چرا اطلاعات دارایی عظیمی است؟

یک پاسخ به این سوال و یک استراتژی برای مدیریت دارایی اطلاعاتی

چکیده

برای هر سازمان؛ اطلاعات دارایی حیاتی است، اما اطلاعات در تعاریف و توضیحات مدیریت دارایی نمی گنجد. این مقاله رشد تکنیک ها و استراتژی هایی برای مدیریت دارایی اطلاعاتی و مسائل و مشکلات مختلف تاثیر گذار بر رشد آن را بررسی می‌کند.

کلمات کلیدی: حاکمیت اطلاعاتی، مدیریت رکوردهای دارایی

مقدمه

برای هر سازمانی اطلاعات یک دارایی تجاری مهم است. هر کاری که انجام می‌دهیم به نوعی شامل استفاده از اطلاعات است. این روند برای پشتیبانی و مطلع شدن از تصمیم گیری های موثر و تسهیل عملیات در حال انجام و ارائه برنامه، محصول و خدمات و به همین ترتیب شواهدی بر فعالیت، عملکرد، حقوق و تعهدات استفاده می‌شود. در عصر افزایش حجم اطلاعات و تحول تعهدات قانونی، یک سازمان برای قفل گشایی ارزش و شناسایی ریسک به دنبال نفوذ بر محتوای اطلاعات است، در این راستا مهم است که داده به خوبی محافظت شود، و به آسانی در دسترس باشد و به صورت مناسبی مدیریت شود.

به هر حال، اطلاعات اغلب در تعاریف مدیریت دارایی ظاهر نمی‌شوند. برای مثال، در ویکی پدیا، تعریفی از "دارایی های ملموس مانند ساختمان و دارایی های ناملموس مانند سرمایه انسانی، مالکیت معنوی، و حسن نیت و دارایی های مالی" با تشریح بیشتر دارایی های زیر ساختی و فیزیکی محسوس برای مثال "ساختارها، تولید، خدمات، برق، آب، ضایعات، و امکانات بازیافت ضایعات، شبکه های توزیع، سیستم های حمل و نقل، ساختمان ها" ارائه شده است (Wikipedia, 2015). با توجه به درک فنی از اهمیت اطلاعات، چرا وقتی به فرآیند مدیریت دارایی رسمی نگاه می‌اندازیم، یک فیل در اتاق می بینیم (یک کار بزرگ)؟

همه چیز در مورد پول

نقل قول خوبی از تحلیل گر گارتنر به نام Doug Laney که مسئله مدیریت دارایی اطلاعاتی را توضیح داد وجود دارد: " اینکه شرکت به ارزش مبلمان اداری خود حس بهتری دارد تا دارایی های اطلاعاتی، ناامید کننده است". یا: آیا ما بیشتر به پرکردن قفسه ها و کامپیوترها اهمیت می‌دهیم تا اطلاعات و چیزهایی که در آن ها هستند؟ شاید به این دلیل است که ارزش اطلاعات را نمی‌دانیم؟

ارزش اطلاعات تجاری بدون شک مانند یک دارایی نامحسوس و حسن نیت است. البته به صورت فزاینده ای کالایی شدن داده و اطلاعات را می‌بینیم، به خصوص با "کلان داده" تولید شده توسط اینترنت اشیا و غیره. Infonomics به عنوان یک مفهوم سریعا در حال رشد است، به ویژه با توجه به کارهای انجام شده گارتنر. شرکت نرم افزاری RSD در حال حاضر مشغول انجام پروژه های Infonomics را با HauteEcole de Gestion deGene`ve (دانشگاه HES-SO علوم کاربردی غربی سوئیس) است.

به هر حال – جدا از هزینه های خرید و نگهداری- در حال حاضر فقدان مدل های ایجاد شده برای اطلاعات برای تعیین سهم درآمد، ارزش بازار، و استهلاک و اثرات بر ترازنامه ها وجود دارد. اما به ما اجازه می‌دهد که امیدوار باشیم. امیدوارم زمانی وجود داشته باشد که بخشی مختص نقش حسابداری اطلاعات وجود داشته باشد. تا آن موقع، این مقاله بر روش های دیگر تضمین بهترین روش های مدیریت اطلاعات تعبیه شده در مبنای شرکت های بزرگ در برخی از راه های ایمن و سالم بحث می‌کند.

تفکر بر تعریف اطلاعات

اگر مدیریت دارایی اطلاعاتی یک فرآیند سیتماتیک از ارزش گذاری، دسته بندی، استقرار، امن سازی، استفاده، نگهداری، سنجش و نظارت و فروش دارایی ها به صورت موثر و کم هزینه باشد، سپس باید دامنه "اطلاعات" را در کسب و کار تجاری فهمید.

واحدهای اطلاعاتی شامل حقایق و دانش ارائه شده در بخش هایی با "محتوای" دیجیتال یا فیزیکی هستند، که در درجه اول در اسناد تجاری وجود دارند. برای تضمین استفاده سازگار از فرآیندها و حاکمیت باید به اطلاعات گذشته، صرف نظر از فرمت یا رسانه آن نگاهی بی اندازیم. بنابراین، باید شامل منابع داده اصلی باشیم که گزارش

های کامپیوتری و دیگر نوع اطلاعات را تولید می‌کنند. بنابراین، دارایی های اطلاعاتی می‌توانند دامنه گسترده ای را پوشش دهند، این دامنه شامل موارد زیر است:

- اشیایی سه بعدی مانند نمونه ای که بخشی از دنباله ممیزی را شکل می‌دهد.
- رکوردهای صوتی و تصویری.
- نوارها و رسانه‌های پشتیبان.
- کتاب‌ها و ژورنال ها.
- نمودار ها، و CAD.
- ایمیل‌ها؛
- صفحه شیشه‌ای؛
- پیام‌های فوری و چت؛
- اسلایدهای شیشه ای؛
- نسخه‌های خطی؛
- نقشه‌ها و طرح‌ها؛
- میکروفیلم/میکروفیش؛
- چاپ؛
- فایل‌های کاغذی؛
- عکس‌ها؛
- پست‌ها و محتوای رسانه‌های اجتماعی؛
- داده ساختاریافته؛
- پیام‌های متنی؛
- داده ساختارنیافته و نیمه ساختاریافته؛
- محتوای وب بر اینترانت، اکتسرانت و وب؛
- بلاگ‌ها و صفحات ویکی.

