پذیرش فناوریهای نوین در سازمان

ترجمه: عباس نصیری زنگ آباد
anasiri18@yahoo.com

باوجود توسعه چشمگیر فناوریهای جدید، برخی سازمانها نیاز به پذیرش چنین فناوریهایی را به‌طور کامل به‌دست فراموشی سپرده اند و یا اینکه نسبت به تصمیم گیری درباره فرایندهای پذیرشی مربوط و اقدام به پیاده سازی آن با سرعت بسیار پایینی حرکت می‌کنند .

برخی از مدیران تمایل دارند تا بهترین فناوریهای موجود دردنیای تجارت را به‌کار گیرند ، در عین حال به‌نظر می رسد که بسیاری از آنها گرایش به چشم پوشی از اثرات انسانی و سازمانی این فناوریها دارند.

جامعیت ایـن فناوریهای جدید و تواناییهای بالقوه آن را می‌توان در واقع به عنوان منبع بالقوه ای از ضعف در نظر گرفت . دلیل این امر ناتوانی مدیران نسبت به استفاده از این فناوریها برابر رقبای خود یا ناتوانی شان در بهره برداری از فرصتهای ناشی از این فناوریها است . جهت حل مسئله بایستی قابلیتهای این فناوریها ، کفایتشان برای کسب و کار ، امکان بهره برداری از مزایای آن و تلاش در جهت کسب ذهنیتی نو از مدیریت را درک کرد . در عین حال ، درک نحوه ارتباط دقیق فناوریهای جدید با سیستمهای اطلاعاتی و نیز چگونگی تضمین تداوم کسب و کار با توجه به امنیت چنین فناوریهایی ، بسیار ارزشمند است .

بسیاری از کسب و کارهای کوچک و متوسط در راستای پرهیز از زوال سازمانی ، خود را از نظر اقتصادی متعهد به اتخاذ این فناوریها می‌کنند . آنها بایستی این کار را از طریق توجه به ریسک‌های ذاتی فناوریهای مزبور و نیز امنیت تداوم کسب و کار خود ـ حتی بعد از رویدادهای غیر منتظره و سخت ـ انجام دهند .

فناوری اطلاعات به عنوان یک نوآوری

برای دهه‌های متمادی ، ارزش و اهمیت سیستمهای اطلاعاتی و فناوری اطلاعات و ارتباطات نقشی تعیین کننده و فراگیر در کسب و کارهای سازمانی داشته است. آرایش سریع اینترنت و پایگاههای داده‌ای سازمانی در دهه های ۸۰ و۹۰ ، فرایند تعدیل رفتارهای تجاری و حیطه ارتباطی آن با بازارهای خود را تشدید کرده است . در این زمان ، ما می‌توانیم به وجود میلیونها آژانـس که تعاملی پیوسته و مستقل با ابزارهای محاسباتی دارند ، اشاره کنیم .

این وضعیت و تحولات احتمالی آن، چالشهای متعددی را در برابر تواناییهای ما نسبت به طراحی و ارائه سیستمهای اطلاعاتی مطرح می‌سازد . به هر حال ، برای بسیاری از سازمانها ، سیستم‌های اطلاعاتی و در کل فناوری اطلاعات و ارتباطات ، هنوز در راستای عملکرد بازاری و ارتباط با دست اندرکاران آن نقشی نوآورانه دارد . این به معنی آن است که ، فرایند پذیرش ، به عنوان عینیتی امکان پذیر از فرایند تصمیم گیری ویا مسائل مدیریتی در آمده است . انگیزه برای نوآوری زمانی در سازمان ایجاد می‌شود که تصمیم گیرندگان شکافهای عملکردی را مورد توجه قرار دهند یا پی برند که وضعیت موجود سازمان رضایت‌بخش نیست .

