بسم الله الرحمن الرحيم

نموذج لتقييم
أمن المعلومات المحاسبية فى النظم الالكترونية

د. سمير رياض هلال*

مقـــدمة

أصبح أمن المعلومات التى تحتويها النظم الالكترونية، وخاصة المالية والمحاسبية،موضع اهتمام وقلق لإدارات المؤسسات والمنشآت التى تستخدم هذه النظم،ولمراجعى الحسابات الذين يقومون بفحصها ومراجعة البيانات المالية المستخرجة منها لإبداء الرأى فى مدى سلامتها. ويرجع هذا القلق إلى تزايد أنواع واحتمالات المخاطر المحيطة بهذه النظم والتى تهدد صحة وموثوقية وسرية وتكامل البيانات المالية والمحاسبية فيها ، وذلك نتيجة لعوامل منها:

١- التقدم التقنى فى صناعة الحاسبات ، وزيادة وتنوع البرامج المتاحة أدى الى سهولة نسخ وتعديل وتغيير البيانات والملفات فى أوقات قياسية وبسيطة لا تستطيع ضوابط الحماية (الرقابة) التقليدية متابعتها.

٢- زيادة خبرة الأفراد ،بصفة عامة، فى استخدام الحاسبات الآلية نتيجة لانخفاض أسعارهاوإنتشارها فى مجالات متعددة، أدى إلى سهولة التغلب على الوسائل التقليدية لتأمين المعلومات فى النظم الإلكترونية.

٣- إتصال نظم المعلومات الإلكترونية ببعضها البعض من خلال شبكات الإتصال العامة (الهواتف مثلا) ، أتاح فرصة للمغامرين للدخول إلى شبكات معلومات محلية وعالمية ، والتلاعب فى بياناتها.

وقد نتج عن هذه المخاطر حوادث تضمنت تدمير وسرقة والتلاعب فى البيانات والملفات مما أدى إلى خسائر كبيرة للشركات والمؤسسات تجاوزت مئات الملايين من الدولارات فى الولايات المتحدة فقط[١] . فمثلا بلغت تقديرات الخسائر الناتجة عن هذه الحوادث ، نصف مليون دولار فى المتوسط لكل حالة من إجمالى ١٤٠٦ حالات تم دراستها[٢] . وأخيرا فإن شركة IBM نفسها، وهى التى تملك تقنيات الصناعة ووسائل الأمن، قد تعرضت لخسائر قدرت بمبلغ ١١ مليون دولار فى عام ١٩٨٧ من حوادث مشابهة[٣] .

---

* أستاذ مساعد بقسم التكاليف ونظم المعلومات - جامعة طنطا

ومع إتساع هذه الظاهرة، إتضح عدم كفاية الأساليب المستخدمة حاليا فى تقييم محددات أمن المعلومات، وهى المخاطر المحيطة بالنظام المحاسبى الإلكترونى،وضوابط الحماية (الرقابة)المصممة لمواجهة تلك المخاطر. وظهرت الحاجة الى إيجاد مقياس كمى منهجى يساعد المراجع الداخلى(الإدارة) فى تحليل وتقييم المخاطر المحيطة بالنظام، وتقديرالخسائر المحتملة من هذه المخاطر .كما تساعد المراجع الخارجى فى الحكم على مدى مأمونية المعلومات المحاسبية، وعناصر أو عمليات النظام المطلوب التوسع فى نطاق فحصها.

أهداف البحث

يهدف هذا البحث إلى تقديم نموذج لتقييم محددات أمن المعلومات في النظام المحاسبى الإلكترونى عن طريق تحليل المخاطر المحيطة بالنظام وتقدير حجم الخسائر المتوقعة من هذه المخاطر، وذلك كأحد المداخل غير المباشرة لتقييم كفاءة الرقابات (ضوابط الحماية)فى النظام.

