نظام امن المعلومات في منظمات الإعمال مع نموذج مقترح لمواجهة تهديدات النظام

د. أمل عبد محمد علي
كلية الادارة والاقتصاد
جامعة بابل

الملخص

تساهم تقنيات المعلومات في رسم سياسة الأداء في المنظمة ، وتعكس السمة المميزة لعالم اليوم ، وتعد مؤشر بقاء ونجاح المنظمات ، لذلك أصبح أمن المعلومات من المواضيع الحيوية لكون أي نظام معلومات يتعرض إلى العديد من التهديدات المحتملة وهذا ما يتطلب إنشاء نظام فاعل لحماية المعلومات . تناول البحث موضوع أمن المعلومات في منظمات الأعمال والتهديدات المحتملة التي تواجهه مع عرض نموذج مقترح تضمن خطوات إنشاء النظام والإجراءات المتبعة٦٦٨٧٤$ لمواجهة تهديدات النظام ، وأختتم البحث بجملة من التوصيات والتي قد تعد كمتطلبات لازمة لتطبيق آلية حماية المعلومات في منظماتنا العراقية من أجل ضمان سرية المعلومات ، وتكاملها ، وتوافرها ، وسلامة محتواها ، وتحديد مسؤولية المتصرف بها .

المبحث الأول

نظام أمن المعلومات

1- مفهوم امن المعلومات :

لكي نتمكن من استيعاب مفهوم امن المعلومات لابد من استعراض السياق التاريخي لتطور هذا المفهوم . لقد ظل هذا المجال من الامن حتى اواخر السبعينات معروفا باسم امن الاتصالات (Communication security) والذي حددته توصيات امن أنظمة المعلومات والاتصالات لوكالة الامن القومي في الولايات المتحدة بأنه :- " المعايير والاجراءات المتخذة لمنع وصول المعلومات الى ايدي اشخاص غير مخولين عبر الاتصالات ولضمان اصالة وصحة هذه الاتصالات". وفي الثمانينات مع النمو للحاسبات الشخصية بدأت حقبة جديدة من الامن سميت امن الحواسيب Computer Security . والتي حددت بكونها" المعايير والاجراءات التي تضمن سرية ، كمال ، توافر مكونات انظمة المعلومات بما فيها التجهيزات ، البرامجيات ، والمعلومات التي تم معالجتها ، تخزينها ، نقلها" .وفي التسعينات من القرن الماضي تم دمج

مفهومي الامن (امن الاتصالات وامن الحواسيب) لتشكل ما اصبح يعرف باسم (امن انظمة المعلومات) Information System security والتي عرفت بأنها :- "حماية انظمة المعلومات ضد أي وصول غير مرخص الى او تعديل المعلومات اثناء حفظها ، معالجتها او نقلها ، وضد ايقاف عمل الخدمة لصالح المستخدمين المخولين او تقديم الخدمة لاشخاص غير مخولين بما في ذلك جميع الاجراءات الضرورية لكشف ، توثيق ، ومواجهة هذه التهديدات " (www.itrainonline.org.) .

وأشير إلى امن المعلومات من زاوية اكاديمية بانه العلم الذي يبحث في نظريات واستراتيجيات توفير الحماية للمعلومات من المخاطر الذي تهددها من انشطة الاعتداء عليها (http://www.Gelbstein et al,2005) ،وعرفه السالمي على انه " العلم الذي يهتم بدراسة طرائق حماية البيانات المخزونة ضمن الحاسوب وانظمة الاتصالات والذي يتناول سبل التصدي للمحاولات الرامية الى معرفة البيانات المخزونة ضمن الحاسوب بصورة غير مشروعة والى تلك التي ترمي الى نقل او تغيير او تخريب برامجيات حماية البيانات" (السالمي ، 392,2000) .

اما من الناحية التقنية فان امن المعلومات تشير الى الوسائل والادوات والاجراءات اللازم توفيرها لضمان حماية المعلومات من الاخطار الداخلية والخارجية (O'Brien 1990,102) ، وعرفها الطائي بانها الحالة التي تتعلق بتدابير واجراءات حماية المعلومات المخزونة في نظام قاعدة المعلومات والتي تم تدفقها عبر انظمة الاتصالات او استرجاعها من خلال انظمة الاسترجاع من الاستخدام غير المشروع سواء كان مقصودا او غير مقصود (الطائي ، 158,2000) .

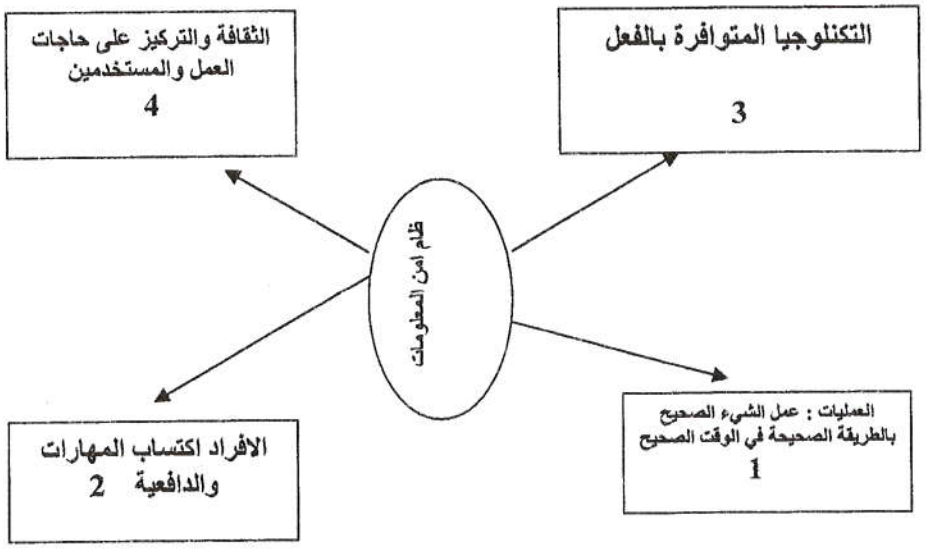
اما تعريفنا الاجرائي في البحث لنظام امن المعلومات فانه مجموعة المعايير والمقاييس والاجراءات والتدابير الوقائية والدفاعية التي تستخدم لحماية انظمة المعلومات بكل مكوناته وتحقيق التكامل على كافة المستويات لضمان سرية المعلومات، وتوافرها وسلامة محتواها، وتحديد مسؤولية المتصرف بها .ان تركيزنا على التعريف اعلاه وذلك بسبب شموليته ولكونه تضمن الخصائص المطلوبة لاية معلومات يراد توفير الحماية لها ، وهذا ما اكدته اغراض وابحاث واستراتيجيات ووسائل امن المعلومات سواء من الناحية التقنية أو الادائية أوالتشريعية ، وهي :

- السرية Confidetiality: وتعني التأكد بان المعلومات لم تصل لاشخاص ، عمليات او اجهزة غير مخولة بالحصول على هذه المعلومات .