شما واقعاً به عملکرد شرکت‌های بزرگ نیاز دارید

من دوست دارم که ببینم همه سازمان‌ها، با اندازه مناسب، دارای عملکرد شرکتی خاصی هستند که به مدیریت اطلاعات (دارایی)، پوشش استراتژی، حاکمیت و ارائه سرویس تخصیص داده شده است.

مدیریت اطلاعات باید به صورت ایده آلی یک تابع مرکزی، در برش متقاطعی از سازمان باشد، که هدف آن کنترل و ارائه منابع در راهی مشابه با دیگر عملکردها است که شامل مدیریت دارایی ها، مانند امورمالی، اموال و منابع انسانی است. این تضمین می‌کند که یک هدف؛ نقش و چشم انداز سازگار ارائه می‌شود که با دیگر اهداف کوتاه مدت و بلند مدت استراتژیک و زمینه سازمانی سازگار است.

شما می‌توانید با حذف تکرار نقش ها و افزایش همکاری در سراسر مرزهای بخش‌های سنتی صرفه‌جویی کارآمدی را کسب کنید.

مدیریت مدارک، امنیت اطلاعات، تداوم کسب و کار، و مدیریت داده همه رشته‌هایی با ارتباطات داخلی هستند، که نیازمند هماهنگی برای تضمین محرمانگی، یکپارچگی، دسترس پذیری و در اختیار داشتن داده و محتوا که به صورت سازگاری در طول چرخه عمر خود مدیریت شده، هستند. همه این رشته ها مبنایی برای مدیریت دارایی اطلاعاتی و کاهش ریسک هستند.

عملکرد اصلی کار شبکه تعریف شده از پشتیبان های "محلی" و کارشناسانی است که تضمین می‌کنند فعالیت ها در کارهای "کسب و کار معمولی" گنجانده شده است. به هر حال، حتی یک تیم اصلی قوی و قدرتمند مهم تر است، چرا که به سازمان ها فعالیت های بیشتری سپرده می‌شود و واحدهای تجاری باید پاسخگو باشند، خدمات استراتژی بحرانی، حاکمیت، ریسک و اطمینان را ارائه دهند.

اتصال به پایین

به گفته توماس جفرسون "در سوال از قدرت، اجازه دهید در مورد چیزی بیش از اعتماد به نفس صحبت کنیم، اما قدرت به شرارت ها و شیطنت‌هایی از زنجیره قانون اساسی پیوند خورده است". این کمی بالاتر از بالا است، هنور ساختارهای حاکمیت باید در راستای تضمین اینکه رهبری، جهت دهی، پاسخگویی، پیاده سازی، گزارش دهی و نظارت بر مدیریت اطلاعات برنامه های فعال و بهترین برنامه های پایدار در حال اجرا وجود دارد، قرار داده

شود. چیزهایی که باید برای پیوند مدیریت دارایی اطلاعات و آنچه در آن گنجانده شده است نظارت کنیم در زیر آمده است:

- مدیریت اطلاعات باید به عنوان یک عملکرد شرکتی شناخته شود، و با تعهدات سازمانی نسبت به حاکمیت اطلاعات و مدیریت اطلاعات (برای مثال اهمیت، و ترتیبی، برای تضمین مدیریت مناسب سوابق کلیدی) نشان داده شده در اسناد استراتژیک کلیدی، مانند برنامه شرکتی، همراه باشد.
- مسئولیت های اصلی مدیریت اطلاعات، همانطور که در بالا بحث شد، باید در درون سازمان نسبت داده شود، و یک فرد در سطح بالای مدیریت باید دارایی مسئولیت های استراتژیک کلی باشد. در کمترین حد، حمایت سطح مدیر عامل باید وجود داشته باشد، و با ساختارهای تحویل و گزارش دهی همراه باشد، و نظارت و بررسی موشکافانه را تضمین کند.
- باید یک استراتژی مدیریت اطلاعات وجود داشته باشد، که شامل اهداف خاصی است. اهداف شرکتی برای مدیریت اطلاعات به اهداف کسب و کار پیوند می‌خورند.
- نقش رئیس مدیریت اطلاعات باید به وضوح تعریف شود و برجسته باشد.
- تابع مدیریت اطلاعات، مدیریت شده توسط رئیس مدیریت اطلاعات، باید سطوح لازم حمایت سازمانی را برای اثربخشی آن دریافت کند.
- تابع مدیریت اطلاعات باید به وضوح مسئولیت ها و اهداف و منابعی که باید کسب شود را تعیین کند.
- فرمی از پنل های امنیتی و چالش ها برای ارائه دستگاه های مستقل و متخصص و نظراتی در مورد دامنه و جهت برنامه های مدیریت اطلاعات سازمانی وجود دارد.

