إدارة مخاطروأمن المعلومات في ظل ثورة نظم وتكنولوجيا المعلومات

مدوكي يوسف
أستاذ مساعد
جامعة محمد خيضر – بسكرة
medouki.youcef@yahoo.fr

الملخص:
نظرا للأهمية الكبرى التي يحض بها مورد المعلومات، التي تمثل أساس اتخاذ القرارات في المؤسسة وفي جميع مستوياتها الإدارية (الاستراتيجية، الإدارية والتكتيكية)، وبالرغم من التطور الهائل في وسائل وتكنولوجيا المعلومات حاليا والتي خلقت فرصة كبيرة للمؤسسات لجمع المعلومات والاستفادة منها ومن سرعة الحصول عليها بالدقة المطلوبة وفي الوقت المناسب ومعالجتها وتخزينها بالشكل الذي لم يكن متاحا له بهذا الكم والنوع من قبل، إلا أنه في نفس الوقت فتح هذا التطور المجال أيضا لتعرض هذا المورد الهام لأخطار وتهديدات، تحول بينه وبين الاستفادة منه في اتخاذ القرارات السليمة والتي من شأنها تعرض المؤسسة في حد ذاتها لمخاطر قد تؤدي بها إلى الزوال، وعلى هذا الأساس جاءت هذه الورقة البحثية لتبيان منهجية إدارة مخاطر المعلومات وأمنها.

Résumé :
Au vu de la grande importance dont bénéficie l'information, qui représente la base de la prise de décisions au sein d'une entreprise et ce, à tous ses niveaux administratifs (stratégiques, administratifs et tactiques), en dépit du développement considérable dans les médias et technologies de l'information de nos jours, ce qui a permis de créer une excellente occasion pour les entreprises afin de recueillir les informations, de les utiliser et de les obtenir rapidement et avec la précision requise et en temps opportun, les traiter et stocker d'une façon qui ne leur était pas octroyée auparavant en pareilles quantité et qualité. Mais en même temps, ce développement a également exposé cette ressource à plusieurs risques et menaces, se posant entre elle et le fait de pouvoir en profiter afin de prendre les bonnes décisions qui peuvent exposer l'entreprise en elle-même à des risques pouvant mener à sa disparition.

مقدمة:

نتيجة لزيادة حجم المؤسسة، درجة تعقدها وتخصصها، وكذا التعقد التكنولوجي للمجتمعات وزيادة ندرة بعض الموارد الطبيعية، حتم على المجتمعات عامة والمؤسسات خاصة أن تنتقل وتركز وتزيد اهتماماتها في الحصول على مورد آخر يتمثل في المعلومات، فتعتبر هذه الأخيرة الركيزة الأساسية لصنع واتخاذ القرار سواء على المستوى الكلي لرسم سياسات التنمية المختلفة، أو على المستوى الجزئي لرسم استراتيجيات المؤسسة. فلقد أصبح المستثمرون ومدراء المال والأعمال يعتمدون بشكل أساسي على المعلومات في إدارة أعمالهم واستثماراتهم على اختلاف أنواعها، حتى أن كثيراً من المسيرين عملوا على إعادة هيكلة أعمالهم ومؤسساتهم الاقتصادية لتتكيف مع التطورات السريعة في مجال تكنولوجيا المعلومات والاتصالات، لتحقيق الميزة التنافسية. ولهذا، ولما للمعلومات والتقنيات المرتبطة بها من أهمية كبرى في إدارة المشاريع ودعم الأعمال والأهداف الإستراتيجية للمؤسسات، فقد أصبح من الضروري التعرف على المخاطر التي تتهدد هذه المعلومات وهذه التقنيات، وكيفية التعامل مع هذه المخاطر وإدارتها بالقدر الذي يقلل من الآثار السلبية الناجمة عنها إلى الحد الأدنى، مما يزيد من كفاءة وفاعلية هذه التقنيات في أداء المهام المنوطة بها. وعلى ذلك، جاءت هذه المقالة بهدف التعرف على كل ما يتعلق بإدارة مخاطر وأمن المعلومات في ظل ثورة نظم وتكنولوجيا المعلومات، وللتوصل إلى ذلك ارتاينا التطرق في هذه الورقة البحثية إلى المحاور التالية:

- **أولا:** مفاهيم عامة حول المعلومات ونظم إدارتها.
- **ثانيا:** أمن المعلومات وأهم المخاطر التي تتعرض لها.
- **ثالثا:** منهجية إدارة مخاطر المعلومات وأمنها.

أولا: مفاهيم عامة حول المعلومات ونظم إدارتها

1- تعريف البيانات:

كلمة "بيانات" مشتقة من كلمة "بيّن" وهي "البيان"، أي ما يتبيَّن به الشيء من الدلالة.[1] وتسمى أيضا المعطيات، وهي المادة الأولية التي تستخلص منها المعلومات، وبتعبير آخر هي عبارة عن أرقام وحقائق ليس لها معنى إلا بعد إجراء عملية المعالجة عليها والاستفادة منها.[2]

وتعرف أيضا بأنها: "عبارة عن أرقام أو كميات رقمية تستخرج (تشتق) من الملاحظة أو التجربة أو الحساب.[3]

إذن فالبيانات خامة بطبيعتها تشتمل على مفاهيم لغوية أو رياضية أو رمزية، خالية من أي معنى، أو متفق عليها لتمثيل الأشخاص، الأشياء، أو الأحداث، ويتم تشغيلها أو معالجتها لتصبح ذات دلالة ومعنى وتتحول إلى معلومة.