منهج وحدود وأهمية الدراسة

هذه دراسة تحليلية تقدم نموذجا نظريا لتحليل المخاطر التى تصمم لها الرقابات فى النظام المحاسبى الإلكترونى وتتضمن مثالا بأرقام إفتراضية لتوضيح كيفية تطبيق النموذج. وترجع أهمية هذه الدراسة إلى عدم كفاية الطرق المستخدمة حاليا لتقييم أساليب الرقابة (ضوابط الحماية) فى النظم المحاسبية الإلكترونية ، وتقدير الخسائر المحتملة من ضعف هذه الرقابات أو الضوابط، حيث أن هذه المعلومات ضرورية وأساسية للمراجع الداخلى (الإدارة) لتقييم جدوى إضافة ضوابط لحماية المعلومات المحاسبية فى النظام الإلكترونى .كما يعتبرهذا النموذج مفيدا للمراجع الخارجى عند تقييمه لمأمونية المعلومات وإحتمالات تلويثها ، وكذلك للحكم على" كفاية Adequacy" الرقابات أو ضوابط الحماية في النظام المحاسبى، كما تتطلبها معايير المراجعة، لما لذلك من أثر على تخطيط برنامج المراجعة من حيث نطاق الفحص والوقت اللازم لذلك.

محتويات الدراسة

تنقسم بقية هذه الدراسة إلى قسمين : الأول يعرض الطرق الشائعة فى تقييم أمن المعلومات المحاسبية فى النظم الإلكترونية .أما الثانى فيقدم النموذج المقترح

لتقييم محددات أمن المعلومات المحاسبية ، ثم توضيح إجراءات تطبيق هذا النموذج من خلال مثال رقمى.

القسم الأول
الطرق الشائعة فى تقييم محددات امن المعلومات المحاسبية فى النظم الإلكترونية

يقصد بأمن المعلومات Information Security ، درجة الحماية التى تتوفر لأجهزة الحاسب الالكترونى وما يدخل إليها من بيانات وبرامج وما يحفظ فيها من معلومات، وتتحدد درجة أمن المعلومات فى النظم الالكترونية،ومنها المالية والمحاسبية ، بأنواع التهديدات والمخاطر Threats التى يتعرض لها النظام وكذلك بطبيعة وكفاية إجراءات الرقابة (ضوابط الحماية controls) التى تتخذها إدارة المنشأة ضد هذه المخاطر.

ويمكن تقييم أمن المعلومات من خلال تقييم هذين العاملين(المحددين) وهما الرقابات والمخاطر. فالتركيز على تحليل وتقييم الرقابات عادة ما يكون منهج المراجع الخارجى إذ تنحصر مهمته، طبقا لمعايير المراجعة، فى التقرير عن مستوى أداء هذه الرقابات (AICPA, 1974,SAS, No.3) . أما التركيز على تحليل المخاطر والخسائر المتوقعة منها فهو منهج الإدارة (المراجع الداخلى) حيث يؤدى هذا المدخل ليس فقط لتحديد ضعف الرقابات بل أيضا لتوفير معلومات جيدة لإقتراح رقابات إضافية ذات جدوى أمنية وإقتصادية. على أنه يجب التأكيد على أن كل من المدخلين سيتعرض لكلا العاملين (رقابات ومخاطر) .ففى مدخل تقييم الرقابات، عادة ما يتم تقسيم ضوابط الحماية (الرقابة) على النظام المحاسبى الالكترونى إلى رقابات عامة General (Environmental) Controls ورقابات تطبيقات Application Controls ، وبينما تتعلق الأولى باجراءات حماية بيئة نظام المعلومات بصفة عامة مثل حماية الأجهزة والمعدات، وتحديد صلاحيات استخدام النظام، وطرق تطوير وتشغيل وصيانة البرامج والتعامل مع ملفات البيانات بصفة عامة ، فإن الأخيرة تتعلق باجراءات استخدام وتشغيل تطبيقات (نظم) أو برامج معينة كالرواتب، أو حسابات المخازن، أوفواتير البيع[٤]. وبضعف أى من هذين النوعين من الرقابة يصبح النظام أكثر عرضة Vulner-able للمخاطر Threats التى قد تحدث ضرراً للبرامج والبيانات الموجودة فى النظام.