- الكمال Integrity: تعكس جودة أي نظام للمعلومات مدى صحته، ووثوقية نظام التشغيل ، التكامل المنطقي للتجهيزات والبرامجيات التي توفر آليات الحماية ومدى تناغم بنى المعلومات مع البيانات المختزنة .
- التوافر Availability: التاكد من استمرار عمل النظام المعلوماتي واستمرار القدرة على التعامل مع المعلومات وتقديم الخدمة لمواقع المعلوماتية عند الحاجة اليها من قبل الاشخاص المخولين بذلك .
- سلامة المحتوى Intact content : التأكد من ان محتوى المعلومات صحيح ولم يتم تعديله او العبث به ، وبشكل خاص لن يتم تدمير المحتوى أوتغييره أو العبث به في اية مرحلة من مراحل المعالجة او التبادل سواء من مرحلة التعامل الداخلي مع المعلومات او عن طريق تدخل غير مشروع .
- عدم انكار التصرف Non-repudiation: ويقصد به ضمان عدم انكار الشخص الذي قام بتصرف ما متصل بالمعلومات او مواقعها انكار انه هو الذي قام بهذا التصرف بحيث تتوفر قدرة اثبات ان تصرف ما قد تم من شخص ما في وقت معين (www.information security.com)

2 - مكونات امن المعلومات :

ان تنفيذ وتشغيل نظام امن المعلومات يمثل طريقة حياة تعتمد على اربع مكونات اساسية كل منها مهم ولا يمكن التعامل معه بصيغة فردية مستقلة كما يظهر في الشكل رقم (١)



الشكل رقم (١)

١. العمليات : تعتبر العمليات لا غنى عنها لاي نظام امن وهي جوهرية وذات طبيعة مستمرة ويحكم اداة عمليات امن المعلومات مجموعة من المعايير كتلك التي اقرتها المنظمة الدولية للتوحيد القياسي (*) ISO والتي تعتبر ذات قيمة كبيرة لاي نظام امن معلومات .

٢. الافراد : وتمثل العاملين ، المستشارين ، المتعاقدين الذين ينجزون كل العمليات والخدمات وتحتاج أي منظمة الى تواجدهم باعداد وتخصصات ملائمة وبمهارات وخبرات ودافعية مناسبة .

٣. التكنلوجيا: وتعتبر متوافرة وجاهزة ولمنتجاتها دورات حياة قصيرة نسبيا. ويعتبر سوق التكنولوجيا ذات طبيعة تنافسية بتوافر عدد كبير من المنتجين والموردين والبائعين والموزعين فضلاً عن التغيرات المتسارعة في البيئة التكنولوجية.

٤. الثقافة : ترتبط بتفسير بيئة الاعمال وتتعلق باخلاقيات المنظمة تجاه المجتمع حيث يكون لادارة المنظمة دورا رئيسيا تؤديه في حفظ خطة ثقافة المنظمة المتوافقة مع ثقافة مجتمعها .وتشمل الاوجه الثقافية في نظام امن المعلومات ما يلي :أ.الانضباط التنظيمي القوي .ب.السياسة الموثقة والموصلة بوضوح لكل العاملين .ج. العمليات الموثقة والمساندة بواسطة المراجعات المستمرة .د. توافق عمليات المراجعة المستمرة .هـ .الاختبارات والمراجعات العادية الدورية.

٣.المخاطر وأنواعها في بيئة المعلومات

ان الاتجاه المتزايد نحو تكديس المعلومات الحساسة داخل اوعية مركزية عرفت بقواعد البيانات (Data base) ادت الى زيادة المخاطر التي تتعرض لها هذه المصادر، كذلك لا يساعد توزيع هذا المصدر على مواقع جغرافية منفصلة على تقليل هذه المخاطر طالما كانت هذه الانظمة مرتبطة من خلال شبكات الاتصال بل على العكس غالبا ما يكون ذلك سببا في وقوع المزيد من حوادث التهديدات . (أنور ، ١٩٩٠ ، ٥)

تقوم استراتيجية أمن المعلومات على تحليل المخاطر وتطال المخاطر والاعتداءات في بيئة المعلومات أربع مواطن أساسية تمثل مكونات تقنية المعلومات وهي :

* الأجهزة : وهي كافة المعدات والأدوات المادية التي تتكون منها النظم ، كالشاشات والطابعات ومكوناتها الداخلية ووسائط التخزين المادية وغيرها .

* البرامج : وهي الأوامر المرتبة في نسق معين لانجاز الأعمال ، وهي أما مستقلة عن النظام أو مخزنة فيه .

(*) . للمزيد من المعلومات راجع المصادر.

* المعطيات : وهي الدم الحي للأنظمة وما سيكون محلاً لجرائم الكومبيوتر وتشمل كافة البيانات المدخلة والمعلومات المستخرجة عقب معالجتها ، وتمتد بمعناها الواسع للبرمجيات المخزنة داخل النظم . والمعطيات قد تكون في طور الادخال أو الاخراج أو التخزين أو التبادل بين النظم عبر الشبكات وقد تخزن داخل النظم أو على وسائط التخزين خارجه .

* الأتصالات : وتشمل شبكات الأتصال التي تربط الأجهزة التقنية بعضها ببعض محلياً ، ونطاقياً ، ودولياً ، وتتيح فرص اختراق النظم عبرها ، كما أنها بذاتها محل للاعتداء وموطن من مواطن الخطر الحقيقي .

ومحور الخطر الانسان سواء المستخدم أو الشخص المناط به مهام تقنية معينة تتصل بالنظام ، فإدراك هذا الشخص حدود صلاحياته ، وادراكه آليات التعامل مع الخطر وسلامة الرقابة على انشطته في حدود احترام حقوقه القانونية تعد مسائل رئيسة يعنى بها نظام الأمن الشامل وتحديداً في بيئة العمل المرتكزة على نظام الكومبيوتر وقواعد البيانات .

ويمكن تصنيف المخاطر المحدقة ببيئة المعلومات تبعاً إلى ما يلي :

- **موضوع المعلومة من النظام**

إن أغلب قوائم تصنيف المخاطر يعتمد معيار موضوع المعلومات من النظام ومن ذلك مثلاً قائمة الشرطة العالمية الأنتر بول والتي صنفت المخاطر إلى ثلاثة أنواع وهي :

-المخاطر التي تتعرض لها المعلومات في مرحلة خلق واسترجاع وتعديل والغاء المعلومات وجامعها وجود المعلومات داخل النظام .

-المخاطر التي تتعرض لها المعلومات في مرحلة النقل أي التبادل بين أنظمة الكومبيوتر

-المخاطر التي تتعرض لها المعلومات في مرحلة التخزين على وسائط خارج النظام .

- **واسطة تقنية المعلومات**

إن المخاطر تختلف تبعاً لواسطة تقنية المعلومات فليست مخاطر الشبكات والدخول عبرها إلى نظم الكومبيوتر كمخاطر الكومبيوترات غير المرتبطة بالشبكة ، ومخاطر الأنترانيت أو الأكسترانيت تختلف عن مخاطر الأنترنيت ،ومخاطر مواقع التجارة الالكترونية على الشبكة تختلف عن مخاطر موقع معلوماتي محدد ، كما أن ثغرات ونقاط الضعف تختلف تبعاً للوسيلة أو الواسطة أو التقنية مدار البحث ، ومن هذه الزاوية تتمثل المخاطر بمخاطر وثغرات الشبكات سواء المحلية أو المناطقية أو الدولية ، كذلك مخاطر الأجهزة بأنواعها (الكومبيوترات الكبرى الرئيسة ، الشخصية ، المحمولة .. ألخ) مخاطر تطال المعطيات والبرمجيات بمختلف مناطق وجودها داخل وخارج النظام .