کسب و کار معمولی

سیاست مدیریت اطلاعات نقش ها و مسئولیت های رئیس حامی/تابع، مدیریت ارشد، متخصص مدیریت پرونده ها و دیگر اطلاعات، مدیران واحد کسب و کار، کارمندان سیستم فنی و کارمندان را پوشش می‌دهد.

سیاست ها نیازمند چارچوب مرتبطی از استانداردهای حامی، رویه ها و راهنماهای پوشش دهنده همه جنبه های چرخه عمر اطلاعات، صرف نظر از رسانه یا فرمت هستند. اساسا، همه کارمندان مسئول و پاسخگوی حفظ سوابق کامل و دقیق از فعالیت های خود هستند. هرکسی نیازمند مدیر اطلاعات و یک کاربر اطلاعات است. به هر حال،

مسئولیت های کاربردی روزانه برای فرآیندهای مدیریت اطلاعات- شامل حفظ رکوردهای دارایی، کاربر برتر بودن برای بخش سیستم های مدیریت پرونده های و اسناد الکترونیک (EDRM)، تلفیق سوابق مناسب برای آرشیو فیزیکی – می‌تواند به یک پشتیبان مدیریت بخش رکوردها/اطلاعات واگذار شود.

مهم است که نه تنها نقش ها و مسئولیت های اطلاعات تعریف شده است و برای تضمین حفظ رکوردهای موثر به همه سطوح سازمانی نسبت داده شده است بلکه روش ها و سیاست های منابع انسانی (HR) باید از شیوه های خوب پایدار در مدیریت اطلاعات حمایت کنند. این باید به عنوان بخشی از "کار روزانه" دیده شود و کاملا در فرآیندهای برنامه ریزی، نظارت و گزارش دهی در سازمان ادغام شود. پاسخگویی و حسابرسی مدیریت اطلاعات در سازمان باید به ضوح و به صورت رسمی تعریف شود و بخشی از سیستم ارزیابی عملکرد شرکت های بزرگ باشد.

مهارت های خاص و مسئولیت های خاص در رابطه با مدیریت اطلاعات باید شناخته شده باشد، و سازمان باید ارزیابی مهارت های مدیریت اطلاعات را انجام دهد و شکاف های بالقوه را شناسایی کند. روش ها و سیاست های منابع انسانی برای استخدام و حفظ کارمندان خوب و با کیفیت باید شامل تحلیل منظم نیازهای آموزشی مدیریت اطلاعات باشد. نقش‌ها و مسئولیت‌های زیر سطح استراتژیک در رابطه با مدیریت اطلاعات باید به وضوح تعریف و مستند شود و در شرح شغلی گنجانیده شود.

روش ها و سیاست های منابع انسانی باید شامل ایجاد و نگهداری یک الگو؛ مانند چارچوب رقابتی، برای شناسایی مهارت ها و دانش و صلاحیت شرکت های بزرگ مورد نیاز در مدیریت اطلاعات و پرونده ها باشد. رویکرد رقابتی باید شامل مشخصه های شغلی و فردی باشد و مسائل رشد و آموزش را بروز دهد.

شیوه ها و روش های سیاست منابع انسانی شامل بررسی معیارهای انتخاب برای پست ها با وظایف مدیریت اطلاعات برای تضمین صلاحیت فعلی با بهترین روش است. آن ها باید شامل ایجاد یک برنامه رشد حرفه ای برای کارکنان با ثبت وظایف مدیریتی باشند. سازمان باید آموزش هایی را برای تضمین اینکه همه کارمندان دارای مهارت و دانش لازم مرتبط با مدیریت اطلاعات هستند، ارائه دهند. ترتیباتی از شرکت های بزرگ برای تضمین اینکه ارائه آموزش مدیریت اطلاعات به صورت دوره ای ارزیابی می‌شود و برای پاسخ به نیازهای در حال تغییر تطبیق داده می‌شود، باید وجود داشته باشد.

روش ها وشیوه ها باید برای همه کارمندان جدید، برای آگاهی از مسائل و روش های مدیریت اطلاعات شامل برنامه های آموزشی القایی باشند.

هر نقطه ضعف شناخته شده در بررسی های داخلی و خارجی مدیریت اطلاعات باید به صورت درستی در برنامه های آموزشی یا جلسات مختصر بررسی شود. سازمان باید قادر باشد تشریح کند دارای رشد آینده شناخته شده است که ممکن است بر مهارت های کارکنان مدیریت اطلاعات و ظرفیت آن ها تاثیر گذارد و به صورت فعالی آن را مدیریت کند.

باید آموزش برای کارمندان در راستای تضمین آخرین تغییرات در قوانین مدیریت اطلاعات، روش‌ها و راهنماها و سیستم های منتشر شده و عمل به موقع، پیوسته به روز رسانی شود. خاتمه فرآیند باید شامل انتقال دانش به کارمندان "سیستم های" نگهداری سوابق و پرونده‌ها باشد.

ارتباط، ارتباط و ارتباط!

تعهد شرکت به مدیریت اطلاعات باید به وضوح، با کمپین های فعلی ارتباط برقرار کند، پیام های اعلان کارمندان به عنوان مسئول مدیریت اطلاعات را، هم راستا با حاکمیت شرکتی، برای تضمین اینکه همه کارمندان از استراتژی، و مزایا و تعهدات آن آگاه هستند، تقویت کنند.

به ویژه، این از مدیریت (فرهنگی) تغییرات در ارتباط بین نتایج مفید برنامه های خاص حمایت می‌کند.