بهبودهای تکنولوژیک و فرایندی ، نقشی ملموس در تحقق اهداف کیفی و عملکردی دارند. تشخیص این بهبودها که باعث افزایش سطح کیفی سازمان می‌شود ، روندی تعیین کننده برای عملکرد فرایندی است. از جنبه استراتژیک ، موفقیت فرایندهای نوآوری مدیریتی بسته به تلاشهای رقابتی است . این تلاشها ممکن است شامل دانش عمیقی از پیشرفتهای تکنولوژیک و تحلیل کافی از مزیتهای شبکه ها باشند . این به معنی آن است که مدیران بایستی فناوریهایی را که الزاما با ایجاد سطوح بالای دانش و نیز بهبود کیفیت بدیلهای ارائه شده تلفیق می‌شوند ، مورد توجه قرار دهند .

این ملاحظات مربوط به ارزش اطلاعات، بایستی بر ارزیابی سازمان از فناوری اطلاعات متمرکز شود . ارزیابی اجرایی قبلی ممکن است مقدم بر فرایند تصمیم گیری باشد ، یعنی قبل از نصب فناوریهای محاسباتی در سیستم‌های اطلاعاتی مربوط به آنها . بعد از این عمل ، سازمان می‌تواند برارزیابی فرا عملکردی این فناوری متمرکز شود ، یعنی ارزیابی مربوط به استفاده عملیاتی ازفناوری اطلاعات .

آشکار است که بسیاری از بخشها از قبیل خدمات مالی ، فناوری اطلاعات ، تولید ، حمل و نقل، مشاوره ، تولید، خرده فروشی، عمده فروشی و انتشارات ، با ارزیابی استفاده عملیاتی از ICT مرتبط هستند ، برای اینکه آنها همیشه بر همه ظرفیتهای IT متکی اند . به‌هرحال ، ارزیابی این تواناییها و مزایای مربوط به آنها که ممکن است از

طریق سازمان مورد بهره برداری قرار گیرد ، فرایندی پیچیده است که در آن هیچ توافقی نسبت به روش ایده آل ارزیابی یا نحوه بهتر انجام دادن آن وجود ندارد .

در زمینه ICT ، فرایند ارزیابی از طریق ابزارهای کمی و یا کیفی برای تعیین ارزش IT نسبت به سازمان تعریف می‌شود . تعریف دیگر شامل تشخیص و کمی سازی هزینه ها و مزایای سرمایه گذاری IT است. برخی پژوهشگران بیان می‌کنند که ارزیابی سرمایه گذاری IT فرایندی است که در نقاط مختلفی از زمان و یا به‌صورت مستمر انجام می‌گیرد . این امر به صورت صریح ، کمی و کیفی به دنبال تاثیرات پروژه IT است .

جهت استفاده بهتر از منابع مدیریتی ، توسعه و پذیرش فناوریهای نوین بایستی با شواهد اثربخشی هزینه ای و مدیریتی آن مرتبط باشد . با این حال ، باوجود پیشرفتهای عمده اخیر در اجرا و ترویج ارزیابی ICT، توسعه این فناوریها تاثیر اندکی در بسیاری از سازمانها دارد .

این امر تا حدودی به دلیل پیچیدگی نیروهایی (ازقبیل مقاومت در برابرتغییر ، اشتیاق مدیر ، مبارزات رسانه ای ، نظرات مشتریان ، مشوقهای کارفرما و توسعه های سازمانی) است که توسعه فناوریهای جدید و روش تعامل ارزیابی ICT با آنها را تعیین می‌کند .

سایر محدودیتها

مضاف بر این نیروهای متعامل ، دو محدودیت دیگر در ارتباط با ارزیابی ICT وجود دارد . اولی محدودیت سازمانی است : پیچیدگی محیط درونی که ارزیابی فناوری بایستی درآن انجام گیرد و درنتیجه ارتباط آن با تصمیم گیرندگان مورد نظر . دومی ، محدودیت مربوط به تعارضهای ارزشی است که با ظهور فناوریهای جدید ایجاد می‌شود و ممکن است بر بکارگیری رویه ها و روشهای سنتی تاثیرگذار باشد . درک روشن این محدودیتها و تعامل متقابل آنها جهت اداره بهینه فناوریها در سیستم ضروری است .