• **شيوع أساليب الهجوم وتقنياته وأغراض الهجوم وقيمة المعلومات**

يمكن أن تصنف العديد من قوائم تصنيف المخاطر والأعتداءات بأنها لا تعتمد معياراً منضبطاً بل تتعدد فيها معايير التقسيم ولذا تختلف المخاطر وطبيعتها والأشخاص الذين يرتكبون الأعتداء تبعاً لدرجة شيوع أنواع الأعتداءات وأساليبها وهو ما قد يتأثر بالوقت الذي تجري فيه المعالجة ، فعام ٢٠٠٠ مثلاً شهد من بين الهجمات اتساعاً كبيراً لهجمات إنكار الخدمة التي استهدفت مواقع الأنترنيت وشهد هجمات فيروسات عالمية ، في حين نجد الحديث في الوقت الحاضر قد ازداد بشأن الأعتداءات التي تستهدف مواقع الأعمال الالكترونية بغرض الحصول على المال عبر ما يعرف باحتيال الأنترنيت . وقد تصنف المخاطر تبعاً للدور المناط بالمعلومات موضوع الأعتداء والحماية ، فقواعد معلومات المواقع العسكرية مستهدفة من جهات عديدة وتصنف المخاطر في مواقع الدراسات إلى قوائم ترصد حركة المخاطر الشائعة وتضم عادة قوائم تبين في الوقت المحدد أكثر المخاطر انتشاراً في بيئة الكومبيوتر والأنترنيت كمخاطر الأخطاء التقنية ، الغش والأحتيال والاستيلاء على البيانات ، احقاد الموظفين ، الأخطار المادية ، الهجمات الحاقدة ، التجسس الصناعي ، التجسس الحكومي ، البرامج الخبيثة .

• **مناطق الاختراق والثغرات**

ويعد من أحدث التصنيفات السائدة على مختلف مواقع الأنترنيت المتخصصة وفيها يصار إلى تحديد المخاطر تبعاً للوصف التقني متصلاً بمصدر الاقحام أو نقاط الضعف أو الثغرات في النظام والتي تعني عنصر أو نقطة أو موقع في النظام يحتمل أن ينفذ من خلاله المعتدي أو يتحقق بسببه الاختراق ، فمثلاً يعد الأشخاص الذين يستخدمون النظام نقطة ضعف إذ لم يكن تدريبهم كافياً لاستخدام النظام وحمايته . وقد يكون الموقع المكاني للنظام نقطة ضعف كأن يكون غير مجهز بوسائل الوقاية و الحماية ، وبالعموم فإن نقاط الضعف هي أحد الأسباب المحركة لتحقيق المخاطر ويرتبط بهذا الأصطلاح اصطلاح الوقاية والتي تعني التكتيك المتبع لحماية النظام ككلمات السر ، والأقفال ، ووسائل الرقابة ، والجدران النارية وغيرها .

٤- نظام امن المعلومات :

ان الهدف من امن المعلومات هو حماية انظمة المعلومات ووسائل الاتصال التي تحتوي على هذه المعلومات وحماية مصالح اؤلئك المعتمدين على هذه المعلومات من أي ضرر قد ينتج في حالة اختراق سرية المعلومات او سلامة محتواها. (I.F.A.C.1998:8)

ان التحديد الواضح للمسؤولية الادارية عن نظام امن المعلومات بكامل مكوناته وأجهزته يساهم في تحديد عملية الانتهاك الامني للمعلومات والتي تعد بمثابة تدخل في عملية التدفق الشامل للمعلومات مابين نقطة اصدارها ونقطة استلامها. وعمليا قد لاتكون هناك اجراءات تتحكم

بالكيفية التي يتم التعامل بها مع هذه الانتهاكات ومن ثم فان الادارة قد لا تقدم على عمل شيء لجهلها بما يتعين القيام به ، وللتغلب على هذا الضعف يجب انشاء نظام لأمن المعلومات تحدد فيه الأشخاص الذين يستخدمون المعلومات البالغة الاهمية وكيفية تداولها وعدم اعطاء الفرصة لشخص واحد بان يكون لديه كامل المعرفة بالنظام الامني (فضل الدين،١٩٩٥:٢٥). وعلى المنظمة ان تكون لها سياسة أو استراتيجية واضحة لامن المعلومات وتتمثل بمجموعة القواعد التي يطبقها الاشخاص لدى التعامل مع التقنية ومع المعلومات داخل المنظمة وتتصل بشؤون الدخول الى المعلومات والعمل على نظمها وادارتها. وتهدف استراتيجية امن المعلومات الى تحقيق الاتي :-

* تعريف المستخدمين والاداريين بالتزاماتهم وواجباتهم المطلوبة لحماية نظم الكمبيوتر والشبكات وكذلك حماية المعلومات بكافة اشكالها، وفي مراحل ادخالها ومعالجتها وخزنها ونقلها واعادة استرجاعها .

* تحديد الآلية التي يتم من خلالها تحقيق وتنفيذ الواجبات المحددة على كل من له علاقة بالمعلومات ونظمها وتحديد المسؤوليات عند حصول الخطر .

* بيان الاجراءات المتبعة لتجاوز التهديدات والمخاطر والتعامل معها وتحديد الجهات المناط بها القيام بذلك.

ولكي تكون هذه الإستراتيجية فاعلة يتعين أن تعمم بشكل شامل على كافة قطاعات الإدارة ، وأن تكون مقبولة واقعيا من المناط بها تنفيذها ، وأن تكون مقبولة واقعيا من المناط بها تنفيذها ، إلى جانب توفر الأدلة التوجيهية والإرشادية لضمان ادامة التنفيذ وعدم التقاعس فيه ، كما يجب أن تشمل الإستراتيجية سياسة واضحة بشأن اقتناء وشراء الأجهزة التقنية ، والبرامجيات ، والحلول المتصلة بالعمل والحلول المتعلقة بإدارة النظام ، كما تبين الإستثناءات التي تعتمدها الإستراتيجية على حق الخصوصية لموظفي المنشأة مع مبررات هذه الإستثناءات.

إن سياسة نظام الأمن المعلوماتي تعزز وتكمل السياسة الكلية للمنظمة من خلال ما يأتي : (I.F.A.C.1998:11-12).

- تحديد التهديدات وتقويمها .
- تقليص التهديدات بتقليص احتمالات حدوثها .
- تحديد المسؤوليات الامنية (الخاصة) واسنادها الى اشخاص مختارين .
- اعداد خطط الاحتواء للتهديدات وتنفيذها ومراقبة خطط الطوارئ والتدريب على تنفيذها.
- الرصد السريع والمتابعة لكافة الاختراقات الامنية.

المبحث الثاني

تهديدات نظام أمن المعلومات مع نموذج مقترح

أولا : التهديدات التي تواجه نظام امن المعلومات :

تتعرض نظم أمن المعلومات التي تعتمد عليها المنظمات للعديد من التهديدات ويمثل التهديد " الخطر المحتمل الذي يمكن أن يتعرض له نظام المعلومات وقد يكون شخصاً كالمتجسس أو المجرم المحترف أو الهاكرز المخترق أو شيئاً يهدد الأجهزة أو البرامج أو المعطيات أو حدثاً كالحريق ، وانقطاع التيار الكهربائي ، والكوارث الطبيعية. (INTOSA , octber , 1995) ان العدد الكبير من التهديدات المحتملة لانظمة المعلومات ادى الى عدد كبير الاستراتيجيات الدفاعية والأدوات ، وان الدفاع عن انظمة المعلومات ليس بالمهمة السهلة والغير مكلفة للاسباب التالية:

١.الموارد الحاسوبية ربما تكون متواجدة في عدة مواقع .

٢.شبكات المعلومات الحاسوبية يمكن ان تكون خارج المنظمة ومن الصعوبة حمايتها .