2- تعريف المعلومات:

إن مصطلح المعلومات (Information) المأخوذ من أصل الكلمة اللاتينية "Informar" والذي يشير إلى إعطاء شكل أو حالة (Forme).[4] أي أن المعلومة تعطي الوصف لهيئة وحالة أو شكل حدث ما أو شيء ما.

"وهي عبارة عن بيانات تم تصنيفها وتنظيمها بشكل يسمح باستخدامها والاستفادة منها".[5] كما تعرف على أنها "البيانات التي تم إعدادها لتصبح في شكل أكثر نفعا للفرد الذي يستقبلها، والتي لها إما قيمة مدركة في الاستخدام الحالي أو المتوقع أو في القرارات التي يتم اتخاذها".[6]

وهناك تعاريف أخرى أن: " المعلومة هي الخبر الذي ينمي معرفتنا حول موضوع ما ".[7]

إذن فالمعلومات هي ناتج معالجة البيانات، تحليلا أو تركيبا، وذلك لاستخلاص ما تتضمنه وما تشير إليه هذه المعطيات، من مؤشرات وعلاقات وكليات وموازنات ومعادلات وغيرها، وذلك من خلال تطبيق العمليات الحسابية والطرق الإحصائية والرياضية والمنطقية، أو من خلال إقامة النماذج وما شابه، وكذلك تؤدي المعلومات إلى تغيير سلوك وفكر الأفراد، وتفيد وتنمي معرفتهم حول محيطهم وبذلك تساعدهم على اتخاذ القرارات. وترتبط جودة المعلومات بتوفر أربعة عناصر فيها وهي: الدقة، التوقيت، السليم، الشمولية والملائمة.

3- مفهوم نظم المعلومات:

تتعدد التعاريف التي يحض بها مصطلح نظام، فمن خلال مختلف التعاريف التي اطلعنا عليها ارتأينا أن نقدم تعريف يعطي صورة شاملة ومتكاملة لنظام المعلومات:

" نظام المعلومات هو مجموعة من العناصر المادية (الماكنات، الوسائط والحواسيب)، والعناصر الغير مادية (الإجراءات والبرمجيات)، والعناصر البشرية (الاختصاصيين والمستخدمين النهائيين للمعلومة)، تعمل معا كجزء واحد، وتتفاعل فيما بينها، فتقوم بالحصول على البيانات والتي تعتبر كمدخلات، وإدخالها للمعالجة، وتحويلها إلى معلومات بصفة مخرجات، وتخزينها و/أو إرسالها إلى مستخدميها بهدف دعم اتخاذ القراروتحقيق الرقابة والتحكم الشامل في المؤسسة، ويتم كل هذا بطرق أكثركفاءة ودقة."

4- موارد نظام المعلومات:

يحتوي نظام المعلومات على أربعة موارد أساسية وتتمثل فيما يلي:[8]

1-3 <u>موارد المادية</u>: ويشمل جميع المعدات المادية والمواد المستخدمة في معالجة البيانات، وهي بالأخص الماكنات مثل الحاسوبات والآلات الحاسبة، كما تشمل أوساط (وسائط) البيانات مثل الأوراق والأقراص المغناطيسية والأقراص المضغوطة، شبكات الاتصال...الخ.

2-3 موارد البرمجيات والإجراءات: هي مجموعة من الأوامر والتعليمات الخاصة بلغة الحاسوب والتي تختص مهمتها في معالجة البيانات، ومن البرمجيات يوجد:

- برمجيات النظام: مثل نظام التشغيل الذي يدير ويدعم عمليات منظومة الحاسوب (كالويندوز windows ولينيكس lunix).
- برمجيات تطبيقية: وهي برامج توجه الحاسوب لاستخدام معين من قبل المستخدم النهائي (كالوورد word)، تطبيقات تسيير المخزون...الخ.
- أما الإجراءات فهي توجيهات تشغيلية للأفراد اللذين سيستخدمون نظام المعلومات.

3-3 موارد الأفراد: هناك حاجة للأفراد لتشغيل جميع أنظمة المعلومات وهذا المورد يتكون من الاختصاصيين والمستخدمين النهائيين:

- الاختصاصيين: هم الأفراد اللذين يصممون ويشغلون ويحللون نظام المعلومات، ويتكونون من محللي الأنظمة، والمبرمجين ومشغلي الحاسوب.
- المستخدمون النهائيون: هم الأفراد اللذين يستخدمون نظام المعلومات، ويمكن أن يكونوا المدراء أو المحاسبين أو المهندسين أو وكلاء البيع أو العملاء...الخ.