تاکید بردرک بافت سازمانی مرتبط با توسعه نوآوریهای ICT اهمیت بسزایی دارد. ما بایستی عوامل متعددی از قبیل وجود عامل تغییر ، حمایت مالی ، جو مدیریتی و مدیریت منابع انسانی را به عنوان ویژگیهای بافت سازمانی تغییر در نظر بگیریم .

موانع پذیرش برخی فناوریهای جدید کدامند ؟

برخی سازمانها واقفند که تلاش نوآوری و پذیرش رویه ها و فناوریهای جدید ممکن است باعث افزایش رقابت پذیری سازمان شود . در حقیقت ، نوآوران می‌توانند همان سرمایه گذاران باشند و این زمانی است که آنها قادر به اداره وظایف تحقیق وتوسعه باشند . به علاوه ، کارکنان دانشی (سرمایه انسانی) می‌توانند با مد نظر قرار دادن بازارهای هدف، قادر به دفاع از سازمان در برابر حرکات تهاجمی رقبایشان باشند .

مدیریت دانش ، بر افرادی نظر دارد که درگیر ایجاد ، توزیع و تقویت دانش در میان حوزه های وظیفه ای هستند .

این درگیری ، پایه فرهنگی سازمان است که بسته به یادگیری ، کار تیمی ، تسهیم دانش و نوآوری است . مدیران می‌توانند برنامه های تشویقی برای درگیرسازی کارکنانشان در نقشها ، فعالیتها و فرایندهای دانش پایه تجویز کنند.

به‌هرحال ، بسیاری از کسب وکارهای با اندازه متوسط قادر به پذیرش سریع فناوریهای جدید نیستند و این مشکل و یا بی میلی بایستی بررسی شود. برخی عوامل مانع پذیرش فناوریهای نوین هستند :

ذهنیت مالکان : کارکنان مثل مالکان فکر نمی‌کنند و رابطه مالکان با کسب وکار تفاوتی بنیادی با سایرین دارد . بسیاری از مالکان کسب و کارهای خود را با توجه به نگرشهای سنتی شان اداره می‌کنند و علاقه‌ای به نوآوری و یا فرایندهای مدرن ندارند .

ابعاد سازمانی : برای برخی کسب و کارهای متوسط ، بکارگیری فرایندهای تجاری که از قبل مورد استفاده بوده است ، کاملا کفایت می‌کند . به علاوه اطلاعات مربوط به مشتریان (نیازها ، رفتارهای خرید و سطوح رضایت) بر مبنای روابط شخصی است.

ضعف کاربران در بهره‌گیری از فناوریهای جدید: این مشکل ممکن است منجر به استفاده ناقص از تجهیزات و کاربردها شود . در نتیجه ، بکارگیری همه ظرفیتهای بالقوه ناشی از فناوریهای محاسباتی غیر ممکن است .

مقاومت در برابر تغییر : باوجود سرعت بالای ICT ، ما هنوز مجبور به رویارویی با چنین وضعیتی هستیم : برخی کارکنان تمایلی به تعدیل روشهای شخصی اجرای وظایف معمول خود ندارند . این امر دو دلیل دارد . نخست ، آنها تمایلی به یادگیری نحوه سروکار داشتن با فناوریهای نوین ندارند . دوم ، برای بعضی افراد بشری ، تغییر ممکن است باعث ایجاد حس نا امنی شود.

محدودبودن بکارگیری فناوریهای نوین به برخی حوزه‌های وظیفه‌ای: (برای نمونه: تولید) این محدودیت می‌تواند به عنوان نیرویی بازدارنده در نظر گرفته شود .

نگرانی از مواجهه با فناوریهای نوین به عنوان منبعی از بی امنیتی سازمانی : زمانی که داده ها با توجه فنون سنتی مورد پردازش قرار می‌گیرند ، اطلاعات به‌دست آمده مشهود و احتمال نابودی یا سرقت آنها بسیار پایین است .