٣. التغيرات التكنلوجية المتسارعة جعلت بعض الاجهزة الرقابية متقادمة حالما يتم نصبها .

٤.العديد من جرائم الكمبيوتر لايتم اكتشافها لفترات طويلة .

٥.الافراد قد ينصرفوا الى انتهاك(اختراق) اجراءات الأمن لكونها غير ملائمة.

العديد من مجرمي الكمبيوتر والذين تم امساكهم غالبا لم يعاقبوا على جرائمهم لذلك فهناك تأثير قليل لمنعهم او ردعهم .

٦. ان كمية المعرفة الحاسوبية الضرورية لمسك جرائم الحاسوب تكون قليلة.

٨ .ان تكاليف منع مصادر الخطر يمكن ان تكون غالية لذلك فأن معظم المنظمات ببساطة لاتستطيع وضع الاجراءات الامنية الضرورية لكل مصادر الخطر المحتملة .

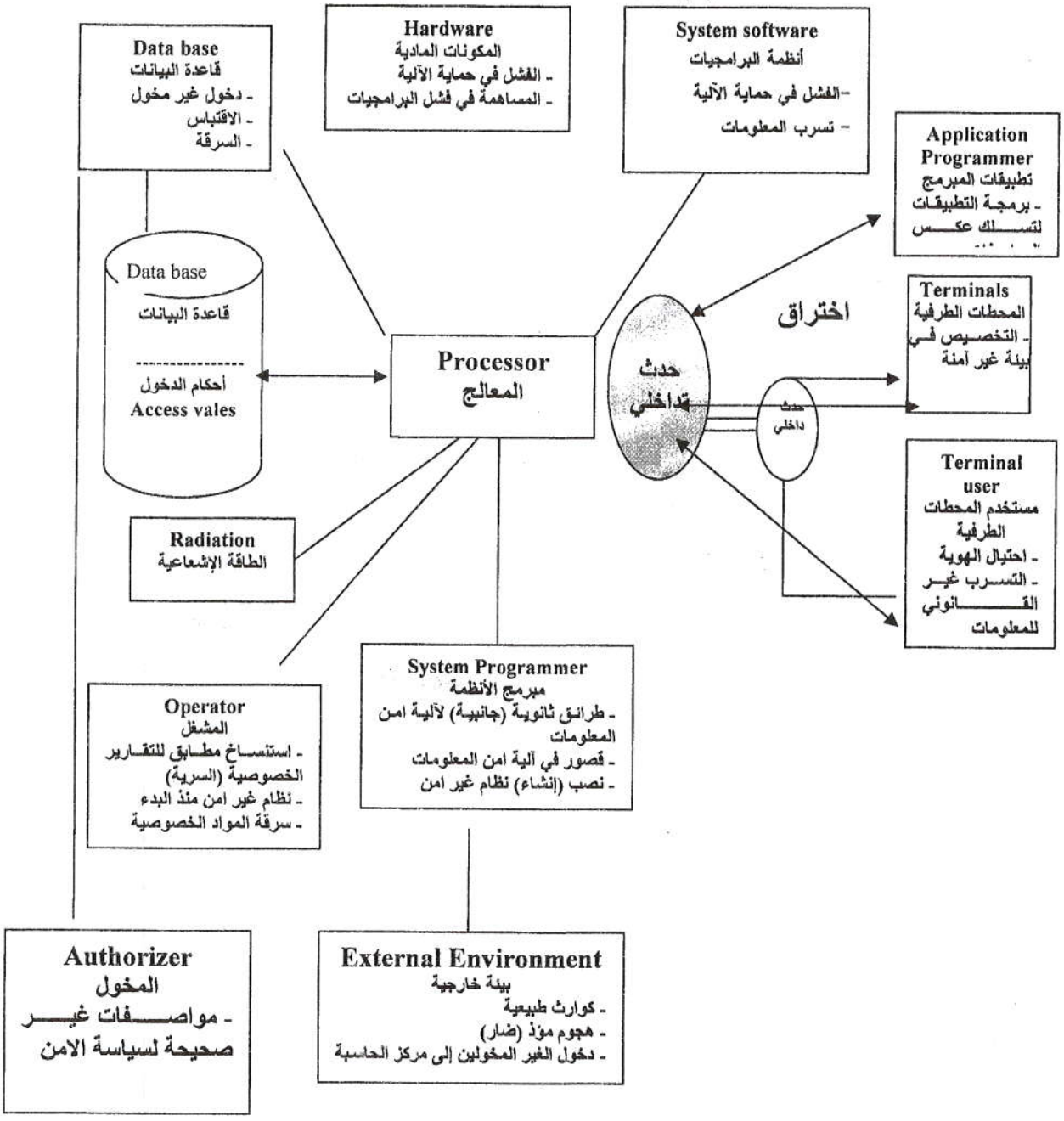
٩ .من الصعوبة تحديد الكلفة – المنفعة (العائد) (cost-benft) للرقابة على المعلومات قبل حدوث الهجوم مادامت انه من الصعوبة تقييم تكاليف الهجوم الافتراضي .

(Turban et al,1999:666)

أوضح (Turban et al,1999:662) أنواع التهديدات كما في شكل(٢)والتي يمكن تقسيمها إلى تهديدات غير مقصودة والتي يمكن تصنيفها إلى ثلاث فئات رئيسة وهي (أخطاء الأفراد ، المخاطر البيئية ، فشل أنظمة الكومبيوتر) ، وتهديدات مقصودة وتتضمن (سرقة البيانات ، الاستخدام غير الملائم للبيانات ، التخريب المتعمد ، الفيروسات .. الخ) . كما قسم (1999 , Steven , 473) أنواع التهديدات إلى نوعين رئيسيين هما : التهديدات غير المقصودة وتتضمن (خطأ المشغل ، قصور الأجهزة ، عيوب البرامجيات ، أخطاء البيانات ، الاداء غير

الملائم للنظام ، الضرر بالتسهيلات المادية ، المسؤولية القانونية) ، والتهديـدات المقصـودة الناتجة من (السرقة ، والتدمير والتخريب المتعمد) .

شكل (٢) تهديدات الأمن Security Threats



Source : Turban Efraim et al , Information technology for management 1999 : 662

والجدول (١) يوضح أنواع هذه التهديدات والظروف التي تزيد التعرض لها والتي يتم عرضها بايجاز :

