إدارة المخاطر ودور نظم المعلومات

تولي معظم المؤسسات الكبرى في مختلف أنواعها المالية والإدارية والصناعية أهمية كبرى لما يعرف بفن إدارة المخاطر أو علم إدارة المخاطر.

إن الخطر هو توليفة (Combination) بين إحتمالية حدث وعواقب هذا الحدث أو هو كما تعرفه مجموعة (Gartner Group) إحتمالية الخسارة أو التعرض للخسارة " The possibility of loss or exposure to loss" .

يعتبر البعض أن إدارة المخاطر فن بحد ذاته لأنه يعتمد على إختيار النماذج المناسبة وتطبيقها على وحدات المؤسسة للتنبؤ بمدى تأثير الخطر على الزمن والتكاليف، بينما يعتبرها البعض الآخر علم من علوم إدارة المشروعات لأنها تعتمد على القياس والحساب والتحليل.

وسواء أكانت فنا أو علما فإن إدارة المخاطر تمثل محورا أساسيا للإدارة الاستراتيجية للمؤسسة لذا فهي بلا شك يجب أن تكون على قائمة الأولويات لكل مؤسسة، إذ أن الكوارث المالية الضخمة التي تعرضت لها بعض الشركات الكبرى والتي أدت في نهاية المطاف إلى إنهيارها، كان بسب فقدان الرؤيا المستقبلية وعدم تطبيق فن إدارة المخاطر.

لقد كانت إدارة مخاطر المشاريع في السابق تعمل بطرق بدائية وتدار بوسائل عشوائية غير نموذجية أي دون الرجوع أو التعاون مع الوحدات التنظيمية الأخرى بالمؤسسة، والأسوء من ذلك إنها لم تكن لها الأولوية في الأهمية أي كانت تعتبر موضوعا جانبيا لا مبدأ رئيسيا تقوم عليه كل العمليات والإجراءات التي تتطلب إتخاذ القرارات، وغالبا ما يصعب إحتواء هذه المخاطر حيث إنها متصلة ببعضها بطريقة معقدة تجعل السيطرة عليها وإدارتها من الصعوبة بمكان.

على الرغم من الاهتمام المتزايد بإدارة المخاطر فإن الوضع الحالي لا يزال غير فعال نسبيا ويرجع السبب في ذلك إلى أن إدارة المخاطر في كثير من المؤسسات تتم بصورة منفصلة لكل وحدة تنظيمية وفقا لإحتياجات وأولويات تلك الوحدة. وتفتقر تلك المؤسسات إلى نظرة شمولية ومركزية لهذه الجهود المنفصلة مما يؤدي إلى فقدان النمذجة أو الجهود الموحدة الخاصة بالمؤسسة، بمعنى آخر لا توجد أطر عمل موحدة تلزم جميع وحدات العمل التنظيمية قي تلك المؤسسة بالالتزام بها مما يؤدي في نهاية المطاف إلى حلول متخبطة، لذلك يجب ان توضع لوائح وأولويات إدارة المخاطر على مستوى المؤسسة وليس على مستوى وحدات العمل وذلك عن طريق إيجاد إطار عمل مشترك يتم إتباعه أو تبنيه من قبل جميع وحدات العمل التنظيمية في المؤسسة حيث يتم إيصال المعلومات وإستخدام نماذج وتقنيات موحدة للتعامل مع الأزمات.

من المعروف أن عالمنا اليوم أصبح أكثر إنفتاحا عما قبل، فسهولة الحصول على المعلومات عن طريق شبكة الانترنت والسرعة الهائلة في التغيرات التقنية والإقتصادية والتوسع الجغرافي لكثير من المؤسسات تعني أن المخاطر الإدارية في إزدياد متنامي ويجب ان تؤخذ بعين

الإعتبار، لذلك فإن العولمة "Globalization" تفرض على المؤسسات بأن تعالج المخاطر الإدارية على أسس وقواعد عالمية.

إن عناصر إدارة المخاطر المشاريع (Enterprise Risk Management) عديدة ومن أهمها هو ما يتعلق بسلامة نظم المعلومات (IT Security Risk) وهذا العنصر يتطلب بدوره التوفير الدائم لأحدث متطلبات نظم المعلومات من أجهزة وبرامج وشبكات لنقل المعلومات بين أفرع المؤسسة.

إن المخاطر كما عرفنا سابقا هي الأحداث غير المتوقعة والتي قد تؤثر سلبا على أداء المؤسسة بطريقة ملموسة وتحول دون تحقيق الأهداف، وهذه المخاطر إما ان تكون مخاطر داخلية أو مخاطر خارجية أو من الإثنان معا ومن أهم أنواعها :-

أ- مخاطر طبيعية مثل : الزلازل والفيضانات والحرائق
ب- مخاطر مالية مثل : التضخم وتذبذب الأسعار والمديونيات

ج- مخاطر إستراتيجية مثل : تقليل رأس المال والأوضاع السياسية غير المستقرة

د- مخاطر تشغيلية مثل : الأعمال اليومية في المؤسسة وإمكانيات القدرات التكنلوجية والعمليات التجارية

