

فصل دوازدهم

چالش های مدیریت سیستم های اطلاعاتی

محمد آزادنیا

azadnia@itrc.ac.ir

09391723415

پاییز 1389

چالش های عام مدیریت سیستم های اطلاعاتی

✱ چالش های عام مدیریت سیستم های اطلاعاتی:

- 1- استفاده مناسب از فناوری ، جهت برآورده ساختن نیازهای اطلاعاتی: سرعت بالای فناوری های نوین ، چالش هایی را برای مدیران ، جهت ارزیابی کیفیت فناوری های موجود جهت برآوردن نیازهای اطلاعاتی ایجاد کرده است و از طرفی ، مهارت های فنی نیز بطور مداوم باید به روز گردد. بکارگیری اثربخش IT به معنی اطمینان از این است که فناوری ، به بهترین نحو ، نیازهای اطلاعاتی مدیران و سازمان را برآورده می سازد.
- 2- اطلاعات خیلی زیاد و متناقض: برای دوری از فزونی اطلاعات ، افراد باید به دقت نیازهای اطلاعاتی خود را مورد ارزیابی قرار دهند و سپس شیوه اثربخش اداره اطلاعات را پیدا کنند.
- 3- تضمین اثربخش بودن هزینه ها: اگرچه اطلاعات ، ارزشمند هستند ولی استفاده از آنها پرهزینه است. بطور کلی ، کسب اطلاعات از طریق منابع غیررسمی و به روش های الکترونیکی ، کاراتر و کم هزینه تر از دیگر شیوه های رسمی است.

چالش های عام مدیریت سیستم های اطلاعاتی

✱ چالش های عام مدیریت سیستم های اطلاعاتی (ادامه):

- 4- تضمین امنیت: مدیران سیستم های اطلاعاتی بایستی نسبت به نصب سیستم های امنیتی پیشرفته که می تواند نفوذ در سیستم ، استفاده غیرمجاز از اطلاعات و ... را کنترل کند ، اقدام نمایند.
- 5- کمبود کارکنان متخصص و کارآمد یا کارکنان دانشی: با پیشرفته تر شدن و پیچیده تر شدن سیستم ها و فناوری های اطلاعاتی ، نیاز به نیروهای متخصص و دانشی ، جهت کار با این فناوری ها روز به روز بیشتر احساس می شود.
- 6- ایجاد تناسب و سازگاری بین فرهنگ سازمان و فناوری های اطلاعاتی جدید: مقاومت کارکنان در بکارگیری موثر سیستم های اطلاعاتی بعلت تفکر کنترل بیشتر و یا از دست دادن شغل ، یکی دیگر از چالشهای مدیران اطلاعات است.

چالش های خاص و اصلی مدیریت سیستم های اطلاعاتی

★ چالش های خاص و اصلی مدیریت سیستم های اطلاعاتی

1- چالش های اخلاقی: امروزه ، سیستم های اطلاعاتی همانند بسیاری از ابزار دیگر ، می توانند بصورت خوب یا بد مورد استفاده قرار گیرند. متأسفانه امروزه اینترنت و دیگر فناوری های پیشرفته اطلاعاتی ، به دلیل استفاده نادرست برخی از افراد ، به ابزاری برای نقض اصول اخلاقی تبدیل شده است. اصول اخلاقی ، مجموعه ای از استانداردهای رفتاری است که از افراد انتظار می رود آنها را رعایت کنند.

چالش های خاص و اصلی مدیریت سیستم های اطلاعاتی

★ چالش های خاص و اصلی مدیریت سیستم های اطلاعاتی (ادامه)

2- چالشهای امنیتی: امنیت بمعنی عدم وجود تهدید و یا عامل تهدید کننده است. امنیت سیستم های اطلاعاتی بمعنی کاهش عوامل تهدید کننده و محافظت از سیستم های اطلاعاتی در برابر دسترسی ، تغییر ، تحریف و انتشار غیرمجاز اطلاعات بوسیله افراد غیرمجاز می باشد. هدف امنیت سیستم های اطلاعاتی بکارگیری مجموعه ای از سیاست ها ، راه کارها ، سخت افزارها و نرم افزارها بمنظور فراهم آوردن محیطی عاری از تهدیدات در تولید ، پالایش و انتقال اطلاعات است.

اصول امنیت اطلاعات

✱ اصول امنیت اطلاعات

- 1- محرمانه بودن: یعنی فقط افراد مجاز حق دسترسی به اطلاعات را داشته باشد.
- 2- صحت و استحکام: یعنی اطلاعات دست نخورده بماند و تغییر در آنها فقط توسط افراد مجاز در صورت لزوم بصورت درست و قابل پیگیری انجام شود.
- 3- در دسترس بودن: یعنی اطلاعات در موقع نیاز بصورت قابل استفاده در دسترس قرار گیرد.

انواع مختلف امنیت سیستم های اطلاعاتی

✱ انواع مختلف امنیت سیستم های اطلاعاتی

- 1- امنیت سایت کامپیوتر: امنیت اتاقها یا مراکزی که منابع سیستم های اطلاعاتی سازمان در آن مستقر است.
- 2- امنیت منابع: امنیت سخت افزار ، نرم افزار ، سیستم ها و پایگاه های داده سازمان
- 3- امنیت شبکه: امنیت شبکه های ارتباطی نظیر اینترنت و اکسترانت
- 4- امنیت خدمات: اطمینان از اینکه خدمات سیستم های اطلاعاتی سازمان ، فقط توسط افراد مجاز قابل استفاده و دسترسی خواهد بود.