أول طرق التقييم هى قائمة التدقيق والمراجعة Check List Method وفى هذه الطريقة تستخدم قائمة تتضمن ضوابط الحماية (الرقابة) على النظام المحاسبى

الإلكترونى، سواء كانت رقابة عامة أو رقابة تطبيقات[٥]. ثم يقوم المراجع بدراسة النظام لتقييم ما إذا كانت الخاصية (وسيلة الرقابة) بالنظام كافية (Yes) أم غير كافية (No) . ويستخدم المراجع هذه القائمة لتقييم مدى كفاية الرقابات بصفة عامة. وحيث لا توجد منهجية محددة لذلك، فقد ينشأ إختلاف جوهرى بين المراجعين فى تقييم درجة حماية النظام . كما يصعب فى ظل هذه الطريقة إقتراح أية ضوابط إضافية لعدم تحديد المخاطر التى تتطلب ذلك ولا الخسارة التى تبرر هذه التكلفة.

أما الطريقة الثانية فهى **طريقة الجداول Tabular Forms Method** وتعتمد هذه الطريقة أيضا على تقدير كفاية إجراءات الرقابة . ولكن تختلف عن سابقتها فى أن التقديرات تأخذ شكل مصفوفة تعبر صفوفها عن خصائص الرقابة (ضوابط الحماية)، بينما تعبر الأعمدة عن المراحل المختلفة لعمل للنظام : مدخلات، تشغيل، مخرجات[٦] وعلى المراجع دراسة النظام وتقدير نسبة مئوية تعبر عن كفاية الرقابة فى كل خانه من خانات المصفوفة.ويلاحظ على هذه الطريقة أيضا أنها لا توفر مقياسا عاما لكفاية الرقابة، أو لأمن المعلومات فى النظام، ربما لعدم وجود أوزان محددة يستخدمها المراجعون فى تجميع بيانات المصفوفة المشار إليها.كما أنها لا تقدر الخسائر المحتمل حدوثها من عدم كفاية هذه الرقابات.

ثم هناك نموذج **" كفاية" الرقابة Adequacy of Control Method.** وترتكز هذه الطريقة[٧]. على إعادة تعريف " كفاية Adequacy" الرقابة الداخلية والتعبير عنها بأربعة خصائص للكفاية هى : الأهمية النسبية Materiality ، إمكانية (سهولة) الإستخدام Accessability، الحساسية (أثر العملية أو النشاط الرقابى) Sensitivity ، وأخيراجدوى التكلفة لعنصر الرقابة Cost effectiveness .ويقوم المراجع بدراسة النظام وعمل تقديرات (مقبول، وغير مقبول)لتغذية خلايا مصفوفة التقييم، والتى تمثل أعمدتها هذه الخصائص الأربعة، وصفوفها وسائل وإجراءات الرقابة (الحماية) الداخلية كما وردت فى معيار المراجعة رقم (٣) والتى تبلغ ٢٣ خاصية أو إجراء.

ويتم بعد ذلك تحليل بيانات الصفوف وبيانات الأعمدة كل على حدة.ففى تقييم **الصفوف** (أى تقييم العنصر أو الإجراء الرقابى) يكون عنصر الرقابة مقبولا أوكافيا إذا حصل على (مقبول) فى ثلاث خصائص على الأقل Rule of thumb . أما فى تقييم **الأعمدة** (أى خصائص كفاية الرقابات) فيتم تقييم كل خاصية على حده .