هـ - مخاطر الموظفين مثل : عدم توفر العمالة المدربة أو الكفؤة ونقص الخبرة العملية للموظف وعدم التفاني والإخلاص في العمل من قبل البعض أو قبول الرشاوي لدى بعض الموظفين

و- مخاطر التقنية مثل : القصور في نظم الأمن والسلامة أو إنشغال الموظقين بإرسال الرسائل القصيرة أو تبادل رسائل البريد الإلكتروني الشخصية أثناء العمل أو تصفح الإنترنت

إن كل هذه الأنواع من المخاطر ذات أهمية بالغة ويجب أن تؤخذ بعين الإعتبار وإن إهمال أيا منها قد يؤدي إلى كوارث قد تسبب في إنهيار المؤسسة.

هناك أربع طرق رئيسية للتعامل ولإدارة هذه المخاطر وهي تجنب الخطر (Avoid) أو نقل الخطر (Transfer) او تسكين الخطر (Mitigate) او قبول الخطر (Accept).

أما خطة عمل إدارة المخاطر فيجب أن تكون تحت رئاسة سلطة مركزية أو قائد او مدير تنفيذي وتنقسم الخطة إلى ثلاث مراحل يتم من خلالها ما يلي :-

1- تحديد مستوى الخطر (منخفض – متوسط – عال)
2- وضع خطوط إرشادية يتبعها جميع العاملين في الشركة لمواجهة الخطر
3- ربط مستوى الخطر بعد تحديده بمستوى الخطورة للإدارة العليا.

إن الخطط هي أي فكرة يمكن ان تقلل من إحتمالية الخطر كحلول تقنية أو إجراءات تحسينية أو الإثنان معا، لذا يجب تحديد وتصميم خطة المسؤلية (Responsibility) والتي توضح كيفية التعامل مع كل خطر، ففي بعض الأحيان يتم قبول الخطر كما هو بدون خطة عمل لإزالته، وفي أغلب الأحيان يجب تصميم خطة تسكين للخطر(Mitigation) توضح كيف يمكن تقليل الخطر إلى أدنى مستوياته وعمل تحليل أو دراسة تكاليف إذ احيانا تكون التكاليف الخاصة بخطة التسكين أعلى من الخطر نفسه.

كذلك يجب مراقبة وملاحظة نجاح أو فشل خطة إدارة المخاطر في المؤسسة بإستمرار ومدى فعالية هذه الخطة، بعد ذلك يجب تجميع هذه المعلومات على مستوى المؤسسة لتعديل الخطة والتحكم بالأنشطة المتعلقة بإدارة الأزمات، حيث يجب أن تكون إدارة الأزمات جزء لا يتجزا من عمل كل فرد بالمؤسسة .

إن الهدف من إدارة المخاطر هو إعطاء قيمة متاحة أكبر لجميع أنشطة المؤسسة ترفع من إحتمالية النجاح وتخفض من درجة الفشل في تحقيق الأهداف الكلية للمؤسسة عن طريق :

1- تحسين طرق إتخاذ القرار وسبل التخطيط
2- التوجية الأمثل لإستخدام روؤس الأموال ومواردها
3- تزويد المؤسسة بخطة عمل تمكنها مستقبليا من دعم اهدافها
4- إستخدام الكفاءة التشغيلية القصوى للمؤسسة

عوامل نجاح برنامج إدارة المخاطر

1- أن تتبنى المؤسسة خطة عمل شاملة وواحدة للشركة أي ان يكون لكل وحدة تنظيمية خطة عمل خاصة بها وترتبط جميع هذه الخطط بالنهاية بالخطة الرئيسية الشاملة للمؤسسة، ولكي يسهل إدارتها ورقابتها يجب ان تدار هذه الخطة وتراقب من قبل مدير تنفيذي.
2- أن تتم مراقبة خطط العمل على فترات ثابتة ومحددة إما بشهر إذا كان مستوى الخطر عال أو كل ثلاثة اشهر إذا كان مستوى الخطر متوسط أو كل ستة أشهر إذا كان مستوى الخطر منخفض أو فترات أخرى حسب ما تراه المؤسسة مناسبا لها.
3- يجب أن تكون أهداف وإستراتيجيات إدارة المخاطر واضحة ومحددة ومن صميم عمل كل موظف بالمؤسسة Everyone's Job

إنه لمن الطبيعي أن يكون هدف كل مؤسسة هو أن تصل بمستوى الخطر الذي يحدق بها إلى حد المستوى المقبول (Acceptable level) لأن الوصول إلى مستوى اللاخطر (Risk Free) يكاد يكون مستحيلا، ويعتمد قبول المؤسسة على مستوى معين من الخطر على مدى قوة الحدث وتأثيرة المحتمل على أداء المؤسسة ومدى قوة الخطر وتأثيرة المحتمل على أداء المؤسسة.