4-3 موارد البيانات: البيانات هي أكثر من المواد الخام لنظم المعلومات، فالبيانات والمعلومات تشكل موارد ثمينة للمؤسسة، ولقد تم التطرق إليها في المحور السابق.

5- الوظائف الأساسية لنظام المعلومات:

تتمثل الوظائف الأساسية لنظام المعلومات لأي مؤسسة في أربعة وظائف:

1-4 وظيفة الإعلام: هي وظيفة الحصول على البيانات وتتضمن اختيار وتحديد كل البيانات اللازمة سواء من داخل المؤسسة أو خارجها في ضوء احتياجات المستويات الإدارية في المؤسسة.

2-4 وظيفة المعالجة: يمكن تعريف معالجة البيانات بمجموعات متباينة (مختلفة) من العمليات التي تسمح بتغيير وتحويل المعطيات إلى مخرجات (المعلومات).

3-4 وظيفة التخزين: وقد تسمى بوظيفة وضع وحفظ المعلومات بتصنيف أو ترتيب معين في ملفات ويتم حفظ وتخزين المعلومات بطريقة يسهل الرجوع إليها عند الحاجة.

4-4 وظيفة الاتصال: إن إيصال المعلومات إلى مستخدمها النهائي هو من الوظائف الحيوية لنظام المعلومات وقد يتطلب ذلك نقلها من مكان معالجتها أو من مكان تخزينها إلى مكان استخدامها.

ثانيا: أمن المعلومات وأهم المخاطر التي تتعرض لها:

1- مفهوم أمن المعلومات:

يعرف أمن نظم المعلومات بأنها الإجراءات والتدابير الوقائية التي تستخدم سواء في المجال الفني أو الوقائي لصيانة المعلومات مثل الأجهزة والبرمجيات، والبيانات المتعلقة بالتطبيقات، وكذلك الأفراد العاملين ضمن هذا المجال.[9]

يمكن إعطاء تعاريف مختلفة لأمن المعلومات، وذلك حسب اختلاف كل مجال تخصص:[10]

1-1 من الناحية التنظيمية: هو المجال الذي يبحث في نظريات واستراتيجيات توفير الحماية للمعلومات من المخاطر التي تهددها، ومن أنشطة الاعتداء عليها.

1-2 من الناحية التقنية: هي الوسائل والإجراءات والأدوات والإجراءات اللازم توفيرها لضمان حماية المعلومات من الأخطار التي تهددها سواء كانت أخطار داخلية أو خارجية.

1-3 ومن الناحية القانونية: فإن أمن المعلومات هو محل دراسات وتدابير حماية سرية وسلامة محتوى المعلومات وتوفرها، ومكافحة أنشطة الاعتداء عليها أو استغلال نظمها في ارتكاب الجريمة

2- مكونات أمن المعلومات:

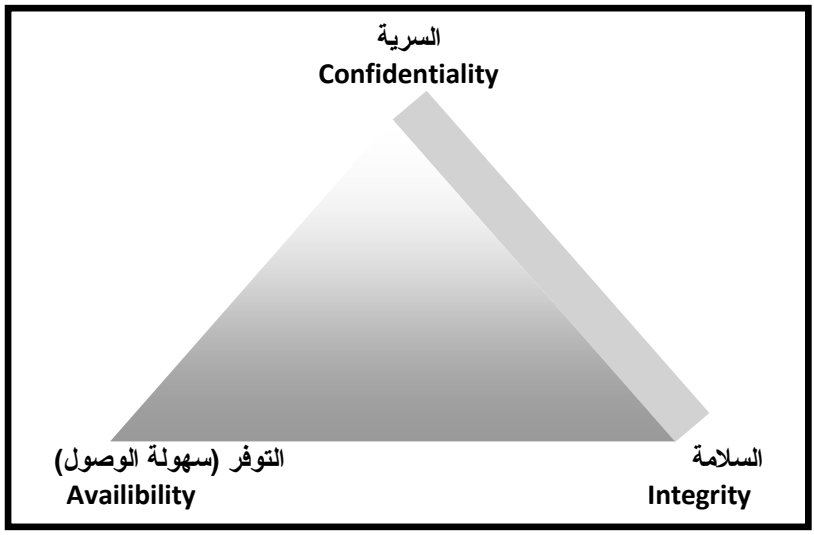
يرى خبراء ومختصون في أمن المعلومات أن هناك ثلاث مكونات (أو تسمى ثلاثية أمن المعلومات **Information Securite Triad**) على درجة واحدة من الأهمية، حيث أنه لو انتهكت أحدها فنعتبر أن المعلومة قد تعرضت للخطر والشكل التالي يبين هذه المكونات:[11]

1-2 سرية المعلومات **(Confidentiality)**: ويشمل هذا العنصر على كل التدابير اللازمة لمنع اطلاع غير المصرح لهم على المعلومات الحساسة أو السرية، ومن أمثلة المعلومات التي يحرص على سريتها: المعلومات الشخصية، الوضع المالي لشركة ما قبل إعلانه، المعلومات العسكرية.