فمن حيث وقوع الأخطاء الجوهرية Material errors ، يقوم المراجع بتقييم كل إجراء رقابى على حده ثم يصدر حكما عاما على إحتمال وجود أخطاء جوهرية فى النظام وإمكانية تصحيحها وتكلفة ذلك. ومن حيث سهولة (إمكانية) الإستخدام Accessability ، فتقدر بأنها كافية إذا كان ٧٥٪ من العناصر أو الإجراءات سهلة الإستخدام. أما من حيث حساسية العمليات Sensitivity ، يتم تقييم كل إجراء على حده ثم يصدر المراجع حكما كليا على مدى حساسية الإجراءات فى النظام ككل. وأخيرا من حيث جدوى(فعالية)التكلفة Cost Effectiveness ،تعتبر مقبولة إذا كانت تكلفة ٧٥٪ من عناصر أو إجراءات الرقابة مقبولة. وهذا النموذج أيضا لا يؤدى الى مقياس كلى لكفاية الرقابة يمكن بواسطته الحكم على مستوى (درجة) أمن المعلومات بصفة عامة. كما أن تحديد نسبة ٧٥٪ كمستوى كفاية لضوابط الحماية لا يستند إلى أسس واضحة، بالإضافة الى أن النموذج لا يوفر بيانات عن التكلفة تبرر للإدارة إقتراح إنشاء ضوابط حماية إضافية

الطريقة الأخيرة هى "نموذج الرقابة الداخلية" The Internal Control Model (TICOM) وهذا النموذج تم تصميمه فى شكل برنامج على الحاسب الآلى، أى نظام خبير Expert System يقوم بتحليل بيانات معينة عن عناصر النظام المحاسبى الإلكترونى وإجراءات وقواعد تشغيل النظام [٨]. ويتم التحليل فى هذا النموذج على مرحلتين : الأولى وصف ونمذجة Modelling النظام بعناصره واجراءاته، والثانية تحليل ضوابط الرقابة فيه وتقييم كفاءتها وتحديد المخاطر التى لا تغطيها الرقابات الحالية. وهذا النموذج لا يأخذ فى الإعتبار المخاطرالتى قد يتعرض لها النظام من خلال غزو تقنى خارجى كالبرامج الجرثومية والإتصال بالشبكات، وسرقة البيانات.

من استعراض الطرق السابقة لتقييم رقابات (ضوابط حماية) النظم المحاسبية الإلكترونية بواسطة المراجعين، يتضح ما يلى:

١- تقتصر هذه الطرق على التأكد من وجود رقابات معينه فى النظام المحاسبى الإلكترونى وفى ذلك تركز على رقابات التطبيقات وليس على رقابات البيئة (أو الرقابات العامة)التى تتعلق أكثر بالمخاطرالتشغيلية والبيئية النظام. ،وقد يرجع ذلك الى أن الأخيرة تتعلق بعوامل ومجالات فنية بطبيعتها، ويتطلب تقييمها معرفة وخبرة بالنواحى الفنية فى الحاسبات الآلية قد لا تكون متوفرة لدى المراجع [٩].

٢- لا تبدأ هذه الطرق بحصر وتحليل المخاطر كمدخل لتحليل الرقابات مما يحصر

إهتمامها فى ما يمكن أن يسمى رقابات أساسية "Key controls" ، وليس النظام الكامل للرقابة أو الحماية Total System of Controls (Security) .

٣- لاتؤدى هذه النماذج إلى مقياس كمى لمستوى الرقابات (ضوابط الحماية) والذى يمكن ترجمته أو الإستدلال منه على مستوى المخاطر التى لا تواجهها هذه الرقابات.

٤- لا توفر هذه النماذج تقديرات للخسائر المتوقعة من نقص أو عدم كفاية الرقابات ، مما يجعل من الصعب معرفة ملاءمة تكلفة إنشاء ضوابط إضافية.

وكما يتضح فإن هذه الطرق لا تمثل منهجا شاملا لتحليل وتقييم أمن المعلومات فى النظام المحاسبى الإلكترونى بخاصتيه الأساسيتين: المخاطر وضوابط الحماية. ، ومن هنا تظهر الحاجة إلى نموذج يكون مدخله تقييم المخاطر المحتمل وقوعها للنظام، والخسائر المترتبة عليها، حتى يمكن إقتراح ضوابط ذات جدوى فنية وإقتصادية.