إن أي برنامج شامل لإدارة المخاطر يجب أن يصمم ويتعامل مع جميع انواع المخاطر التي قد تتعرض لها المؤسسة، ومن اهم هذه المخاطر هو أمن نظم المعلومات منها على سبيل المثال خطر مخترقوا أمن الشبكات (Hackers) وخطر دخول أشخاص غير مخولين على نظم

وتطبيقات المؤسسة وهذه الأمثلة تتطلب خطة تسكين قوية لجعل هذه المخاطر في أدنى مستوياتها.

إن من أهم المستويات المناطة بإدارة نظم المعلومات في أي مؤسسة هي حماية وصيانة المصادر الرقمية التابعة للمؤسسة فمخاطر الدخول غير المشروع أو غير المسموح لا يمكن قبوله إطلاقا ، لذا فمن الضروري وجود بنية تحتية قوية للتحكم في الدخول لنظم وتطبيقات الشركة. فعندما يكبر حجم عمل المؤسسة بإفتتاح أفرع جديدة ودخول شركاء وعملاء جدد للمؤسسة فهذا يعني حاجة هؤلاء للدخول المباشر (On Line) على خدمات وتطبيقات المؤسسة وهنا يتبين مدى كفاءة إدارة نظم المعلومات في صيانة وحماية خصوصية معلومات المؤسسة إذ أن المعلومات الخاصة بالشركة يجب أن تحمى حماية بأقصى درجات الحماية وأن تخلق سياسات مركزية تحدد من خلالها صلاحية كل موظف بالمؤسسة من إدخال البيانات او مشاهدة المعلومات فقط أو طباعة المعلومات أو تعديلها أو الصلاحية الشاملة، فليست الحماية القوية لموقع المؤسسة على الإنترنت هي المطلوبة فحسب بل إن إستخدام الخدمات الالكترونية ضمن موقع المؤسسة على الإنترنت هو الأهم في الحماية اما بالنسبة لملفات المؤسسة وقواعد البيانات فتتم وقايتها بحماية كلمة السر وطرق ربط قواعد البيانات فيما بينها، وكذلك يجب حماية ملفات النظام من الدخول غير المصرح به، وتعتمد قوة هذه الحماية على قوة البنية التحتية الإدارية المشرفة على إدارة نظم المعلومات والتي يجب أن تكون لديها سياسات مركزية واضحة عن طبيعة عمل كل موظفي المؤسسة والوحدة التنظيمية التي يتبعونها، ففي إدارة نظم المعلومات في اي مؤسسة غالبا ما يكون هناك مستويات إدارية متعددة من مدير إدارة إلى نائب مدير وإختصاصي نظم تطبيقية ومحلل نظم وغير ذلك وغالبا ما يكون للمدير ونائبه صلاحية الدخول على كل النظام وهو ما يعرف بالمستخدم السوبر (Super User) وهذا من الخطأ الفادح الذي تقع فيه بعض المؤسسات، إذ أن الطريقة المثلى هي إحتفاظ المدير فقط أو نائبه فقط – وليس الإثنان معا – بكلمة السر الوحيدة التي تسمح بالدخول على جميع التطبيقات وذلك حتى تنحصر المسئولية بفرد واحد وبالتالي نتجنب الصعوبات والمشاكل التي قد تنتج من إستخدام الإثنان معا لنفس رمز المستخدم وكلمة السر.

ومن الأمور الأخرى التي يجب أن لا تغيب عن إدارة نظم المعلومات عند إدارة مخاطرها هي مسالة ترك الموظف العمل في المؤسسة، إذ يجب على إدارة نظم المعلومات إلغاء أو إيقاف صلاحية دخول الموظف للنظام فورا وإلا حدث خطرا كبيرا وخصوصا إذا كان الموظف مقال من وظيفته، وهذا يعني ان إدارة شئون الموظفين مطالبة بإشعار إدارة نظم المعلومات بإقالة الموظف من المؤسسة قبل إعلان الموظف المعني بالإقالة.

كذلك في حالة إنتقال موظف من وحدة تنظيمية إلى أخرى في نفس المؤسسة، يصبح أحيانا للموظف رمزين للإستخدام وهذا أيضا يمثل خطرا على عمل المؤسسة، لذا يجب على إدارة نظم المعلومات التأكد من فترات إستخدام الموظفين لرموزهم الآلية وإلغاء رمز الموظف الذي لم يدخل على النظام مدة تزيد عن شهر أو شهرين او حسب الفترة التي تقررها المؤسسة . وهناك خطرا آخر وهو معاناة بعض المؤسسات من وجود موظفين لديهم الصلاحية لدخول تطبيقات هم ليسوا بحاجة إليها في عملهم، وهذا الخطر لا يندرج تحت تصنيف الخطر المقبول بل هو خطر يجب التخلص منه .

وأخيرا، فإن هناك العديد من البرامج والتطبيقات الجاهزة للإستخدام في مجال إدارة المخاطر منها على سبيل المثال لا الحصر :-

eTrust Site Minder – eTrust Transaction Minder – eTrust Access Control – eTrust Security Command Center – eTrust Audit – eTrust Antivirus

المصدر :

IT Security Risk Management (March 2007) – By Sumner Blount – Computer Associates International.

عبداللطيف حمد السالم

الجهاز المركزي لتكنولوجيا المعلومات