پایه های اساسی امنیت سیستم های اطلاعاتی

☀ پایه های اساسی امنیت سیستم های اطلاعاتی:

الف- سیاست ها و دستورالعمل های امنیتی: طرح ها و برنامه های مرتبط با نحوه محافظت از سیستم های اطلاعاتی و داده های آنها در این قسمت مورد توجه قرار می گیرد. راهبرد امنیتی در دو بخش غیرفنی و فنی ارائه می گردد. بخش غیرفنی شامل تعیین سطوح امنیتی و سطوح دسترسی و انتخاب استانداردهای امنیتی مطلوب و بخشی فنی شامل تهیه دستورالعمل های لازم برای بکارگیری و نظارت بر اجرای سیستم امنیتی، جهت نیل به اهداف راهبردی است.

ب- فناوری و محصولات امنیتی: شامل تمام ابزار مورد استفاده در بخش های مختلف امنیتی برای اعمال دستورالعمل ها و کنترل ها

و

نظارت های امنیتی است.

ج- عوامل اجرایی: شامل مدیران سیستم های اطلاعاتی و شبکه های ارتباطی و کارکنان و کاربران عادی این سیستم ها است. این عوامل از فناوری ها و ابزار پیشرفته در جهت اجرای سیاست ها و دستورالعمل های امنیتی استفاده می کنند.

منابع تهدید کننده امنیت سیستم های اطلاعاتی

☀ منابع تهدید کننده امنیت سیستم های اطلاعاتی

- کارکنان
- خطرات ناشی از عوامل طبیعی مانند سیل ، زلزله
- نواقص سیستمی نظیر نقص سخت افزار و نرم افزار
- هکرها یا کلاهبرداران اطلاعاتی
- ویروس های رایانه ای

سطوح پیاده سازی مدیریت امنیت اطلاعات

✱ سطوح پیاده سازی مدیریت امنیت اطلاعات

1- برآورد اولیه امنیت سیستم

الف – سطح اول: پیاده سازی کلی ، فرهنگ سازی و تغییر جو سازمانی

ب- سطح دوم: پیاده سازی جامع تر مدیریت تجاری و کنترل های نهایی

2- مدیریت امنیت سیستم ها و اطلاعات

برآورد اولیه امنیت سیستم

1- برآورد اولیه امنیت سیستم:

در ابتدا باید وضعیت فعلی سازمان از لحاظ امنیت اطلاعات ، سنجیده شود.

الف — سطح اول: بر روی پیاده سازی فرآیندهای مدیریتی و تجاری و نیز بر روی پشتیبانی از فرآیندهای امنیت اطلاعات در سازمان تأکید داشته و شامل فرهنگ سازمانی و آگاهی از مفاهیم کلی امنیت اطلاعات و خط مشی های سازمان است. مقوله هایی که در سطح اول باید اندازه گیری شوند شامل: آگاهی های امنیتی ، فرهنگ امنیتی ، مدیریت ، استانداردها ، فرآیندها و خط مشی هاست.

ب — سطح دوم: در این سطح ، سازمان نیازمند انجام کنترل روندها و کنترل فنی فرآیندهای مدیریتی و تجاری است. در این مرحله ، سازمان می تواند هماهنگی و تطابق خود را با استانداردها بسنجد.

مدیریت امنیت اطلاعات

2- مدیریت امنیت اطلاعات:

بعد از پیاده سازی فرآیندهای مدیریتی و تجاری و نیز پیاده سازی فنی و کامل امنیت ، سازمان می تواند اطمینان یابد که مدیریت امنیت اطلاعات ، بطور کلی پوشش داده شده است. سازمان در این زمان می تواند فرآیند دریافت تأییدیه از يك استاندارد مقبول بین المللی را آغاز کند. عوامل انسانی ، مهم ترین عامل در امنیت بخشیدن به سیستم های اطلاعاتی هستند.

رویکرد مدیریت چهار مرحله ای برای مقابله با چالش های اطلاعاتی

★ رویکرد مدیریت چهار مرحله ای برای مقابله با چالش های اطلاعاتی:

- 1- شناخت: ارزیابی موقعیت تعیین نیازها: یعنی مدیران ، کارکنان و افراد دیگر ، ابتدا باید نیازهای اطلاعاتی خود را با توجه به موقعیتی که در آن قرار گرفته اند ، تعیین کنند. شناخت نیازهای اطلاعاتی می تواند در سطح فردی ، مدیرتی ، سازمان یا جامعه باشد.
- 2- ارزیابی: کاستی های سیستم موجود و ارزیابی نیازهای اطلاعاتی ، یعنی سیستم ها و فناوری های موجود برای اداره اطلاعات ، مقایسه سیستم های موجود با سیستم های قابل دسترسی و جدید و نیز تعیین نیازهای اطلاعاتی که برآورد نشده اند ، باید در این مرحله بررسی شوند.
- 3- طراحی: طراحی سیستم های جدید و یا تغییر سیستم موجود ، این مرحله شامل تصمیم گیری درباره فناوری اطلاعات و ادغام آن با سیستم اطلاعاتی و نیز تجزیه و تحلیل هزینه — منفعت جهت اطمینان از اینکه طراحی جدید ، هزینه ها را کاهش میدهد ، می باشد.
- 4- اجرا: مشخص کردن مسئولیت ها ، نقش ها و منابع اجرای تحقیق

سؤالات؟