القسم الثانى
نموذج مقترح لتقييم محددات امن المعلومات
فى النظام المحاسبى الالكترونى

يرتكز النموذج المقترح لتقييم ضوابط حماية البيانات فى النظام المحاسبى الإلكترونى على مفهوم تحليل الخطر Risk Analysis* والذى يمكن تعريفه بأنه فحص منظم لبيئة ونظام المعلومات لتحديد المخاطر المتوقعة على النظام، واحتمالات حدوثها، والخسائر التى قد تنتج عن هذه المخاطر، وهذا النموذج يمثل أسلوبا منهجيا ومقياسا كميا لإحتمالات المخاطر المحيطة بالنظام، والخسائر المتوقعة من هذه المخاطر. ويهدف تحليل الخطر إلى:

١ - تحديد وتقييم أنواع واحتمالات الأحداث الضارة بالنظام ،

٢ - تقدير الخسائر المحتمل وقوعها من جراء هذه الأحداث،

٣ - تكوين مجموعة مدروسة من القواعد والمعايير لتصميم ضوابط فعالة وكافية لتقليل إحتمالات هذه المخاطر والخسائر.

---

* يعتبر تحليل الخطر المرحلة الأولى فى مفهوم أوسع هو إدارة الخطر Risk Management . فبينما يقتصر تحليل الخطر على عمليات تشخيص وتحديد احتمالات المخاطر التى تهدد النظام والخسائر التى قد تنتج عن ذلك، يمتد مفهوم إدارة الخطر إلى تصميم وتطبيق اجراءات الأمن والرقابة اللازمة لحماية المعلومات والنظم من هذه المخاطر المحتملة.

ولكى تتحقق هذه الأهداف يجب أن يكون تحليل الخطر شاملاً Comprehen-sive بمعنى أن يغطى كافة الجوانب البيئية والفنية لنظام المعلومات . كما يجب أن تكون هذه النتائج مفهومة Understandable سواء للمراجع أو للإدارة حتى يمكن تقييمها دون لبس أو خطأ. كما يحتاج تطبيق تحليل الخطر إلى خبرات متعددة تتضمن معرفة فنية بالحاسبات. لذلك يجب ألا يقتصر التحليل على الجوانب الإدارية فى بيئة ونظام المعلومات.مما يترتب عليه الحاجة إلى رأى فنى يساعد المراجع فى تقييم بعض المخاطر والضوابط . ويوضح الشكل رقم (١) الهيكل العام للنموذج المقترح لتقييم ضوابط الحماية (الرقابة) فى نظم المعلومات المحاسبية الالكترونية. ونتناول فيما يلى بالمناقشة والتحليل كل من عناصر النموذج.

