک سایبری خود را به طور قابل توجهی ارتقاء دهند و در عین حال، دفاع سازمان در برابر تعهدات قانونی و نظارتی فزاینده را نیز تقویت کنند.

• مدیران ارشد و رهبران خطوط کسب‌وکار

این کتاب به اهمیت درک امنیت به عنوان یک عمل ریسک برای تصمیم‌گیرندگان سطح بالا می‌پردازد. با درک این موضوع، این افراد می‌توانند:

- مسئولیت‌های خود را در قبال امنیت به طور کامل درک کنند: تصمیم‌گیرندگان سطح بالا باید از نقش خود در محافظت از سازمان در برابر این تهدیدات و عواقب احتمالی عدم انجام این کار آگاه باشند.

¹ Fraud Management

² Operational Resilience

○ از خود در برابر افزایش مسئولیت محافظت کنند: درک امنیت به عنوان یک عمل ریسک به آنها کمک می‌کند تا اقدامات پیشگیرانه لازم را انجام داده و از خود در برابر این مسئولیت‌های فزاینده محافظت کنند.

○ انتظارات امنیتی را به طور مؤثر تنظیم کنند: تصمیم‌گیرندگان سطح بالا باید انتظارات واضحی از سطح امنیت مورد نیاز در سازمان خود تعیین کنند. این امر مستلزم درک ریسک‌های مختلفی است که با آنها مواجه هستند و انتخاب اقدامات کنترلی مناسب برای کاهش این ریسک‌ها است.

○ تصمیمات ریسک امنیتی مناسب و آگاهانه‌ای اتخاذ کنند که با راهبردهای کلی آنها هماهنگ باشد.

• نهادهای نظارتی

نهادهای نظارتی می‌توانند از راهبردهای موجود در این کتاب برای کمک به توسعه مقررات کاملاً تعریف شده بر اساس انتظارات معقول و قابل تکرار استفاده کنند. یک طبقه‌بندی مشترک و انتظارات مشترک، تلاش‌های آنها را کارآمدتر، مؤثرتر و هم‌افزایی می‌کند.

• حسابرسان

در دنیای دیجیتال امروز، امنیت سایبری به دغدغه‌ای حیاتی برای تمامی سازمان‌ها تبدیل شده است. متخصصان حسابرسی، به عنوان ناظران امین، نقشی خطیر در ارزیابی و ارتقاء سطح امنیت سایبری در این سازمان‌ها ایفا می‌کنند. تمرکز اصلی حسابرسان در حوزه امنیت سایبری، بر بهترین شیوه‌ها و کارایی کنترل‌ها و فرآیندهای امنیتی است. آنها با بررسی دقیق این موارد، انطباق آنها را با سیاست‌ها، استانداردها، چارچوب‌ها و مقررات تعیین شده ارزیابی می‌کنند. این کتاب، با ارائه **ساختاری جامع** برای حسابرسان، به آنها در انجام این وظیفه خطیر یاری می‌رساند. چارچوب ارائه شده در این کتاب، بر اجرای امنیت در رابطه با **اشتهای ریسک و تحمل ریسک** مورد انتظار کسب‌وکار تمرکز دارد.

• رهبران کسبوکار و متخصصانی که ممکن متأثر از ریسک‌های ناشی از دیجیتالی شدن

قرار گیرند

تحول دیجیتال دنیای ما را با سرعتی بی‌سابقه در حال تغییر است. این دگرگونی، پیامدهای گسترده، پیچیده و گاه غیرقابل پیش‌بینی برای افراد، جوامع و سازمان‌ها به همراه دارد. در این میان، رهبران کسبوکار و تصمیم‌گیرندگان در تمامی سطوح سازمانی، نقشی کلیدی در هدایت و مدیریت این تحول ایفا می‌کنند. برای موفقیت در این دنیای در حال تغییر، آنها باید با چالش‌ها و فرصت‌های ناشی از دیجیتالی شدن آشنا باشند و بتوانند تصمیمات آگاهانه‌ای در مورد نحوه استفاده از فن‌آوری برای ارتقاء اهداف سازمان خود اتخاذ کنند. در نتیجه، متخصصان در بسیاری از رشته‌های مختلف - بیشتر رهبران کسبوکار و تصمیم‌گیرندگان در اکثر عملکردهای سازمانی - ارزش واقعی را در یادگیری نحوه شناسایی ریسک‌های دیجیتال سازی و تصمیم‌گیری آگاهانه در مورد متعادل کردن ریسک و پاداش خواهند یافت.

• نکته نهایی

تحول دیجیتال یک سفر است، نه مقصد. این یک فرآیند مداوم یادگیری، سازگاری و نوآوری است که بر نحوه زندگی، کار و ارتباط ما با یکدیگر تأثیر می‌گذارد. در این سفر، هیچ راه حل سریعی وجود ندارد. چالش‌ها و موانع متعددی در مسیر وجود دارد و یادگیری و ظرافت‌های آن بی‌انتهاست. با این حال، ارزش این سفر بسیار فراتر از چالش‌های آن است. تحول دیجیتال فرصت‌های بی‌ظنیری را برای بهبود زندگی، ارتقاء کسبوکار و ایجاد دنیایی پایدارتر به ارمغان می‌آورد. برای موفقیت در این سفر، باید تصورات خود را به چالش بکشیم. ما باید از راه‌های سنتی تفکر و انجام کار فراتر رفته و ذهن خود را برای ایده‌ها و امکانات جدید باز کنیم. همچنین باید مشتاق یادگیری باشیم. دنیای دیجیتال دائماً در حال تحول است و برای همگام شدن با این تغییرات، باید دانش و مهارت‌های خود را به طور مداوم به

روز کنیم. و در نهایت، باید کنجاو باشیم. کنجاوی موتور محرکه نوآوری است و کلید کشف فرصت‌های جدید در دنیای دیجیتال است.

سفر حرفه‌ای شما فرصتی برای یادگیری، رشد و پیشرفت است. با کسب دانش، مهارت‌ها و تجربیات جدید، می‌توانید به توانمندترین نسخه از خودتان تبدیل شوید و به اهدافتان دست پیدا کنید.

www.ketab.ir