پیام‌ها و اصول کلیدی:

- چشم انداز (مانند یک رابط برای استراتژی کسب و کار).
- استراتژی تحقق مزایا و منافع کسب و کار برای برنامه های خاص (شناسایی پیوسته، بهینه سازی و ردیابی برای تضمین نتایج حاصل می‌شود، موفقیت چگونه سنجیده می‌شود).
- برنده چابک کسب می شود.
- نقش ها و مسئولیت های (جدید) حامی و مدیر اطلاعات (لذا کارمندان می‌داند از انها چه چیز انتظار می‌رود و چرا انتظار می‌رود).
- استانداردها، رویه ها، سیاست ها، FAQ و راهنماهای حمایت تایید شده، سازمان باید قادر باشد تضمین کند که به صورت فعالانه کارمندان را از هر سیاست و رویه به روزرسانی به موقع مطلع می‌سازد.

- آگاهی از فرآیندهای حمایت کننده (لذا دیده می‌شود که سازمان دارای افراد ماهر در دسترس با مهارت ها و تجربه های مربوطه برای راه اندازی و مدیریت و ارائه برنامه مورد نیاز است).
- تصمیم گیری بر حاکمیت، برنامه یا جلسات هیئت مدیره پروژه.
- بررسی مسائل مربوطه بروز کرده از بررسی آگاهی کارمندان و نظرات با توجه به اصول و روش های حفظ سوابق.
- FAQ می‌تواند شایعات و سوالات را برطرف سازد.
- ارتباطات در زمانی که تغییرات رخ می‌دهند حیاتی هستند.

تفکر بر تاکتیک ها و روش ها

- هر کمپینی باید به یادماندنی باشد و به صورت درستی تکنیک های رسانه ای را ترکیب کند.
- باید مشارکت ذی نفعان و حلقه بازخوردی از مشتریان وجود داشته باشد (اعتماد از اشتراک گذاری و مداخله می‌آید).
- تولید تلفیقی، مستند سازی مراجع، با راهنمای مرجع سریع.
- گردش به روزرسانی ها و یادداشت های خلاصه (خبرنامه های الکترونیکی، ایمیل، تابلوهای آگهی و ابزارهای اجتماعی).
- حفظ عرصه های اختصاصی اینترنت.
- رویکردهای پاسخ به سوالات تعاملی.
- نمایش و تشریح.
- یادگیری الکترونیک در جای ممکن،
- استفاده و نفوذ بر "حامیان" محلی.

ثبت، ثبت، ثبت!

بیان می‌کند که جمع آوری و حفظ ثبت دارایی های اطلاعاتی (IAR) یک مرحله مهم در تضمین این است که اطلاعات درک شده، ارزش گذاری شده، بر آن نفوذ شده و ریسک های آن مدیریت شده است. این می‌تواند رکورد جامعی از همه دارایی های دیجیتالی و فیزیکی شهودی و اطلاعاتی مهم فراهم کند. دارایی ها می‌توانند تشریح

شوند و اطلاعاتی مانند نوع، مالک، محل، فرمت، امنیت، حساسیت، منبع، فعالیت و غیره را مشخص کند، و با واژگان عملکردها و فعالیت های یک الگوی دسته بندی کسب و کار برچسب بخورند، و در نتیجه با سیاست های نگهداری و فروش تنظیم شود.

سازمان شما، شامل مجموعه-C، می‌تواند اطمینان حاصل کند که (۱) درکی از مسائل قانونی و نیازمندی های برای کل چشم انداز اطلاعاتی شرکت و مسئولیت های "وطایف مراقبتی" در محل وجود دارد و (۲) سازمان در راستای کسب بینش و نوآوری بر اطلاعات نفوذ می کند.

تعدادی مزیت و مورد قابل تحویل وجود دارد که یک IAR می‌تواند برای دامنه متفاوتی از ذی نفعان در سازمان آن را ارائه دهد:

مدیریت رکوردها و حاکمیت اطلاعات: یک تشخیص و درک از همه نوع اطلاعات، همراه با مسائل و ریسک ها وجود دارد و به ان معتقد هستند. تراکنش ها و فرآیندهای اطلاعاتی می‌توانند خودکار باشند، شامل ارزیابی ریسک ها، درخواست های دسترسی به اطلاعات (برای مثال آزادی اطلاعات (FOI) و حفاظت از داده)، اقدامات فروش و انتقال. یک IAR می‌تواند برای ایجاد و نگهداری الگوهای دسته بندی و حفظ زمان بندی ها و درک اثرات بر دارایی های هر تغییر آینده در قوانین و مقررات استفاده شود.

امنیت اطلاعات: شناسایی، حفاظت و مدیریت اطلاعات حساس و محرمانه شخصی و تجاری، به ویژه در کمک برای اجتناب از گم شدن داده و نقض داده. می‌تواند به عنوان یک ISO 27001 سیستم موجودی و ثبت دارایی استفاده شود.

تداوم کسب و کار: شناسایی، حفاظت و مدیریت ریسک سوابق "مهم" که برای اجرای یک سازمان بحرانی هستند، و اگر اصل آنها گم شود یا از بین برود نمی‌تواند جایگزین شود، و به صورت جدی کسب و کار را مختل می‌کند و ممکن است سازمان را تحت خطرات مالی و قانونی قرار دهد.

مدیریت فناوری: توانایی برای نگاشت، ارزیابی و مدیریت خطوط کاربردهای تجاری در محل، شامل جنبه هایی مانند استفاده، نسخه برداری، احتمالات، صدور مجوز، بازنشستگی، پلت فرم ها، آرشیو داده، نگهداری و فروش است. این می‌تواند به عنوان ثبت دارایی برای نرم افزارهای سیستمی، تجهیزات کامپیوتری و ارتباطی استفاده شود.