2-2 سلامة المعلومات **(Integrity)**: وما يهمنا في هذا العنصر هو اتخاذ التدابير اللازمة لحماية المعلومات من التغيير.

3-2 توفر وضمان الوصول إلى المعلومات **(Availibility)**: إن الحفاظ على سرية المعلومة وسلامتها في الحقيقة أمر مهم لكن لا يكفي، لأن هذه المعلومات ليس لها قيمة إذا كان من يحق له الإطلاع عليها لا يمكنه الوصول إليها، أو أن الوصول إليها لا يتم في التوقيت المناسب (يحتاج وقتا طويلا)،

الشكل (1): ثلاثية أمن المعلومات



المصدر: من إعداد الباحث نقلا عن موقع: http://blog.infosanity.co.uk/2010/06/07/infosec-triads-c-i-a

إذن ومن خلال ما تطرقنا إليه في قضية أمن المعلومات يتبين لنا أن أمن أي معلومة في المؤسسة يتطلب توفر سرية، سلامة وإمكانية أو ضمان الوصول إليها، وإن تعرضت إحدى العناصر أو كلها للانتهاك فهذا يعني تعرض المعلومة للخطر وبالتالي تفقد جودتها، وهذا ما يؤدي إلى اتخاذ القرارات الخاطئة فيما يخص التخطيط والتحكم الشامل في المؤسسة، وهذا ما يرجع بالسلب على المؤسسة وتنافسيتها واستمراريتها.

3- المخاطر التي تتعرض لها نظم وتكنولوجيا المعلومات:

إن المخاطر والتخريب التي تتعرض لها نظم وتكنولوجيا المعلومات كثيرة ومتنوعة منها ما يكون بنية القصد أي تنفيذ الخطر يكون عمدا ومقصود وكمثال على ذلك القرصنة، ومنها ما يكون غير مقصود، كإهمال العاملين أو وجود خلل في المنظومة الأمنية. وإن أي منظومة للمعلومات في المؤسسات تكون عرضة للهجوم من جهتين مختلفتين ألا وهي الجهة الداخلية، والجهة الخارجية، وسنتناول فيما يلي أهم وأصعب المخاطر التي تتعرض لها نظم المعلومات.

1-3 المخاطر المقصودة من الداخل (المهاجمون من الداخل):

يقصد بالمهاجمين من الداخل، هم الأفراد الذين ينتمون للجهة المستهدفة (الموظفون والعاملون)، سواء كانت الجهة المستهدفة شركة أو منظمة أو حكومة، ويظهر تقرير صدر في الولايات المتحدة الأمريكية في 2003، أعده كل من مكتب التحقيق الفدرالي (FBI) بالمشاركة مع معهد أمن الحاسوب (CSI)، أن 36% من العينة التي شملتها الدراسة تعتبر المستخدمين من الداخل أكبر خطر على أنظمة المعلومات التي تستخدمها تلك الجهات، وفي تقرير صدر عن وزارة الدفاع الأمريكية سنة 2000، ذكرت فيه أن 87%من الهجمات المكتشفة والتي شنت على أنظمت المعلومات بالوزارة، قام بها أشخاص من داخل الوزارة نفسها.[12] وإن من دوافع الفرد لشن هجوم ضد أنظمة المعلومات التي تخص الجهة التي يعمل فيها ما يلي:

- عدم رضا الشخص بظروف العمل (عدم الرضا بالراتب، سوء معاملة المسؤولين الكبار...الخ)، فباختراقه لنظم المعلومات يشعره بلذة الانتقام.
- إثبات الشخص لمهاراته الفنية وقدرته على تنفيذ هجوم إلكتروني، وشعوره بالفخر أمام قرنائه في ذلك.
- لتحقيق المكاسب المالية كسرقة معلومات سرية وابتزاز الجهة المعنية لدفع الفدية.

إن الهجوم من الداخل يمكن إن يخل بأي من مكونات أمن المعلومات، أي أنه يمكن أن يلحق الضرر بسرية المعلومات أو سلامتها، أو يمنع ويعيق الوصول إلى المعلومات، والمهاجم الذي يكون ماهرا لا يترك خلف هجومه أي أثر يدل على ارتكابه له، وأهم جوانب الأخطار التي تأتي من الداخل تتمثل في:

أ- مهاجمة الشبكة الداخلية للمؤسسة التي يعمل فيها.

ب- مهاجمة المعلومات بالسرقة أو التغيير أو الحذف.

ج- فتح ثغرات في أنظمة الحماية التي وضعتها المؤسسة لتحصين وحماية أنظمة المعلومات فيها.[13]

2-3 المخاطر الغير مقصودة من الداخل:

مهما تقدم علم البشر وزادت الأفراد في المعرفة العلمية والتطبيقية، تبقى مشكلة النقص في التركيبة البشرية أمر حقيقي وموجود، إذ يبقى عمل الإنسان ناقصا وفيه بعض الخلل والثغرات التي تمثل في حد ذاتها مشكل بل خطر كبير عليه وعلى العمل الذي قام به. هذا ما يؤدي إلى ظهور المخاطر التي ينفذها الموظفين ومصمم نظم المعلومات عن غير قصد والتي نذكر منها:[14]

- الإدخال الغير مقصود لبيانات غير سليمة بواسطة الموظفين.
- التدمير الغير متعمد للبيانات بواسطة الموظفين.
- الإدخال الغير مقصود للفيروسات لنظم المعلومات.