جدول (١) انواع التهديدات والظروف التي تزيد التعرض للهجوم

	Type of Threat نوع التهديد	Condition that increase Vulnerability الظروف التي تزيد التعرض للهجوم
تهديدات أمن الحالات غير المقصودة Threats from Unintentional occurrence	١) operator error خطأ المشغل	- صعوبة في توقع كيفية عمل الانظمة في التطبيق وكيفية تكيف المستخدمين والاخرون معها . - الرضا الذاتي في افتراض ان النظام سيعمل كما هو مفترض . - عدم وجود الطاقة والاهتمام في ضمان عمل الانظمة .
	٢) Hardware malfunction قصور داخل الاجهزة	- عدم الايمان بامكانية قصور الاجهزة . - الصعوبة في اتخاذ القرار فيما اذا كان هناك خلل في نظام الانذار والاجهزة
	٣) Software bugs عيوب البرامجيات	- التصميم والاختبار غير الملائمين . - العوامل غير المتوقعة التي تؤثر على تشغيل النظام . - عدم القدرة على اثبات صحة البرامجيات .
	٤) Data errors اخطاء البيانات	- العيوب في الإجراءات . - عدم قابلية البرامجيات على اكتشاف الانواع العديدة من الاخطاء . - الاهمال وعدم الانتباه .
	٥) Inadequate system performance الاداء الغير الملائم للنظام	- التصميم الغير ملائم . - اعباء الذروة (peak load) غير المتوقعة (التحميل الزائد) او تباينات الطلب .
	٦) Damge to physical facilities الضرر بالتسهيلات المادية	- الدعم غير الملائم . - الامن المادي الغير الملائم المرتبط بالظواهر الطبيعية. - الحماية الغير ملائمة ضد فشل الانظمة الخارجية .
	٧) Liability المسؤولية القانونية	- الحدود الغير الملائمة على المسؤولية القانونية . - النوعية الغير الملائمة للنظام .
تهديدات من الحالات المقصودة Threats from intentional actions	٨) Theft السرقة	- التصميم الغير الملائم لنظام الحاسوب والمعالجة البشرية . - وجود العديد من الاهداف سهلة السرقة . - الانظمة الموزعة .
	٩) Vandalism and sabotage التدمير والتخريب المتعمد	- الوقاية غير المناسبة في الدخول غير المخول . - السيطرة غير المناسبة على تغيير البرامجيات . - الإجراءات التنظيمية الغير المناسبة .

Source : Alter steven , Information systems , 3th ed ., Addison wesley , 1999 : 473

(١) تهديدات الحوادث غير المقصودة :

وهي التهديدات او الخروقات التي يتعرض لها النظام ليس بقصد الاساءة او الحصول على معلومات وانما بسبب قلة الخبرة في مجال التعامل مع تكنلوجيا المعلومات وهذه التهديدات لاتقل خطورة عن غيرها خاصة اذا تسببت في ضياع او فقد المعلومات ، وهذه تتم على الاكثر من قبل أشخاص مخولين باستخدام النظام او قد تحدث بسبب استخدام النظام من قبل اشخاص غير مخولين للدخول الى النظام ، وقد تحدث الحوادث الغير مقصودة لافتراض العديد من الاشخاص بان نظم المعلومات ستعمل كما هي مصممة لكي تعمل ، وبأنها ستعمل بشكل موثوق به ، وعندما يثبت التطبيق بان هذه الافتراضات خاطئة فان النتائج يمكن ان تكون مدمرة .وهذه التهديدات ناجمة من سبعة اسباب رئيسة وهي: (١) خطأ المشغل .(٢) قصور (خلل) الاجهزة.(٣) عيوب البرامجيات.(٤) اخطاء البيانات (٥) الضرربالتسهيلات المادية (٦) الاداء الغير ملائم للنظام (٧) المسؤولية القانونية عن اداء النظام. وقد أغفل (Steven) التهديدات البيئية بالرغم من اهميتها . ولابد من الاشارة بانه لايفترض بان كل

نوع من الحوادث يسببه بشكل كامل العنصر الذي يرتبط به وتعد التفاعلات بين اسباب الحوادث نقطة اساسية للاستيعاب .

(٢) تهديدات الحوادث المقصودة :

وهي التي يمكن ان يتعرض لها أي نظام للمعلومات وتعد من الناحية الامنية اخطر من التهديدات الغير مقصودة لانها تمثل محاولات مقصودة من قبل اشخاص مخولين او غير مخولين باستخدام ذلك النظام وباستخدام شتى الطرق وبمختلف الوسائل للحصول على المعلومات او إتلاف محتوياتها. (Steven , 1999 , 467)

*** تهديد جريمة الحاسوب :**

ان جريمة الحاسوب هي استخدام انظمة الحاسوب للقيام باعمال غير قانونية ويمكن تقسيمها الى مجالين رئيسيين هما السرقة ، والتدمير ، والتخريب المتعمد ويزداد القلق بشأن جريمة الحاسوب بينما تصبح انظمة الحاسوب اكثر شيوعا، و قد اتضح تماما احتمال الضرر الكبير بالمصالح التجارية والدفاع الوطني من خلال الفيروسات Viruses في النظام ، من خلال البرمجيات المصابة Infected، المتطفلين parasiter ، والاشكال الاخرى من التخريب في الحاسوب المستخدمة لتعطيل النظام ، وتشويه ، وإتلاف ،او تخريب بياناته ووظائفه المختلفة. وعموما يمكن تقسيم مرتكبي جرائم الحاسوب الى موظفين وخارجيين ومتلاعبين ويسمى الشخص مرتكب الجريمة من الخارج بـ:(criminal hacker) بينما الشخص مرتكب الجريمة من الداخل يسمى بـcracker .وتصنف الهجمات التي تكون معرضة للهجوم في ضوء مناطق ومحل الحماية إلى أنواع وهي : خرق الحماية المادية ، وخرق الحماية المتعلقة بالأشخاص وشؤون الموظفين ، خرق الحماية المتعلقة بالاتصالات والمعطيات ،والهجمات المتصلة بعمليات الحماية . وتكشف العديد من الحالات التي تسمى جريمة الحاسوب بان الحاسوب لعب دورا صغيرا نسبيا مقارنة بدور الاجراءات المهملة ووثائق الصفقات المزيفة ، وكان يمكن ان تتوقف غالبية الحوادث من خلال الاجراءات الوقائية والتنظيمية الافضل.

*** السرقة :**

يمكن تقسيم السرقة المرتبطة بالحاسوب الى خمسة أنواع هي :

١. سرقة البرامجيات ومعدات الحاسوب ٢. الاستخدام الغير مخول (مرخص) لشفرات الدخول وكلمات السر٣. السرقة عن طريق ادخال بيانات احتيالية عن الصفقات .٤. السرقة عن طريق تعديل البرامجيات

٥.السرقة عن طريق اختلاس أو تعديل البيانات .