مدیریت تاسیسات و امکانات: شناسایی اسناد و دیگر مجموعه پرونده های فیزیکی، اتخاذ محل آن ها و متریک هایی برای پشتیبانی از برنامه ریزی فضا، حرکت اداری و تغییرات. این می‌تواند به عنوان سیستم مدیریت موجودی داخلی برای سوابقی که توسط امکانات ذخیره سازی آرشیو خارج از محل ارائه شده است استفاده شود؛ اگر تحت کنترل امکانات باشد.

مدیریت بیمه: کمک به درک دامنه و ریسک هایی برای اطلاعات محرمانه برای حمایت از برنامه ریزی برای بیمه سایبری.

ریسک، حسابرسی و تطبیق: ارائه بینشی بر وجود اطلاعات، مالکیت و محل برای توانمندسازی مدیریت فعال ریسک فعال و بررسی ها. این به برآورده سازی تعهدات منظم برای حفظ رکوردها و امنیت اطلاعات و تضمین سیستم های خوب و کنترل ها در محل کمک می کند. همچنین از تضمین حد مدیریت مناسب و ساختارهایی کنترلی برای مدیریت دارایی اطلاعاتی و ریسک ها در محل، که این دارایی ها را خرید و فروش می‌کند، و بر استفاده و عملکرد آن ها نظارت می‌کنند؛ حمایت می‌کند. مدیریت دارایی اطلاعاتی اساسا بخشی از شیوه های خوب مدیریت ریسک عملیات عمومی است.

امور قانونی: در نگاشت چشم انداز اطلاعاتی، یک IAR می‌تواند به هر دو کشف فیزیکی و الکتریکی برای دادخواهی، تحقیق یا دادگاه، و به همین ترتیب تسهیل مسائل اعلان قانونی برای تعلیق فرآیندهای اختیاری کمک کند.

آرشیو تاریخی: استفاده از IAR برای شناسایی اطلاعاتی با ارزش میراثی و رکوردهایی برای انتقال آرشیوهای تاریخی مناسب در یک نقطه مناسب در چرخه عمر.

مدیریت دانش: یک سازمان با عملکرد بالا به صورت سازگاری استفاده از داده و اطلاعات را برای افزایش دانش خود، و در نتیجه ارتقای حکمت و تدبیر و نوآوری بهبود می‌بخشد. IAR می‌تواند به درک کامل دانشمندان اطلاعاتی و تحلیل گران اطلاعاتی از دامنه که سازمان در آن است و فعالیت می‌کند کمک کند. بنابراین، این می‌تواند از بازاریابی، تحقیق و رشد و غیره حمایت کند.

پس یک دارایی چیست (در IAR)؟

چیزی که از دیدن آن خوشحالم این است که بسیاری از سازمان هایی که با آن ها صحبت کرده ام فرآیند ایجاد IAR را خلق کردند یا در آن هستند. رویکردهایی بسیاری برای ایجاد یک رجیستر – صفحه گسترده، دسترسی یا پایگاه داده های قراردادی دیگر، لیست های شیر پوینت، ابزارهای مدیریت دارایی در سیستم ERP؛ سیستم های EDRM و به طور فزاینده ای تعدادی برنامه متخصص وجود دارد. منصفانه است بگوییم که، در بیشتر موارد، در حال حاضر، آن ها در صفحه گسترده ها ایجاد می‌شوند. من فکر می کنم یک رویکرد پایگاه داده ایده آل است، و بر محدودیت هایی که برای تغییرات پروفایل هایی برای انواع فرمت های ترکیبی، تسهیل بررسی یا دنباله فرآیندهای اطلاعاتی مجاز در نظر گرفته نشده اند غلبه می‌کند.

ابتدا، بر دامنه ای از "دارایی" در IAR بحث می‌کنم. آرشیو ملی UK (۲۰۱۵) بیان می‌کند که: "یک دارایی اطلاعاتی یک بخش از اطلاعات است، که به عنوان واحد منحصربفردی تعیین می‌شود و مدیریت می‌شود لذا می‌تواند درک شود، به اشتراک گذاشته شود، حفاظت شود و به صورت موثری بهره برداری شود" و " دارایی های اطلاعاتی دارای ارزش ها، ریسک ها، محتواها و چرخه های عمر قابل تشخیص و قابل مدیریت هستند". این به صورت شیوا بیان شده است و در این مقاله به دنبال اصلاح آن نیستم.

آن ها به صورت مهمی بیان می‌شوند، و در کل موافق هستم که " ارزیابی هر فایل تکی، ورودی پایگاه داده یا قطعه اطلاعات، واقع بینانه نیست. شما باید اطلاعات را در بخش های قابل مدیریتی گروه بندی کنید".

یک دارایی ضرورتا یک گروه هم ریشه از اطلاعاتی است که قوانین و اهداف را به اشتراک می‌گذارد، و هر واحد اطلاعات فیزیکی و دیجیتالی که شما خواهان شناسایی، تعیین مشخصات و مدیریت آن هستید، با ارزش است. این می‌تواند چیز منحصربفرد فوق العاده یا مجموعه ای از چیزها باشد.

بنابراین، برای مثال، ممکن است کارمندان فایل های کاغذی را ترک کند، و اطلاعات دیجیتال و فناوری ارتباطات به به ثبت سیاه های مربوط به یک سال فرد به عنوان دارایی منحصربفرد کمک کند، و به یک روش منحصر بفرد آرشیو شوند. به هر حال، بیمه ها یا دیگر مجوزهای به اندازه پروندهای شخصی مهم هستند، و ممکن است در نوع خود یک دارایی باشند.