- إهمال وغفلة المصممين على تصميم نظام معلومات متكامل ومحمي من جميع المخاطر.

3-3 المخاطر من الخارج (الهجمات الخارجية):

وهي مختلف التهديدات والهجومات التي تخص المعلومات وتكون هذه الأخيرة من مصدر خارجي، وتندرج معظمها ضمن ما يسمى "الجرائم الإلكترونية" وتعرف على أنها أي فعل ضار يأتيه شخص عبر استعماله مواد الكترونية، كما تعرف على أنها تلك القضايا الحاسوبية الغير قانونية أو الدخول الغير شرعي للبيانات والملفات والبرامج مثل قضايا التحايل السرقة والتجسس والتزوير وقضايا التخريب.[15] فالمعلومات كونها ثروة ذات قيمة أصبحت عرضة للتهديد والاختراق والاعتداء عليها سهل وغير مكلف (خاصة عبر الانترنت)، وأصبح بالإمكان خرق امن المعلومات عن بعد ومن أماكن جغرافية متباعدة، من خلال أقمار التجسس والأقمار الصناعية المنتشرة في الفضاء الخارجي ويعرف هذا بجرائم المعلومات التي تأخذ أشكال متعددة منها:

1- السرقات : كسرقة البيانات، والبرمجيات، والأجهزة، واستخدام المعلومات في سرقة الأموال...الخ.

2- تدمير المعلومات: حيث يتم إزالة وإزاحة المعلومات المخزنة بالحاسوب بالكامل.

3- تعديل المعلومات: حيث يتم إجراء تغييرات على ملفات ومعلومات معينة بغرض التضليل.

4- الانتهاكات والاختراق والدخول غير المشروع إلى الملفات: للاطلاع على معلومات غير مسموح إلا لأشخاص معينين والدخول أليها.

5- تغيير بروتكولات الاتصال. 6- الفيروسات.

ثالثا: منهجية إدارة مخاطر المعلومات وأمنها

عندما نتحدث عن إدارة مخاطر أمن المعلومات نكتشف أن مصطلح "إدارة المخاطر" مستخدم في العديد من التخصصات و المهن، فالعاملين في البنوك يستخدمونه للإشارة إلي مخاطر الائتمان(من بين أمور أخري)، أما المتخصصين في مجال تكنولوجيا المعلومات فيستخدمونه للإشارة إلي المخاطر التي تتعرض لها المعلومات نتيجة هجوم فيروسات الكمبيوتر علي سبيل المثال،.والمدققين الداخليين يستخدمونه للإشارة إلي الضوابط المالية الداخلية بالمؤسسة، وضباط الأمن والسلامة .

1- مفهوم إدارة مخاطر أمن المعلومات:

إدارة المخاطر: هي عملية قياس وتقييم للمخاطر وتطوير إستراتيجيات لإدارتها، تتضمن هذه الإستراتيجيات نقل المخاطر إلى جهة أخرى وتجنبها وتقليل آثارها السلبية وقبول بعض أو كل من تبعاتها.

كما يمكن تعريفها بأنها النشاط الإداري الذي يهدف إلى التحكم بالمخاطر وتخفيضها إلى مستويات مقبولة. وبشكل أدق هي عملية تحديد وقياس والسيطرة وتخفيض المخاطر التي تواجه الشركة أو المؤسسة.

2- مراحل إدارة مخاطر أمن المعلومات:

هناك ثلاثة مراحل تمثل الأعمدة الرئيسية التي تكون برنامج ناجح لإدارة مخاطر تكنولوجيا المعلومات، ولكل مرحلة منها أنشطتها ومهامها وهذه المراحل تتمثل في:[16]

2-1 مرحلة تحديد وقياس المخاطر: في هذه المرحلة الأولي من مراحل برنامج إدارة مخاطر تكنولوجيا المعلومات، يتم التركيز علي تعريف المخاطر التي تتعرض لها المؤسسة والتكنولوجيا المستخدمة بها، مع زيادة التوعية بتلك المخاطر وتحديد التأثير المتوقع حدوثه على دورة العمل في المؤسسة في حال حدوث الكارثة، وتتمحور الأنشطة

الرئيسية في هذه المرحلة حول

- عمل قائمة بكل الأصول المعلوماتية والتكنولوجية التي تمتلكها المؤسسة.
- تحديد مستوي الامتثال لسياسات أمن المعلومات المعلنة في المؤسسة.
- قياس وتقييم المخاطر التي تتعرض لها المؤسسة.
- استعراض الخيارات المتاحة للتخفيف من حدة المخاطر.