برخی مدیران ممکن است تصور کنند که پیچیدگی صرف شبکه های مدرن کسب و کار ، بزرگترین ضعف برای سازمانهاست. به‌هرحال مدیرانی که مسئول ارزیابی ICT هستند ، مجبور به درک نحوه تعامل این فناوریهای نوین با طرح های موجود هستند. آنها همچنین باید اطمینان حاصل کنند که منابع کافی برای نگهداری سطوح عملکردی مورد نیاز موجود است . تردیدی نیست که تقریبا همه خدمات ارتباطی می‌تواند به عنوان ریسکی امنیتی در نظر گرفته شود، برای آنکه مزاحمان توانایی اختلال در سیستم را دارند و بیانیه های امنیتی به صورت حقایقی عام تلقی می‌شوند . به‌هرحال ، پتانسیل آسیب‌پذیری به معنی ضعف نیست . روشها و فنونی نیز جهت حفاظت از سرمایه های سازمانی وجود دارد .

پذیرش ریسک‌های نوین

تلاشهای نوآوری شامل پیگیری آزمایشها، توسعه فناوریهای جدید، خدمات

ویا محصولات جدید ، فرایندهای نوین و ساختارهای جدید سازمانی است. اندیشمندان جدید مدیریتی واقفند که اطلاعات نتیجه تکامل دانش بوده و شبکه‌ای یکپارچه از رابطه میان تلاش هوشمندانه ونوآوریهای تکنولوژیک در حال گسترش است .

با توجه به برخی کارهای انجام شده در این زمینه ، سازمانهایی که قادر به شبیه سازی و بهبود دانش سرمایه انسانی خود هستند ، آمادگی بیشتری جهت مواجهه با تغییرات سریع امروزی و نیز عرضه نوآوری در جاهایی که مصمم به سرمایه گذاری و رقابت هستند ، دارند .

مدیران بایستی بدانند که مهارتهای منابع انسانی و سطح انگیزشی آنان امکان دریافت پیشنهادهای خلاق و متفاوت و همچنین فعالیتهای تحقیقاتی مربوط به نوآوریها را به وجود می آورد .

با این وجود ، سازمانها در حال تجربه برخی واقعیتهای ناشناخته‌اند و این به معنی آن است که مدیران مجبور به رویارویی با ریسک‌ها هستند . با توجه به دیدگاه ریسک ، می‌توان گفت که احتمال بروز چنین نتیجه ای ، تابعی از میزان حفاظتی است که سازمان در برابر سطح ریسک‌های رویاروی خود به عمل می آورد . مدیران مجبور به ارتقای مدیریت امنیتی در داخل سازمان خود هستند و این امر در درجه اول از طریق اتخاذ ارزیابیهای جامع از ریسک صورت می‌پذیرد .

سازمانهای امروزین ، حتی بیشتر از قبل ، نیازمند گزینه های استراتژیک برای کنترل ریسک‌های اجتناب ناپذیر هستند. این فرایند کنترلی نیازمند شناخت دقیق ریسک و تشخیص طیفهایی است که ممکن است جهت طبقه بندی کنترل‌ها به‌کار روند . ارزیابی ریسک بایستی بر مبنای احتمال رویداد و تاثیر بر بهره وری سازمان صورت گیرد . همچنین مهم است که سازمانها بدانند مدیران از چه منابعی می‌توانند اطلاعات مربوط به امنیت و پیشنهادهای فنی را جمع آوری کنند. این به‌دلیل آن است که آنها قادر به ارائه پیشنهادهایی درباره آسیب پذیری امنیتی و روشهای کاهش ریسک آسیبهای

نگرشهای سنتی مالکان کسب و کار، نبود پذیرش سازمانی، ضعف کاربران در بهره‌گیری از فناوریهای جدید و محدودبودن بکارگیری فناوریهای نوین به برخی حوزه‌های وظیفه‌ای از جمله موانع پیش روی پذیرش فناوریهای نوین در سازمان است.