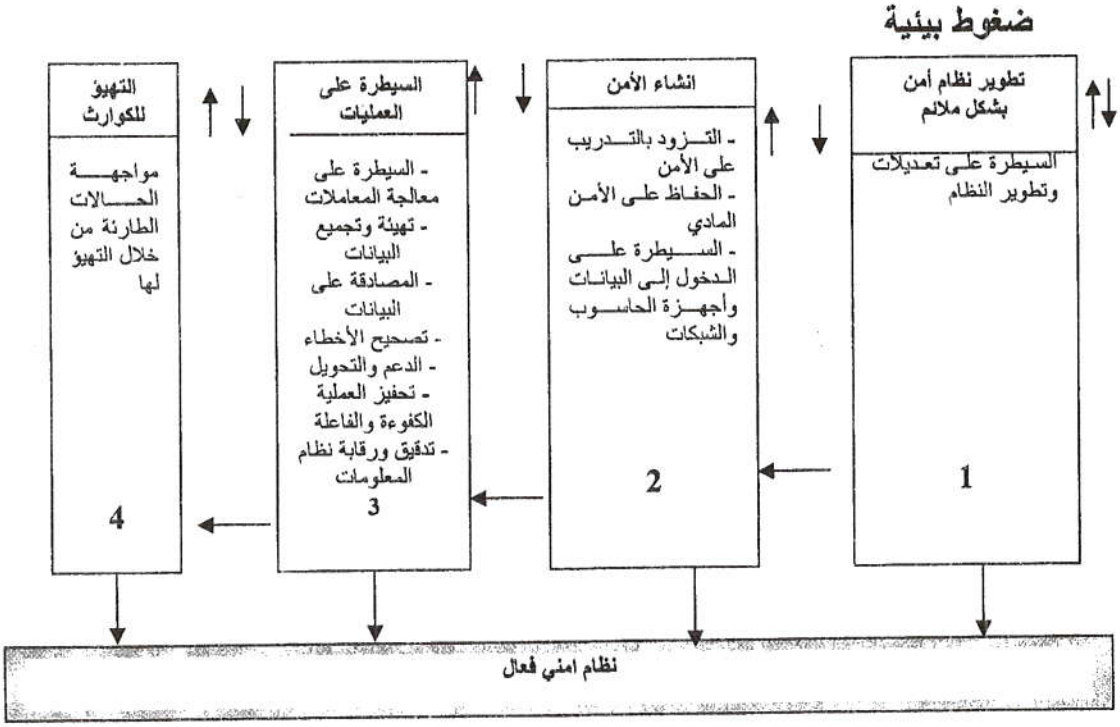
*** التدمير والتخريب المتعمد :**

يحاول مرتكبوا التدمير والتخريب المتعمد غزو أو تدمير أجهزة النظام وبرامجياته أو بياناته ، وقد يتراوحون من المتلاعبين الى الموظفين المستائين الى الجواسيس . وقد ولدت شبكة الانترنيت العديد من الاحتمالات للتدمير والتخريب المتعمد باستخدام العديد من تقنيات البرمجة للتدمير والتخريب منها الباب المسحور، حصان طروادة ، أبواب الشرك ، الفايروسات ، الديدان Worms ، القنابل المنطقية Logic Bombs ، وغيرها .

ثانيا : النموذج المقترح لمواجهة تهديدات النظام

يوضح الشكل (٣) النموذج المقترح لمواجهة تهديدات نظام امن المعلومات بما يحقق فاعليته .

شكل (٣) نموذج مقترح لنظام امني فعال



١)تطوير نظام أمن بشكل ملائم:

يمثل الهدف من أي برنامج أمن لنظام المعلومات حماية معلومات المنظمة لتقليل التهديدات التي قد تؤثر على سرية المعلومات ، وتوافرها وسلامتها ، بمستوى مقبول ومحدد ، وتتلخص المنطلقات والأسس التي تبنى عليها استراتيجية أمن المعلومات القائمة على الاحتياجات المتباينة لكل منظمة من الاجابة عن اربعة تساؤلات رئيسة وهي : ماذا تريد المنظمة أن تحمي ؟ من ماذا تحمي المعلومات ؟ كيف تحمي المعلومات ؟ ما العمل إن تحقق أي من التهديدات رغم وسائل الحماية ؟ إن اجابة التساؤل الأول يتطلب من المنظمة ووفقاً للأمن من برنامج الهدف أن تصنف البيانات والمعلومات من حيث أهمية الحماية ، إذ تصنف المعلومات تبعاً لكل حالة على حدة من معلومات لا تتطلب الحماية ، إلى معلومات

تتطلب حماية قصوى . كما أن على المنظمة أن تحدد عند انشاء النظام مناطق أمن المعلومات التي تتضمن بشكل عام ما يلي :

* أمن الاتصالات : ويراد به حماية المعلومات خلال عملية تبادل البيانات من نظام لآخر .

* أمن الكومبيوتر : ويراد به حماية المعلومات داخل النظام بكافة أنواعها : كحماية نظام التشغيل ، وحماية برامج التطبيقات وتدعو المحافظة على نوعية البرامجيات إلى ضرورة اخضاعها إلى الاختبار الدقيق قبل توزيعها في المنظمة فضلا عن استخدام برامج تلقيحية لتحديد وازالة الفيروسات ، وحماية برامج ادارة البيانات ، وحماية قواعد البيانات بأنواعها .

* أمن الأنترنيت : ويتركز على مواضع ثلاث هي : أمن الشبكة ، أمن التطبيقات ، أمن النظم ، وكل منها ينطوي على قواعد ومتطلبات تختلف عن الأخرى . ولا يحقق أمن المعلومات دون توفير الحماية المتكاملة لهذه القطاعات الثلاث أعلاه عبر معايير أمنية تكفل توفير الحماية الملائمة ومن خلال تعيين مستويات أمن متعددة منها (حماية مادية ، حماية شخصية ، حماية أدارية ، حماية إعلامية ، حماية معرفية) .

أما اجابة التساؤل الثاني فيحدد المخاطر (*) التي تتعرض لها المعلومات بتصور كل خطر يمس المعلومات محل الحماية ويهدد أمنها ، ويصار إلى تصنيف هذه المخاطر ضمن قوائم تبعاً لأساس التصنيف كما أشرنا إليه في متن البحث .

أما أجابة التساؤل الثالث فيتم من خلال تحديد وسائل الحماية وهنا تجد كل منظمة طريقتها الخاصة في توفير الأمن من التهديدات ، وتحدد متطلبات حماية المعلومات المخصوصة التي تم تحديدها وبحدود امكانياتها المادية والميزانية المخصصة للحماية ، ومن الضرورة أن لا تكون اجراءات الأمن المقترحة رخوة ضعيفة لا تكفل الحماية ، وبالمقابل لا تكون مبالغاً فيها إلى حد تؤثر عنصر الأداء لنظام أمن المعلومات ، وأخيراً فإن اجابة التساؤل الرابع وهو ما يعرف بخطط مواجهة التهديدات عند حصولها على الرغم من وسائل الحماية المتوافرة في المنظمة .

٢) انشاء الامن وتتضمن ما يلي :-

أ- **توفير التدريب على الامن** :إن مهام المتصلين بنظام أمن المعلومات تبدأ في الأساس من حسن أختيار الأفراد المؤهلين وعمق معارفهم النظرية والعملية ، على أمن يكون مدركاً أن التأهيل العملي يتطلب تدريباً متواصلاً ولا يقف عند حدود معرفة وخبرة هؤلاء عند تعيينهم ، ولذا ينبغي على المنظمات ان تدرب مستخدميها على ادراك الامور الامنية وفهم كيفية ارتباط

(*) المخاطر قد تستخدم بشكل مترادف مع تعبير التهديدات مع أنها حقيقة تتصل بأثر التهديدات عند حصولها .

هذه الامور بالقوانين والاجراءات. وينبغي ان يعرف كل موظف يستخدم الحاسوب او يشترك في معالجة الصفقات كافة القضايا المتعلقة بالنواحي الامنية ، وعلى المنظمة ان تضع التوجيهات الكافية لضمان وعي عام ودقيق بمسائل الامن ، والمطلوب ايضا بناء ثقافة الامن Culture security لدى العاملين والتي تتوزع بين وجوب مراعاة أخلاقيات استخدام التقنية وبين الاجراءات المتطلبة من الكل لدى ملاحظة أي خلل وعلى المنظمة ان تحدد للعاملين ما يتعينن عليهم القيام به ، والاهم ما يحظر عليهم القيام به عند استخدامهم للوسائل التقنية المختلفة.

ب- المحافظة على الامن المادي :تعد المحافظة على الامن المادي امرا اساسيا لحماية تسهيلات الحاسبات والاتصالات وينبغي ان تاخذ اجراءات الامن المادي بنظر الاعتبار التهديدات بضمنها الاحداث والحوادث الخارجية التي لايمكن السيطرة عليها والهجوم من المتطفلين . وتحافظ السيطرة على الدخول المادي من الدخول المادي الى البيانات وتسهيلات الحاسوب والدليل العام هو ابعاد الاشخاص غير المخولين من غرف الحاسوب ، مراكز الاتصالات ، ومواقع خزن البيانات ، ويمكن ان يتم ذلك باستخدام وسائل حماية التعريف التي تهدف من التثبت من الهوية . وتبذل الشركات ما بوسعها لحماية معالجة البيانات الحاسمة وقد ادى القلق بشان الامن المادي لنظام الحجر بالخطوط الجوية الامريكية الى بناء تسهيلات تحت الارض في (Oklahma , Tuisa) .