ويتم التركيز دائما علي المخاطر التي سيكون لها - في نهاية المطاف - تأثير اقتصادي سلبي علي المؤسسة، ومن المتوقع أن تسبب خسائر متنوعة مثل:[17]

- خسائر تشغيلية: ناتجة عن تأثر مستوي التشغيل المعتاد لمنظومة العمل واستمرارية تقديم الخدمات التجارية بسبب أعمال التخريب، أو إصابة نظم المعلومات بالمؤسسة بفيروسات الكمبيوتر أو توقف الخدمة المقدمة للعملاء.

- خسائر قانونية: نتيجة العقوبات المالية المنصوص عليها في عقود قانونية نتيجة إفشاء المعلومات لأفراد أوجهات أو منافسين لم يكن من المفترض حصولهم عليها.

- خسائر مالية: خسائر في الإيرادات بسبب الإخلال باتفاقيات وفقدان السرية، والنزاهة، والخصوصية، أو إتاحة المعلومات لأفراد أو جهات لم يكن من المسموح لهم الإطلاع عليها.

- خسائر استراتيجيه: ناتجة من تأثر الإيرادات المستقبلية وفقدان العملاء أو الإخلال بحقوق الملكية الفكرية.
- خسائر تأثر في سمعة المؤسسة: نتيجة لفقد ثقة العملاء والجمهور في المؤسسة.

2-2 مرحلة إدارة المخاطر: بمجرد أن تقوم إدارة المؤسسة بتعريف المخاطر ومنهجية تنفيذ برنامج إدارة والتخفيف من المخاطر بالمؤسسة، تبدأ في الاختيار بين عدة

إجراءات مقترحة منها:

- تجنب المخاطر عن طريق تجنب استخدام معدات تقنية لا تستطيع المؤسسة حصر التعامل مع المخاطر المحتملة الناتجة عن تشغيلها.
- تقليل المخاطر من خلال تنفيذ ضوابط التخفيف من المخاطر.
- قبول المخاطر لفترة زمنية محددة، إذا كانت التكلفة تزيد عن العائد المتوقع.
- نقل المخاطر ليتحمله طرف آخر، (علي سبيل المثال التأمين على التكنولوجيا المستخدمة لدى شركة تأمين).

إذا مهما كان القرار المتخذ، فالإجراء المنفذ من قبل الإدارة على ضوء الخيارات المتاحة يجب أن يتم توثيقه في وثيقة مكتوبة ليتم مراجعته في المستقبل، لفترة لا تزيد عن عام من تاريخ قرار قبول المخاطر وتحديد هل المخاطر لازالت موجودة، وما إذا كان بالإمكان التخفيف منها بتطبيق الضوابط المقترحة.

3-2 مرحلة رصد وتقييم المخاطر: بعد التنفيذ المبدئي لبرنامج إدارة مخاطر تكنولوجيا المعلومات، يجب تأسيس مجموعة من الآليات لضمان استمرار عمليات التعريف والتوعية وقياس وإدارة المخاطر، وتعتبر إجراءات دمج تقنيات إدارة مخاطر تكنولوجيات المعلومات في دورة حياة المشروع خطوة جيدة للحفاظ على استمرارية ثقافة إدارة المخاطر بالمؤسسة وهناك عناصر رئيسية مكونة لهذه المرحلة منها:

- المحافظة على استمرارية تحديث قائمة الأصول المعلوماتية والتكنولوجية للتأكد من أن كل وحدة عمل بالمؤسسة تقوم بتنفيذ إجراءات إدارة المخاطر.
- إجراء تقييم ذاتي سنوي لتحقيق متطلبات أمن المعلومات للمشروع بأكمله.
- مراجعة دورية لسياسات أمن المعلومات، للتأكد من أنها وما يتبعها من متطلبات تستطيع التعامل مع المخاطر التي استجدت نتيجة لاستخدام تقنيات جديدة في العمل.

3- أدوات وإجراءات حماية أمن المعلومات:

1-3 تقنيات الحماية ضد البرامج الخبيثة: إن البرامج الخبيثة هي أي برنامج يكون كل مهامه أو إحداها عمل خبيث، من تجسس أو تخريب أو استنزاف للموارد (الوقت، المعالج، الذاكرة، وحدة التخزين، سعة النقل الشبكي)، وهناك العديد من البرامج الخبيثة:[18]

- الفيروسات Viruses والديدان Worms والأحصنة الطروادية Trojan Horses وبرامج التجسس Spyware وصفحات فقاعية أو انبثاقية Popup وبرنامج تسجيل نقرات لوحة المفاتيح Keystroke Logger

وتصاب أنظمة المعلومات بهذه البرامج الخبيثة عن طريق:

- انتقالها عن طريق وسائط التخزين كالفلاش يو أس بي (USB) وكروت الذاكرة والأقراص المرنة والمدمجة.
- عبر البريد الإلكتروني وذلك بـ: مجرد فتح الرسالة، عن طريق المرفقات، عن طريق رابط معطى في الرسالة.
- تصفح المواقع المشبوهة خاصة الإباحية منها.
- عن طريق برامج المراسل الآني مثل (Messenger, ICQ MSN Messenger, Yahoo)
- تحميل برامج من الإنترنت قد تظم برامج خبيثة بداخلها.