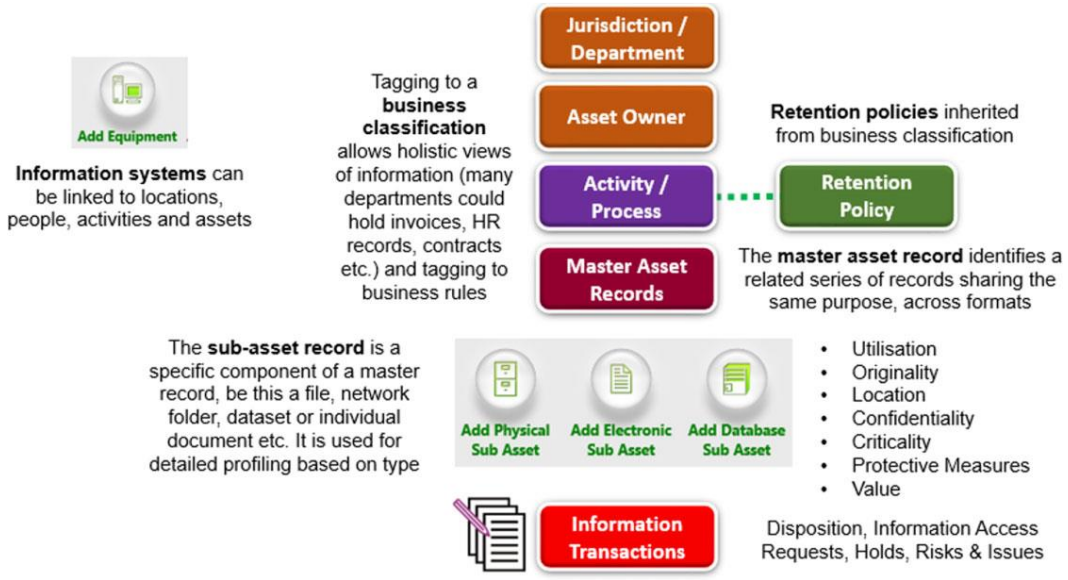
اغلب دارایی به یک مجموعه اشاره می کند. بنابراین، مفهوم دارایی اصلی را با زیردارایی های مرتبط بیان می کنم. یک دارایی مستر سری رکوردهای مربوط به هم هستند که یک هدف را به اشتراک می گذارند و آن را شناسایی و تشریح می‌کند. یک رکورد از دارایی های فرعی، که به دارایی اصلی پیوند خورده است، در جایی که به تعیین دقیق مشخصات نیاز است، برای ردیابی دارایی و پردازش تعیین وضعیت دارایی نیاز است، استفاده می‌شود. بنابراین، برای مثال، اگر رکوردهای حساب های پرداختی دارایی اصلی باشد، رکوردها برای یک سال مشخص باید به عنوان دارایی فرعی در زمانی که آرشیو می‌شود یا از بین می روند، ذخیره شوند. دارایی های فرعی می‌توانند برای انعکاس موجودیت های مختلف در فرمت های متفاوت استفاده شوند و دارایی های اصلی را ایجاد کنند – این ممکن است برای مثال فایل هایی متناظر با اسناد کاغذی، صفحه گسترده ردیابی وضعیت؛ و پایگاه داده مدیریت ارتباطات اصلی باشد. هر یک از این موارد دارای مشخصه های بر اساس فرمت خود هستند، بنابراین سه نوع دارایی فرعی – فیزیکی، دیجیتال و مجموعه داده - داریم. البته برای مثال، تجهیزات، با انواع فیزیکی تخصصی مانند میکروفرم ها و غیره وجود دارند.

مرتبط با این نهاد دیگری وجود دارد – نهاد سیستم اطلاعاتی. یک سیستم واحد؛ در راستای کاربردهای تجاری یا سیستم مدیریت آرشیو/سند/محتوا/رکوردها است، و می‌تواند چندین دارایی فرعی را ذخیره کند.

شکل ۱ معماری نمونه ای را برای یک IAR نشان می‌دهد: در ادامه لیستی از ایده ها و دارایی های کلیدی که یک سازمان ممکن است داشته باشد آورده شده است:

- ممیزی: شامل پروندهای حسابرسی مالی و خارجی.
- پروندهای مربوط به زمین و ساختمان: مانند نقشه ها، طرح ها، ثبت ها، بررسی ها، رسم ها، کارهای پروژه ای، توافق با پیمانکار، اعمال، اجازه ها، خرید و فروش.
- عملکرد تجاری: بهبود تجاری و ثبت عملکرد.
- طرح های تجاری: همه طرح های تجاری، شامل طرح های تحویل محلی.
- ثبت شده در کمیته: دستورکارها، گزارش ها برای هر جلسه کمیته.

- حاکمیت شرکتی و منشیگری شرکت: پرونده‌های مربوط به قوانین، حساب ها، هیئت مدیره و مدیریت سرمایه گذاران تحت قوانین شرکتی، به همین ترتیب دستور استقرار، قوانین کار، ثبت ریسک، دستورالعمل های مالی و سفارشات نیاز است.
- شکایات: شکایات و دیگر مکاتبات با مشتریان کلیدی، شامل سوال، انتقاد و پیشنهادات.



شکل ۱: معماری ثبت دارایی اطلاعاتی

- قراردادها: همه قراردادها، توافقات، زمان بندی ها و تغییرات.
- رکوردهای مربوط به محیط زیست: رکوردهای مدیریت ضایعات و زیست محیط کلیدی.
- رکوردهای تجهیزات: رکوردهای مربوط به همه تجهیزات شامل موجودی، تعیین مشخصات، بازرسی، تست و نگهداری.
- رکوردهای استقرار: مانند ساختارهای سازمانی.
- رکوردهای مالی: مجموعه رکوردهای مالی برای هر سال مالی، شامل حسابرسی مدیریت و مالی.
- رکوردهای بودجه: همه کمک های مالی جمع آوری شده، هدیه های خیریه و رکوردهای بخشش و احسان.
- سلامتی و ایمنی: رکوردهای همه فرآیندهای بهداشتی بالقوه حرفه ای و بازرسی ها.
- علایق گذشته: در کجا ملاحظات فرهنگی و تاریخی را متحمل می‌شوند.