جـ- السيطرة على الدخول الى البيانات واجهزة الحاسوب والشبكات : بعد توفير الامن المادي فانه من الضروري تحديد الاجراءات الامنية للدخول الى المعلومات السرية وفرض القوانين الاساسية الاجبارية وهذه تتضمن وسائل السيطرة على الدخول ،ووسائل السرية ، ووسائل منع الأنكار ويلخص الجدول (٢) جوانب السيطرة على الدخول إلى البيانات وأجهزة الحاسوب والشبكات .

جدول (٢) السيطرة على الدخول الى البيانات واجهزة الحاسوب والشبكات

تقنية السيطرة Control technique	مثال Example
فرض ادلة معالجة البيانات اليدوية (الارشادات)	قفل المكاتب تمزيق الكراسات والوثائق المرمية
تحديد امتيازات الدخول	- اعطاء اشخاص مختلفين مستويات مختلفة الامتياز لاستخدام الحاسوب - اعطاء اشخاص مختلفين مستويات مختلفة الدخول الى ملفات بيانات معينة
فرض امتيازات الدخول - ماذا تعرف - ماذا تمتلك - مكانك / اين انت - من انت	البيانات الشخصية الخاصة - بطاقة الهوية - المفتاح الى التسهيلات المادية (Physical facility) - استدعي نظام الاتصال ثانية - بصمة الاصبع او بصمة اليد - نموذج الشبكية - نموذج الصوت
السيطرة على البيانات الواردة من الشبكات والاوساط الاخرى	- استخدام جدران النار - فحص الفايروسات
جعل البيانات غير مفهومة لاي شخص ليس لديه تخويل	- ترميز البيانات

Source : Steven , Alter, information systems , Management perspective , 3th ed . 1999 : P477

٣- السيطرة على العمليات :

وتتضمن كلا من السيطرة على معالجة المعاملات ، والحث على العملية الكفوءة والفاعلة ، وتدقيق ورقابة نظام المعلومات .

أ- السيطرة على معالجة المعاملات :

تبدأ السيطرة على معالجة المعاملات (الصفقات) بجمع البيانات وتتضمن الطريق التي تعالج فيها اجهزة الحاسوب البيانات والطريقة التي تصحح فيها الاخطاء. وتتضمن نقاط السيطرة (تهيئة وتجميع البيانات ، المصادقة على البيانات ، تصحيح الاخطاء ، الدعم والتحديث) .

١- تهيئة وتجميع البيانات :

وهي عملية اساسية لدى بناء أي نظام أو بيئة أي نشاط تتعلق بالمعلومات وتولد هذه العملية بيانات المعاملة التي ستدخل في نظام معالجة المعاملات ، وتوضح قصة شركة (Equity funding) اهمية السيطرة على تهيئة البيانات فخلال (١٥) سنة تعاون (تآمر) الموظفون ومبرمجو الحاسوب لجعل الشركة تبدو في مسار نمو سريع عن طريق اصدار ٦٠٠٠ بوليصة تامين مزيفة تمثل ٦٥% من المجموع الكلي للشركة وقد بعثت البوليصات المزيفة الى شركات اعادة التامين . ويعد فصل الواجبات منهج سيطرة تجعل من الصعب ارتكاب جرائم الشخص الواحد وجرائم التآمر .

٢- المصادقة على البيانات :

تشير المصادقة على البيانات الى فحص بيانات المعاملات لايجاد اية اخطاء اوحذف يمكن اكتشافها عن طريق النظر الى البيانات وتكون بعض تدقيقات المصادقة واضحة وبسيطة من حيث تتطلب تدقيقات اخرى معالجة اكثر تعقيدا . وتتطلب عمليات المعلومات اتباع نظام لتوثيقه مع كافة وسائل المعالجة والتبادل وإن ذلك يعتبر ضروري لنظام التعريف والتخويل .

٣- تصحيح الاخطاء :

ان تصحيح الخطأ هو مكون اساسي لاي نظام لمعالجة المعاملات لانه من المستحيل ضمان صحة كل البيانات في النظام بغض النظر عن مدى دقة المصادقة على البيانات عندما أدخلت لأول مرة . ومن المثير للدهشة ان تصحيح الخطأ في العديد من نظم معالجة المعاملات (Transaction processing system)TPS يكون معقدا بسبب احتمالية الاحتيال ولغرض السيطرة عليها يعالج تصحيح الخطأ كمعاملة منفصلة تسجل وتفسر

٤- الدعم والتحديث :

ان الخطوة الاخيرة في السيطرة على معالجة العمليات هي التأكد من انه كلما تعطل نظام حاسوب فان المعالجة الاعتيادية ستبدأ من جديد بحد أدنى من الضرر وعدم الراحة. ويجب مراعاة النقاط التالية في خطة استعادة النشاط للشركة (انور ، ١٩٩٠ : ٤٣) وهي :-

- بساطة الاجراءات بحيث تحول مهام الاستعادة المعقدة الى خطوات واضحة
- تحديد الاجراءات التي يمكن تنفيذها بالتوازي وتلك التي يجب تنفيذها بالتعاقب .
- الاختبار الدوري لاجراءات استعادة النشاط .
- توفير مستوى من المرونة والتناسق في الاجراءات .
- ان تكون الاجراءات قابلة للقياس .

ب- تحفيز العملية الكفوءة والفعالة :

ان الجانب الاخر للسيطرة على العمليات هو خلق الحوافز للعملية الكفوءة والفعالة وخاصة عن طريق مراقبة استخدام نظام المعلومات واستخدام الاسعار لتحفيز الكفاءة . ان نظم المعلومات المصححة بشكل جيد لابد من احتواءها على مقاييس اداء لكل من عملية الاعمال (Business Process) الداعمة ولنظام المعلومات ذاته . فمثلا لو تمعنا في نظام معلومات خدمة الزبون في شركة تسويق عن بعد فانه يتضمن مقاييس لنتائج الاعمال مثل (المبيعات في الساعة ، وقت انتظار الزبون للتحدث الى الوكيل) ، كما قد يحتوي على مقاييس لكفاءة نظام المعلومات مثل (وقت التعطل عن العمل ، معدل الاستجابة على أسئلة قاعدة البيانات ، كلف تشغيل الاسبوعية ....الخ) . ومن الضرورة ان يتضمن عرض المؤشرات معرفة الجميع باهميتها وادراكها لجودة عمل المنظمة. وقد يؤدي عدم وجود مقاييس ممكنة للعديد من انظمة الحاسوب بالمستخدمين الى تجاهل كلفها واستخدامها بشكل غير كفوء واحيانا سوء الاستخدام ، وهذا هو احد الاسباب الموجبة لفرض الاسعار لتحفيز الاستخدام الكفوء عن طريق تحديد كلف نظام المعلومات لاقسام المستخدم .

جـ- تدقيق نظام المعلومات :

تصمم المقاييس لضمان عدم تشويه او تهديد العمليات. ويمكن تصنيف المناهج للتحقق من مراحل المعالجة على انها التدقيق حول الحاسوب ، او التدقيق من خلال الحاسوب . ففي التدقيق حول الحاسوب يختار المدقق عادة وثائق المصدر ويتعقب المداخل المرتبطة من خلال المطبوعة المتوسطة للحاسوب ، ويفحص المداخل الناتجة في تقارير موجزة . اما التدقيق من خلال الحاسوب يحاول المدقق فهم واختبار معالجة الحاسوب بتفصيل اكبر ويتبغي ان يدرس المدققون ايضا قضايا مثل الدخول غير المخول والسيطرة على ملفات البيانات وعلى نقل البيانات واجراءات التجديد عندما يتعطل نظام المعلومات بشكل غير متوقع .