ومن الإجراءات الوقاية والحماية من البرامج الخبيثة ما يلي:

- استخدام برامج مكافحة الفيروسات واستمرارية تحديثه.
- عمل مسح كامل ويومي للأجهزة الحاسوب بواسطة برامج الحماية.
- العمل على فحص كافة وسائط التخزين الخارجية عند توصيلها أو إدخالها في الحاسوب، وذلك قبل الشروع في استخدامها.
- استعمال الجدران النارية (Firewall) لسد المنافذ غير الآمنة وتقليل الأخطار على الأجهزة.

2-3 استخدام الأنظمة الذكية وتقنية التشفير: ومن بين الإجراءات والأدوات التي من شأنها توفير الحماية والأمن للمنظومة المعلوماتية هو استخدام الأنظمة الذكية، وهي أنظمة تمتاز بالكشف المبكر للتهديدات التي ستلحق بنظم المعلومات، وفي حالة عجز المنظمة عن توفير هذه الأنظمة بمفردها، تستطيع اللجوء إلى وكالات أو هيئات خاصة بتقديم هذه الخدمة وذلك بسرية تامة. ومن بين هذه الأنظمة:[19]

- البطاقة الذكية للتعرف على الشخص المستخدم: تستخدم هذه البطاقة الرقائق الالكترونية ولاتي تحمل عليها كلمة السر الخاصة بصاحب البطاقة.

- استخدام البيولوجيا الإحصائية: وهي طريقة تستخدم للتعرف على الأشخاص وتستند على الخصائص البيولوجية أو السيكولوجية للفرد منها:

- ملاحظة الوعاء الدموي للعين والذي يمكن معرفته عن طريق أخذ صورة لها.

- ديناميكية الضربة على المفاتيح التي تستخدم في لوحة مفاتيح الحاسوب وسرعته في استخراج المعلومات المخزونة.

- البطاقة الصوتية الذكية، وتستخدم للتعرف على أصوات الأفراد والتي لها استخدامات أمنية مثل مراقبة الدخول إلى معلومات أو بيانات مخزنة ذات طابع سري للغاية.

- التعرف على بصمات المستخدم وهو نظام متطور لتأمين حماية الدخول الغير مشروع إلى الحاسوب.

- استعمال تقنية التشفير: عند الحاجة إلى نشر البيانات عبر شبكة الحاسوب تستخدم تقنية التشفير Encryption وهي طريقة أمنية تستخدم تقنية ترميز الرسائل لتصبح غير مفهومة لأي شخص يعترض الرسائل أثناء عملية مرورها عبر الشبكة، إذ يتم تشفير الرسالة قبل نشرها وإعادة فك الشفرة عند استلامها من الجهة المقابلة، حيث لا يفهم هذه الشفرة إلا الجهة المرسلة والجهة المستقبلة فقط.

3-3 إجراء الرقابة العامة على أنظمة المعلومات في المنظمة: ويقصد بها الرقابة الشاملة وهي طريقة العمل التي بواسطتها تتم الرقابة على التصميم والأمن، واستخدام برامج الحاسوب الموجودة في المؤسسة، وللتأكد من فعالية العمليات الخاصة بإجراء البرمجة، ومن أنواع هذه الرقابة:

- الرقابة على التصميم: يتم بناء خصائص ومعايير الرقابة على تصميم النظام من خلال محللي النظام ومديري قواعد البيانات، مع مراعاة مبدأ التكلفة والمنفعة.
- الرقابة على البرمجيات: وهي تغطي برامج تشغيل النظام، والتي تقوم بتنظيم إدارة موارد الحاسوب وهذا بهدف تسهيل استخدام وتنفيذ البرمجيات التطبيقية.
- الرقابة على المكونات المادية: يجب حماية الأماكن التي يوجد بها الحاسوب بالطريقة التي تسمح للأفراد المرخص لهم فقط بالتعامل معه، وتتضمن الحماية أيضا الظروف التي يعمل بها الحاسوب كدرجة الحرارة ونسبة الرطوبة ...الخ.

- الرقابة على تشغيل واستخدام الحاسوب: وذلك للتأكد من أن إجراءات البرمجة متناسقة، وتطبق بطريقة صحيحة بالنسبة لتشغيل وتخزين البيانات والمعلومات.

- الرقابة على عمليات تنفيذ النظام: وهي التأكد من أن نظم المعلومات المبنية على الحاسوب تقابل احتياجات المستخدمين من خلال التعرف على احتياجات كل مستخدم من المعلومات، تحديد معايير الأداء، وضع معايير التصميم والتشغيل لنظم المعلومات المبنية على الحاسوب، وتحديد اختبار قبول النظام ومراجعته وصيانته من قبل المتخصصين.[20]

رابعا: الاستنتاجات والتوصيات

من خلال ما تم التطرق إليه في المحاور السابقة من هذه المقالة نستنتج ما يلي:

- أن تهتم جميع المؤسسات بالمعلومات التي تعتبر مورد مهم من موارد المؤسسة التي تساعد كثيرا في اتخاذ القرارات، وأن أي خطر أو تهديد يمسها ينعكس أثره بالسلب على القرارات المتخذة من قبل المسئولين.