- حوادث: همه "موارد" سانحه ای، در سازمان، برای مثال مربوط به بهداشت و ایمنی، زیست محیط، موارد منطبق یا حاکمیت اطلاعاتی.
- درخواست های دسترسی به اطلاعات: همه درخواست های دسترسی به اطلاعات، تحت مقررات اطلاعات محیطی، FOI و حفاظت از داده قابل اجرا هستند.
- سرویس های داخلی: رکوردهای مربوط به سفارش کار و تحویل سرویس های داخلی، مانند IT و تاسیسات.
- سیستم های IT: مربوط به دامنه و استفاده از همه سیستم های IT مورد اعتماد، شامل اسناد کلیدی مربوط به مالکیت و پشتیبانی.
- موارد حقوقی و دادگاهی: همه موارد حقوقی باز و بسته و سوابق مرتبط و اطلاعات مرجع کلیدی.
- سرانه- مستمری: همه رکوردهای مربوط به الگوهای مستمری/ حقوق بازنشستگی.
- سیاست ها و رویه ها: همه سیاست ها، استانداردها، ابزارها و روش ها.
- تدارکات و تامین کننده ها: همه رکوردهای مربوطه به مناقصه ها، مدیریت تدارکات، ارزیابی عرضه کننده و فروشگاه ها.
- رکوردهای پروژه و برنامه: همه رکوردهای پروژه ها و برنامه ها، خواه یک شرکت بزرگ باشد یا بخشی از آن.
- اتشارات: همه انتشارات تولید شده و استفاده شده توسط سازمان ها.
- رکوردهای موجودی: همه شاخص های مدیریت رکوردها، لیست های رجیستری، الگوهای انتشار، و به همین ترتیب رکوردهای مستندسازی آرشیو، انتقال و تخریب.
- گزارش ها: همه گزارش های کلیدی، شامل بازده های آماری، تولید شده توسط سازمان یا برای سازمان.
- پژوهش و توسعه: همه رکوردهای مربوط به فعالیت های پژوهشی و رشد.
- توسعه خدمات: همه رکوردهای توسعه خدمات، شامل موارد مربوط به راه اندازی خدمات خارجی/برون سپاری.
- کارکنان فعلی و کارکنانی که سازمان را ترک کرده اند: رکوردهایی از همه کارمندان و کارکنان، شامل HR شرکت های بزرگ و رکوردهای کارمندان گروهی و داوطلبان.

- رخدادهای آموزشی: همه رکوردهای رخداد و مطالب آموزشی.
- حمل و نقل: همه رکوردهای مدیریت ناوگان، شامل مجوزهای عملیاتی، نگهداری وسایل نقلیه و لاگ های مربوط به رانندگان.
- محتوای وب: همه رسانه های اجتماعی و وب، شامل محتوایی که آرشیو شده است.
- ردیابی کار: همه پایگاه داده ها و صفحه گسترده هایی که نمونه های موردی و کارها را ثبت می‌کنند.

نگاه مختصری به دسته بندی داده

روش های بسیاری برای دسته بندی دارایی یا دارایی های فرعی وجود دارد. اساسا، این در مورد تعامل با لیستی از ذی نفعان در مدیریت دارایی های اطلاعاتی است که در بالا شناخته شده، و نیازمندی ها و اهداف آن ها درک شده است، بنابراین به تعیین آنچه باید حسابرسی شود و شناسایی شود منجر می‌شود.

سه ناحیه کلیدی را پوشش می‌دهد: امنیت، بقا و تداوم کسب و کار.

دسته بندی امنیت

به عنوان بخشی از فرآیند مدیریت ریسک، یک هدف اصلی تضمین این است که سنجش های فعالانه مناسبی برای اطلاعات حساس تجاری و محرمانه صورت می گیرد. اطلاعات مناسب قوانین و روش ها را هندل می‌کنند و سپس می‌توانند آن ها را به دارایی ها اعمال کنند.

در سال ۲۰۱۴ در UK، سیستم دسته بندی جدید؛ سیاست دسته بندی امنیت دولتی، با الگوی قدیمی برچسب گذاری دولت های حفاظتی جایگزین شد. به صورت خلاصه، این استاندارد به این شرح است:

- فوق سری: اطلاعاتی که به عنوان فوق سری برچسب می خورند به معنی این است که هرکس که باعث نشر این اطلاعات شود، باعث می‌شود زندگی خود را از دست دهد، یا حوادث دیپلماتیک رخ دهد یا به شدت بر عملیات اطلاعاتی تاثیر می گذارد. افشای همچین اطلاعاتی فرض می‌شود بالاتر از آستانه قوانین مربوط به پیگرد قانونی قانون اساسی رسمی است.
- سری: این برای اطلاعاتی استفاده می‌شود که نیاز است در برابر تهدیدات جدی حفاظت شود و می‌تواند در صورت به خطر افتادن باعث آسیب جدی شود – مانند تهدید برای زندگی، به خطر انداختن بررسی جرم و جنایت یا آسیب به روابط داخلی.