٤- التنبؤ للكوارث (مواجهة الحالات الطارئة) :

لا تكتمل عملية مواجهة الاخطار الا اذا توفر لدى المنظمة خطة كاملة ومتكاملة لمواجهة الحالات الطارئة التي تهدف الى منع حدوث الخسائر او تقليلها الى ادنى حد ممكن في حالة وقوع حالة طارئة ، ويجب اعتماد خطة طوارئ رسمية مصادق عليها من قبل الادارة العليا وتكون محتوية على تفاصيل مكتوبة لمواجهة كل نوع من الحالات الطارئة . ان خطة الكوارث هي خطة اجرائية للتخلص من الحالات التي قد تعطل او تضر نظم المعلومات الرئيسية ، وتتضح الحاجة الى مثل هذه الخطة من التأثير المحتمل للحوادث والتخريب والحوادث الطبيعية مثل الفيضانات او الهزات الأرضية وغيرها . وتعتمد طبيعة ومدى خطة الكوارث لنظم المعلومات للاعمال على دور نظم المعلومات في العملية اليومية للاعمال .

المبحث الثالث

الخلاصة والتوصيات

من خلال ما تم عرضه في البحث لاحظنا زيادة التهديدات التي تتعرض لها مصادر المعلومات وكذلك صعوبة اكتشاف او تتبع التغيرات التي تطرا على المصادرالمعلوماتية بسبب تشعب وتعقد النظم . كما تبين لنا ان الكثير من التهديدات التي يتعرض لها نظام أمن المعلومات تكون بسبب سوء استخدام الحاسوب نتيجة للاخطاء غير المقصودة والاجراءات الخاطئة او غير الكافية المستخدمة في التطبيق .

وبناء على ذلك يمكن ان نقدم بعض التوصيات :

١- رصد التجارب والممارسات الناجحة الدولية والعربية منها فيما يخص ادارة نظام امن المعلومات بهدف دراستها والاستفادة منها والوقوف على عوامل نجاحها والصعوبات والمعوقات التي تواجهها والعمل على وضع آلية قابلة للتطبيق في ضوء خصوصية منظماتنا العراقية وبيئتها المحلية .

٢- العمل على بناء بنية تحتية معلوماتية (infrastructure information) كمطلب أولي لابد منه من اجل استخدام أنظمة المعلومات الرقمية(Digital information) بكفاءة وفاعلية .

٣- وجود منهجيات تستند على ثقافة المعلومات كسلوك والتي تعني فهم وادراك المعلومات كثروة في مجتمع المعلومات والمعرفة لضمان النجاح المستمر في اداء منظماتنا لعملها واعطاء مكانة متميزة لقطاع المعلومات وامنه في البلد.

٤- تنمية رأسمال الفكري لمنظماتنا وخاصة للعاملين في مجال النظم المعلوماتية الحاسوبية والعمل على اشراك العاملين في مجال الحاسبات ببرامج تدريبية في مجال أمن المعلومات .

٥- العمل الدؤوب على بناء الثقة (Building confidence) لمستخدمي نظم المعلومات وتطبيقاتها وطبقا لاستراتيجية الامن المتبعة .

٦- ضرورة ديمومة المراجعة والرقابة والتقويم لنظم امن المعلومات ومجابهة حالات الاختراق اول باول والعمل على تحديث النظام مع تغيير احتياجات الاعمال .

٧- من الملاحظ ان تطور الاوجه القانونية والتشريعية لا تكون دائما بخطى متوازنة مع التقدم التكنولوجي لذلك نوصي بضرورة احداث التوازن المطلوب بينهما فضلا عن تناسق وانسجام القوانين والتشريعات المرتبطة بنظم المعلومات .

٨- خزن نسخ من البرامج والوثائق والبيانات في مراكز الاسناد.

٩- الاعتماد على العناصر الجيدة في مجال العمل الخاص بامن المعلومات وادامة كفاءتهم واخلاصهم من خلال تقديم مختلف انواع الحوافز .

١٠- الوقاية من مخاطر الاعتداء على المعلومات من خلال خدمات حماية التعريف ، خدمات السيطرة على الدخول ، الخدمات السرية ، خدمات حماية التكاملية وسلامة المحتوى ، خدمات وسائل منع الانكار ..... الخ .

١١- التهيوء للحالات الطارئة ووضع الخطط اللازمة لمواجهتها .

١٢- الدعم المتواصل من قبل الإدارات العليا لحماية وتامين المعلومات، بحيث تصبح لها الاولوية في تخطيط وعمل نظم المعلومات على كافة انواعها وتوجهاتها .

١٣- ضرورة أن تكون استراتيجية أو سياسة الأمن موثقة ومكتوبة .

المراجع References

المراجع العربية

١- انور ، سلوى ، امنية البيانات ، المركز القومي للحاسبات الالكترونية ، بغداد ، ١٩٩٥ .

٢- السالمي ، علاء عبد الرزاق ، تكنولوجيا المعلومات ، الطبعة الثالثة ، دار المناهج للتوزيع والنشر ، الاردن ، ٢٠٠٠ .

٣- فضل الدين ، عبد القادر ، الحماية والسيطرة على البيانات تجاه الاشخاص المخولين ، رسالة ماجستير غير منشورة مقدمة الى معهد الدراسات العليا للحاسوب والمعلوماتية ، المركز القومي للحاسبات ، بغداد ، ١٩٩٥ .

٤- الطائي ، محمد عبد حسين ، نظم المعلومات الادارية ، الطبعة الثانية ، وزارة التعليم العالي والبحث العلمي ، دار الكتب والطباعة والنشر ، موصل ، ٢٠٠٠ .

المراجع الاجنبية

1- Steven ,Alter , Information system , A management Perspective , 3th ed , Addison , Wesley , 1999 .

2- O'Brien , James A, management Information system , Amanagemerial End user Perspective , IRWIN , 1990 .

3- Turban , Efraim and Mcler , Ephraim , and wetherbe James , Information Technology for management , making connection for strategic Advatage , 2nd ed , John Wiley & sons . INC . 1999 .

4- Turban , Efraim et al , Introduction to Information Technology , John Wiley & sons INC , 2001.

5- I . F . A . C . International fedration of Accountauts Managing security of Information , No . 1 . Jan . , 1998 .

6- Gelbstein,Eduardo and Kamal , Ahmed , Information security, Asurvival Guide to the uncharted Territories of cyber , New York , UN ICT , 2005 .

الانترنيت Internet

1- WWW. Itrain online org.

2- http://WWW.common criteria.org

3- http://WWW. Information security .com.

4- http://ar.wikpedia . org.

5- http://information.net /ir/ paper

6- http://WWW. Information accountants .com

7- ISO 15408 common criteria for information security Evaluation (http://WWW.common criteria. Org.)

ISO 13353 : Afive part set of Guidelines for the management of information security

ISO 177799 code of practice for managemental of information security .

8- WWW.arablaw.org.information security.com.

9- INTOSAI. EPP- Audit committee (international organization for supreme institution), Information system scurity review methodology : Aguide for reviewing information system scurity in government organizations , October 1995 .