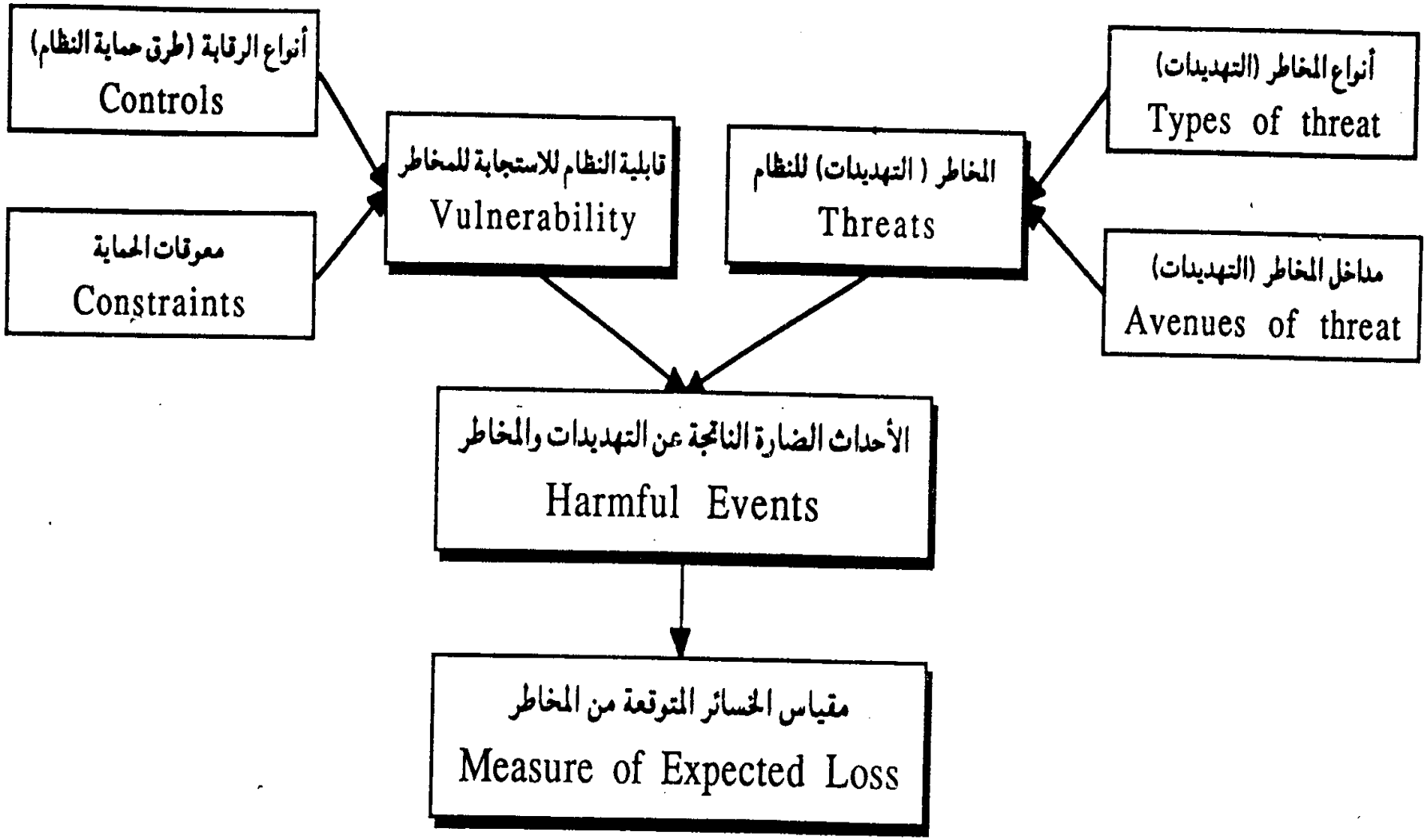
أولا : المخاطر التى يتعرض لها النظام Threats

المخاطر أو التهديدات التى يتعرض لها نظام المعلومات المحاسبى هى إحدى خصائص البيئة التى يعمل فيها النظام ، وليست خاصية داخلية له.وقد تتعدد أنواع ومداخل هذه الأخطار أو التهديدات الى النظام. ونلخص فيما يلى هذه الأنواع والمداخل للمخاطر الشائعة.

أنواع المخاطر (التهديدات) لنظام المعلومات Types of Threat

أول أنواع المخاطر التى يتعرض لها النظام هوالتلاعب فى البيانات بقصد تدميرها Data Destruction سواء بالحذف ، أو بالدمج غير الصحيح لبعضها ،أو بخلطها ببيانات أخرى غير حقيقية أو تبويبها بشكل خاطئ تفقد معه مدلولها ومعناها. ويمكن أن يحدث ذلك فى أجزاء مختلفة من نظام المعلومات المحاسبى كحسابات التكاليف، أو المخزون،أو النقدية، أو المبيعات، أو المصروفات.أو قد يكون تدمير البيانات ناتجا من تغييرها (تعديلها) فى البيانات Data Change (Modification) بشكل يجعلها لا تعبر عن الحقائق التى نتجت عنها أصلا. وتتضمن أمثلة التغيير فى البيانات، التلاعب فى حسابات المدينين والدائنين بقصد الغش. و قد يحدث هذا التلاعب فى مراحل مختلفة من النظام مثل المدخلات أو التشغيل أو التخزين أو المخرجات. و تدمير البيانات قد يكون جزئيا أو كليا وفى الحالة الأخيرة قد يصعب تصحيح البيانات أو استعادتها ، مما يشكل خسارة كبيرة لنظام المعلومات وما ينتج عنه من قرارات.وكذلك قد يغير من نتائج أعمال الشركة أو مركزها المالى ويتيح تغطية سرقات أو اختلاسات فى أصول الشركة. (١٠)