ویژه نسبت به سیستم‌های مختلف عملیات کامپیوتری هستند . در هرچیزی که با ICT سروکار دارد ، مدیران بایستی چالشی مستمر را در نظر بگیرند . در محیط کسب و کار امروزی حفظ اعتماد مشتریان و پشتیبانی از کسب و کار خویش به معنی تامین امنیتی شبکه ها و ارتباطات با طیف وسیع است. موفقیت ما بسته به اتخاذ گامهایی جهت محافظت از داده های حیاتی است. زمانی که کسب و کارها رشد می‌یابد و متناوبا" از اینترنت جهت ارتباط با ادارات، مشتریان و دست اندرکاران استفاده می‌شود ، سازمانها خود را در برابر تهدیدات بزرگتری قرار می‌دهند . این به معنی آن است که آنها نیازمند مجموعه ای از راه حلهای معتبر برای امنیت اینترنتی هستند . برخی برنامه‌ها امنیت تثبیت شده ای را برای کسب و کارهای متوسط به همراه راه حلهای فنی مختلف ارائه می‌دهند . برپایی برخی از آنها به‌طرزی استثنایی ساده بوده و از طریق ابزارهای مبتنی بر جستجوگر قابل اداره هستند. این امر به مدیران اجازه می‌دهد تا امنیت شبکه هایشان را براحتی برقرار سازند. برای مثال کاربران را قادر می‌سازد تا به ایجاد شبکه های اختصاصی مجازی مبادرت نمایند . فعالیت این شبکه‌ها مانند شبکه های تجاری خصوصی پر هزینه است، اما از زیر ساختار اینترنتی کم هزینه بهره می‌برند .

دانش تامین امنیت اطلاعات

مدیران برای تامین پشتیبانی و دفاع از سازمان خود بایستی سطح مناسبی از دانش را در ارتباط با جنبه های اصلی امنیت اطلاعات در اختیار داشته باشند . به عنوان نمونه :

۱. برداشتی کلی و درکی واقع بینانه از امنیت اطلاعات.

۲. ساختارهای امکان‌پذیر امنیت اطلاعات، شامل چیستی و چگونه بکارگیری آن.

۳. روش مناسب برای نگهداری کنترل‌های ریسک.

٤. نقش مدیریت در توسعه ، نگهداری و اعمال سیاستها ، استانداردها ، فعالیتها، رویه ها و رهنمودهای مربوط به امنیت اطلاعات.

۵. تهدیدات پیش‌روی امنیت اطلاعات و تهاجمات متداول، مرتبط با این تهدیدات.

٦. چگونگی توسعه یک طرح اقتضایی (شامل طرح واکنش به رویدادها ، طرح آشکارسازی اختلالات ، طرح های تداوم کسب و کار و بخشهای آن).

۷. نیاز به برنامه های امنیت فیزیکی.

۸. مشکلات عمده حاصل از تغییرات سریع و تاثیر بالقوه آنها بر امنیت اطلاعات.

۹. نحوه ایجاد یک برنامه کامل نگهداری امنیت اطلاعات.

آیا می‌توان ادعای تداوم داشت ؟

برخی اختلالات تکنولوژیک تاثیر زیان آوری بر صنعت و تجارت ـ هم ازجنبه زمان و هم هزینه ها ـ دارند . درصد بالایی از کسب و کارهای کوچک که رویدادهای مختل کننده را تجربه می‌کنند ، هرگز شروع مجددی نداشته اند . تجارت و صنعت می‌توانند، فعالیتهای بازدارنده ای را نسبت به محدودسازی آسیبها و زیانهای ناشی از اختلالات تکنولوژیک تدارک ببینند و به عملیات عادی خود در زمانی کوتاه برگردند . این امر از طریق طراحی و ایجاد طرح اقتضایی میسر می‌شود . این طرح شامل سه عنصر اصلی است : طرح واکنش الزام آور، طرح آشکارسازی اختلالات و طرح تداوم کسب و کار .