- على المؤسسات تصميم نظم معلومات جيد وبمعايير حديثة لضمان تأدية مهامه التي صمم من أجلها، من جهة، ولضمان أمن المعلومات من جميع المخاطر التي تتعرض لها.

- إن التهديدات الأمنية التي تخص نظم المعلومات تتطور بتطور الزمن شأنها في ذلك تكنولوجيا المعلومات، وعلى المنظمات تطوير أدواتها وإجراءاتها الأمنية لمواكبة هذه التطورات.

- الإتباع الدائم لمنهج إدارة مخاطر أمن المعلومات، مع صياغة إستراتيجية محكمة ومتكاملة للتصدي لكافة أنواع التهديدات والمخاطر التي تواجه أمن معلوماتها.

- العمل على معرفة رغبات وتطلعات الأفراد العاملين وتلبيتها، مع توعيتهم وتدريبهم في مجال المعلوماتية، وإتاحة الفرصة لهم لإظهار مهاراتهم وقدراتهم، لتستفيد منها المؤسسة لا لترجع بالسلب عليها (الهجوم من الداخل).

الاحالات والمراجع:

1. محمد محمد الهادي، **التطورات الحديثة لنظم المعلومات المبنية على الكومبيوتر**، دار الشروق، بيروت، ط 1، 1993، ص: 55.

2. سلوى أمين السمرائي، **متطلبات التحول نحو الاقتصاد المعرفي**، ورقة بحث مقدمة في إطار المؤتمر العلمي الدولي الرابع حول: إدارة المعرفة في العالم العربي، جامعة الزيتونة الأردنية، 28/ 26 أفريل 2004، ص: 2.

3. Brayen Bergeron, **Essentials of knowledge management**, Jhon Wiley and son; INC,2003, P: 10.

4. Chabha Bouzar, Abderahmane Batach, **NTIC et les entreprise de l'information à la connaissance**, colloque international : les impacts de la fracture numérique nord/ sude sur la gestion des PME/ PMI : métier, sous-traitance et externalisation, Univ-Biskra, 28,29/04/2007, P : 3.

5. براهيم بختي، **تكنولوجيا ونظم المعلومات في المؤسسات الصغيرة والمتوسطة**، مطبوعة مقدمة لطلبة الماجستير تخصص، تسيير المؤسسات الصغيرة والمتوسطة، ص: 14.

6. إسماعيل السيد، **نظم المعلومات لاتخاذ القرارات الإدارية**، المكتب العربي الحديث، الإسكندرية، 1989، ص: 97.

7 .RONAGNI.(P) et WILD.(V): **l'intelligence économique au service de l'entreprise, ou l'information comme outil de gestion**, Les presses de management, Paris, 1998, p : 92.

8 . سعد غالب ياسين، **تحليل وتصميم نظم المعلومات**، دار المناهج للنشر والتوزيع، الأردن، ط 1، 2000، ص ص: 17، 18.

9. علاء عبد الرزاق السالمي، **تكنولوجيا المعلومات**، دار المناهج، عمان، 2000، ص: 391.

10. سناء عبد الكريم خلاق، إدارة مخاطر أمنية المعلومات: التهديدات والحماية،

11. خالد بن سليمان الغثبر، محمد بن عبد الله القحطاني، **أمن المعلومات بلغة ميسرة**، مكتبة ملك فهد الوطنية، الرياض، 2009، ط 1، ص ص: 22، 23.

12. خالد بن سليمان الغثبر، محمد بن عبد الله القحطاني، مرجع سابق، ص: 26.

13. خالد بن سليمان الغثبر، محمد بن عبد الله القحطاني، مرجع سابق، ص ص: 27، 28.

14. عصام محمد البحيصي، حرية شعبان شريف، **مخاطر نظم المعلومات المحاسبية الإلكترونية: دراسة تطبيقية على المصارف العاملة في قطاع غزة**، مجلة الجامعة الإسلامية (سلسلة الدراسات الإنسانية)، المجلد السادس عشر، العدد الثاني، جويلية 2008، ص: 904.

15. الشرايعة أحمد عبد العزيز، فارس سهير عبد الله، **الحاسوب وأنظمته**، دار وائل للنشر، عمان، 2000، ص: 100.

16.أحمد عبيد، **إدارة مخاطر أمن المعلومات**، مقال منشور على موقع: http://secureminds.net/articleRiskManagement.aspx، تصفح يوم: 2012/04/11.

17. نفس المرجع السابق

18. خالد بن سليمان الغثبر، محمد بن عبد الله القحطاني، مرجع سابق، ص ص:57-63.

19. سناء عبد الكريم خلاق، مرجع سابق، ص: 8.

20. المرجع السابق، ص: 11.