- رسمی: همه روتین های کسب و کار بخش عمومی، عملیات و سرویس ها رسمی گفته می‌شوند. یک زیرمجموعه محدوده شده از اطلاعات رسمی (برای افراد، سازمان یا دولت در کل است) اگر گم شود، دزدیده شود، یا در رسانه های دسته بندی شده به عنوان رسمی و حساس منتشر شود، دارای پیامدهای آسیب پذیری بسیار است.

برای سازمان هایی که دارای طرح موجود یا اجباری نیستند، مانند بالا، مثالی به شرح زیر آورده شده:

- محدود شده: اطلاعاتی که، اگر برای افراد غیرمجاز افشا شود، می‌تواند بر تعهدات قانونی یا نظارت سازمانی یا وضعیت مالی، مشتریان، یا فرانشیزها تاثیر شدیدی گذارد و نیاز است که بر مبنای " نیازبه دانستن" مدیریت شود.
- محرمانگی: اطلاعاتی در مورد مشتریان، کارمندان یا کسب و کار شرکت یا متعلق به آن ها که یک سازمان متعهد است از آن حفاظت کند، برای مثال، سیاست ها و مقررات داخلی.
- داخلی: اطلاعاتی که معمولا در یک سازمان به اشتراک گذاشته می‌شوند معمولا نباید به بیرون نشر داده شوند و به عنوان یک مورد محدود یا محرمانه دسته بندی می‌شود.
- عمومی: اطلاعاتی که آزادانه خارج از سازمان در دسترس هستند و هدف آن استفاده توسط عموم است.

طبقه بندی حساسیت:

به طور مشابه، برای تداوم کسب و کار و بازیابی فجایاع شناسایی و حفاظت مناسب از هر فایلی، و فولدر الکترونیکی، مجموعه داده یا سند خاص شامل اطلاعات لازم برای یک سازمان مهم است، اگر فایل اصلی گم شود یا از بین رود و نتواند جایگزین شود، کسب و کار را جدا مختل می‌کند، و ممکن است سازمان را در معرض مشکلات حقوقی و مالی قرار دهد یا حقوق شهروندان را به خطر اندازد.

یک مثال از طرح دسته بندی برای دارایی های حساس اطلاعاتی در زیر نشان داده شده است:

- حیاتی: رکوردهای بحرانی مانند عملیات قانونی نمی‌توانند بدون فرم اصلی ادامه یابند.
- ضروری: رکوردهایی که در عملیات روزانه استفاده شده اند اما می‌توانند جایگزین شوند یا اطلاعات آن‌ها بازیابی شوند یا مجددا ایجاد شوند.

- غیر ضروری: همه رکوردهای دیگر که شامل موارد منتشر شده ای هستند که به صورت کلی برای کپی مرجع یا کپی های تکراری مختلف و یا کپی های معمولی رکوردها استفاده می‌شوند.

نگهدارای و فروش

اگر سازمان دارای برنامه حفظ رکورد و سوابق تایید شده شرکت باشد، سپس می‌تواند در یک IAR ثبت شود، به الگوی دسته بندی تجاری نگاشت شود و در هنگام اضافه شدن توسط دارایی های اضافی ارث برده شود.

اگر این طور نباشد، هرگز سریعا موردی را ایجاد نمی‌کند که تضمین کند که اطلاعات برای حداقل دوره زمانی لازم حفظ می شود، اطلاعات شخصی محرمانه به مدت طولانی حفظ نمی‌شوند و این به نوبه خود فروش دفاعی است.

این مقاله بر چگونگی ایجاد برنامه حفظ رکوردها، از جمله تخصیص دوره زمانی و تاریخ راه اندازی رخدادها متمرکز نمی‌شود، به هر حال، برخی از ملاحظات کلیدی یا اصلی در تعیین دوره نگهداری در زیر داده شده است:

اصولی برای تعیین مدت زمان دوره‌های نگهداری:

- قانونی: دوره نگهداری خاص با قوانین یا مقرراتی برای نوع رکورد خاص تنظیم می‌شود.
- شواهد حقوقی: رکوردها برای پشتیبانی و شواهد قراردادهای مربوطه یا حقوق و تعهدات قانونی قابل اجرا نگهداری می‌شوند، شامل دوره های محدود برای اقدامات قانونی و تقویتی.
- پاسخگویی مالی: رکوردهای مستند فعالیت های مالی که نیاز است ممیزی و نیازمندی های مالیاتی را برآورده سازند یا تصویر مالی دقیقی را در طول زمان حفظ کنند.
- مقررات داخلی: رکوردهایی برای برآورده سازی اهداف ممیزی داخلی و یا اجرای سیاست شرکت نگهداری می‌شوند.
- نیازهای تجاری: مقدار رکورد تجاری که برای پشتیبانی از عملکرد فعلی یا کارهای آینده، از جمله ارزش پژوهشی یا اطلاعات بلند مدت نیاز است.
- میراث: در کجا ملاحظات فرهنگی و یا تاریخی وجود دارد.
- حفاظت از داده: داده های شخصی پردازش شده برای هر هدفی یا اهدافی نباید طولانی تر مدت لازم برای آن هدف، نگهداری شوند.

نتیجه گیری با یک جمله

اگر شناسایی سطح C، صریح باشد، دیگر نیازی به فیلی در اتاق نیست، در عوض می‌تواند یک ببر اقتصادی یا دگرگون شده برای هر سازمانی باشد.

اعلان منافع متضاد

نویسندگان هیچ تضاد مناقع بالقوه ای را با توجه به پژوهش، مالکیت و یا انتشار این مقاله بیان نکرده است.

بودجه‌ها

نویسندگان هیچ پشتیبان مالی برای پژوهش، نویسندگی و یا انتشار این مقاله دریافت نکرده است.