باوجود تعدد اختلالات ، سازمان باید

طرحی برای فراهم سازی تداوم وظیفه ای کسب و کار وجود داشته باشد . این طرح بسته به شناسایی وظایف حیاتی کسب و کار و منابع لازم برای پشتیبانی از این وظایف است.

رویدادها و کنترل

با توجه به قوانین و فرایندهای کنترل داخلی ، می‌توان رویدادها را جهت به‌دست آوردن درکی بهتر از تهدیدات و آسیب پذیریهای سازمانی به‌صورت داخلی مورد مطالعه و بررسی قرار داد . ظرفیت اداره رویدادها و پیش بینی پیامدهای آنها مبنای مقابله با زیانهای ناشی از حوادث آینده است. وقوع چنین حوادثی مستلزم فرایندی واکنشی بوده و شامل شناسایی آن ، ارزیابی میزان ریسک آن و نیز مجموعه فعالیتها و رویه های قابل اکتشاف می‌باشد . به این دلایل ، اتخاذ فناوریهای جدید ـ چه فناوریهای اختصاص یافته به تولید وچه فناوریهای ادغام شده با حیطه اطلاعات ـ مستلزم تلاشی جهت توسعه طرح اکتشاف اختلالات و بخشهای مختلف آن است .

هدف این طرح ، آماده سازی همه عناصر سازمانی (انسانی ، فنی ، مالی و مواد) برای ارائه واکنش سریع به رویدادها و فراهم سازی امکان تداوم مدل‌های معمول عملیات کسب و کار و روابط آن با تامین کنندگان ، توزیع کنندگان و مشتریان است. به‌هرحال با توجه به اینکه هر کسب وکاری در بعدی موقتی اجرا می‌شود ، این طرح نمی‌تواند موجودیتی مستقل داشته باشد . با توجه به این اصل ، سازمانها بایستی ذهنیتها و نگرشهای خود نسبت به امنیت را جهت ایجاد طرح تداوم مناسبی از کسب و کار مجددا طراحی کنند .

امنیت، برای تداوم کسب و کار

مدیران زمانی که برای اعمال امنیت داراییهای خود تصمیم می‌گیرند ، بایستی با اصول امنیت سیستمی عام شروع کنند و با اقدامات مشترکی که در حفاظت از سیستم‌های ICT به‌کار می‌رود، ادامه دهند . اصول امنیت سیستمی مشخص کننده امنیت فیزیکی و منطقی از یک دیدگاه سطح بالا

ارزیابی ریسک سیستم‌های اطلاعاتی باید برمبنای احتمال رویداد و تاثیر آن بر بهره‌وری سازمان صورت گیرد. در هرچیزی که با IT سروکار دارد، مدیران باید چالشهای مستمر را پذیرا باشند.

بوده و دربردارنده حوزه های وسیعی مانند پاسخگویی ، اثربخشی هزینه و تلفیق است . ضرورت دارد ا مدیران ، حسابرسان داخلی، کاربران و توسعه گران سیستمی بتوانند برخی نگرشهای گرایشی را جهت تقویت درکی وسیع از الزامات امنیتی که اغلب سیستم‌های ICT مجبور به داشتن آن هستند، اتخاذ کنند .

به هر حال مراقبت از اثر بخشی مدیریت امنیت ضروری است. دلیل این امر ، هزینه های بالقوه زیاد ناشی از امنیت غیراثر بخش یا ناکافی است ، برای آنکه برخی داراییها نقشهای مهمی در ایجاد درآمد یا ارائه خدمات بازی می‌کنند . برای نمونه آنها می‌توانند شامل این موارد باشند :

- هزینه تجدید ساخت ، تعمیر یا جایگزینی سیستمهای آسیب دیده.
- سازش یا از دست دادن داراییهای تجاری.
- هزینه اختلالات تجاری به دلیل توقفهای کاری ناخواسته.
- افول کسب و کار به دلیل ازدست دادن اعتماد مشتریان ، دست اندرکاران و شرکا.

صرفه‌جوییهای هزینه ناشی از فرایندهای بهبود کارایی و بهبود مدیریت ریسک می‌تواند ارزش ارزیابی امنیت را دقیقتر سازد . سازمانهایی که قادر به اعمال فناوری امنیتی پیشرفته هستند ، اجرای بهتر و قابل اعتبارتری خواهند داشت . بنابراین ، بررسی امنیت اطلاعاتی به‌طور منظم انجام شده و گزارش بررسی نیز با پیشنهادهای کافی برای بهبود امنیت، آماده می‌شود . این امر منجر به افزایش ارزش برای سازمان ، شرکای آن و نهایتا شبکه های عمومی در مقیاسی بزرگ می‌شود .

نتیجه گیری

فعالیتهای برتری که نیازمند سنجیدگی یکپارچه ، بینشی وسیعتر و مدیریت استراتژیک هستند ، بایستی متهورانه و ریسک پذیر در نظر گرفته شوند . به‌هرحال، در بسیاری از مواقع ، ریسکها دو بعد عمده را ارائه می‌کنند : ۱ - همراهی با پذیرش فناوریهای نوین و ۲ - عدم همراهی‌نکردن با آن که در حالت اخیر فرایندهای قدیمی جهت اجرای کسب و کار به‌کار گرفته می‌شود . این به معنی آن است که برخی مدیران مجبور به تعدیل ذهنیتهای خود و نیز عمق بخشیدن به آن هستند. در واقع اعمال نکردن نوآوری ، مترادف با خود کشی خواهد بود .

اگر مدیران کسب و کارهای کوچک آشکارا نیاز به مدرن سازی سازمانهای خویش را در نیابند ، نه تنها قادر به بهره‌مندی از مزایای بالقوه منابع خود نخواهند بود ، بلکه از ویژگیها و ظرفیتهای منابع انسانی شان نیز سودی نخواهند برد . اخیرا بسیاری از دست اندرکاران سازمانی، ویژگیهای خاصی را در حیطه مربوط به ICT کسب کرده اند و می‌توانند به گشایش مسیرهای سرنوشت ساز جدیدی برای رشد کسب و کار کمک کنند . بایستی در نظر داشت که هر فناوری نوینی با منابع جدیدی از ریسک همراه است . با این حال، ریسک‌ها لزوما دارای اثرات منفی و بدی نیستند . آنها را بایستی با روشهایی مناسب اداره کرد تا دست‌یابی به ارتقای بهره وری و تقویت توان رقابتی سازمان امکان‌پذیر شود .□

منبع:
Alberto carneiro، adopting new technologies، hand book or business strategy، 2006، pp 307-312

قابل توجه علاقه مندان مباحث مدیریتی

ماهنامه تدبیر به منظور دسترسی سریع پژوهشگران، دانشجویان، کارشناسان و اساتید دانشگاهها به مقالات و مطالب شماره های گذشته، کلیه مطالب خود از سال اول انتشار تا پایان سال ۸۲ (جمعاً ۱۴ سال) را طی دو عدد CD به قیمت فقط ۴/۰۰۰ تومان به علاقه مندان عرضه می نماید.

یادآور می شود فهرستگان موضوعی طبقه بندی شده ۱۴ سال مجله تدبیر برای بازیابی سریع مطالب در انتهای هر CD قرار داشته و برای همگان قابل دسترسی است.

نحوه عرضه: متقاضیان برای تهیه و خرید CD تدبیر می توانند به مجله تدبیر، بخش اشتراک مراجعه کنند.

نشانی: تهران - خیابان ولی عصر - بالاتر از پارک ملت - نبش جام جم - سازمان مدیریت صنعتی - دفتر تدبیر

تلفن: ۲۲۰۴۲۰۱۵ - ۲۲۰۴۳۰۰۵ دورنگار: ۲۲۰۴۳۰۰۱