وقد يهدف التلاعب بالنظام إلى الاطلاع على بيانات سرية Disclosure of



شكل رقم (١)

نموذج تقييم محددات

امن المعلومات المحاسبية فى النظم الالكترونية

Confidential Data مثل بيانات تخطيط الربحية ،أو بيانات الأفراد (الرواتب والترقيات والعلاوات). ويمكن للمتلاعب فى هذه الحالة ليس فقط الاطلاع على البيانات وإساءة استخدامها بل أيضا سرقة بعضها أو كلها. ذلك كله قد ينتج عنه خسائر للمنشأة تكون كبيرة فى بعض الحالات. (١١)

وأخيراً فإن من المخاطر التى تتعرض لها البيانات المحاسبية فى النظم الالكترونية أن يتم تغيير صلاحيات الدخول إلى النظام بحيث يمنع **الأشخاص المخولين من استخدام النظام** Denial of Services. وقد يتم ذلك عن طريق تغيير مصطلحات الدخول إلى النظام Passwords لفترة ما يمنع خلالها المخولين من ذلك وبالتالى يصعب اتخاذ قرارات سليمة لعدم التمكن من التعامل مع النظام، ويتأخر إصلاح هذه المشكلة قد تتضاعف الخسائر الناتجة عن هذا الخطر. (١٢)

طرق (منافذ)المخاطر إلى نظام المعلومات المحاسبى Avenues of Threat

تتعدد منافذالمخاطر على المعلومات المحاسبية فى النظم الالكترونية. وقد تكون المخاطر Threats من داخل المنشأة Inside أو من خارج المنشأة Outside. وسواء كانت المخاطر داخلية أو خارجية فإنها تهددعناصر النظام التى تشمل البيانات، البرامج، المستخدمين، أو شبكات الاتصال.

فالبيانات Data هى منفذ شائع للتلاعب والغش يستخدمه المتلاعبون من داخل المنشأة Insiders فى إدخال بيانات غير صحيحة أو غير حقيقية (وهمية) إلى الحاسب، بهدف تدمير أو تلويث البيانات الصحيحة الموجودة داخل النظام (١٣).

كذلك **البرامج Software**، فهى من المنافذ السهلة والشائعة للتلاعب فى النظام. ومن البرامج التى شاعت فى السنوات الأخيرة ، هى ما يطلق عليها فيروس (جرثومة) الكمبيوتر Computer Virus وهى برامج تعمل على تغيير أوتدمير أو حذف البرامج والبيانات لتحقيق نتائج معينة تهم المتلاعب بالنظام (١٤). وهذه البرامج تلتصق ببرامج أخرى فى الحاسب عن طريق إدخال تعليمات سرية ضمن تعليمات البرامج الأصلية لتعطيلها عن العمل أو تحويلها إلى أعمال معينة لم تكن مصممة لها أصلا. وتنتقل هذه العدوى من برنامج لآخر فى نظام المعلومات (١٥) . وهناك نوع آخر من البرامج المعدية (المدمرة) يسمى ديدان Worms. وهذا النوع من البرامج له قدرة ذاتية على نسخ نفسه من بيئة (أو نظام)البيئة أخرى وتشغيل نفسه فى البيئة الجديدة (١٦). وعلى عكس برامج الجراثيم Viruses، فإن برامج الديدان لا تلتصق ببرامج أخرى وإنما تحوى بداخلها تعليمات تقوم بتنفيذها. لتدمير البيانات أو سرقة المعلومات أوإحداث

مشاكل فى التشغيل. والنوع الثالث من البرامج المدمرة هو ما يسمى "حصان طرواده Trojan Horse". وهذا البرنامج يبدو فى شكل البرامج المعروفة والمستخدمة على نطاق واسع مثل (Lotus, Data Base, etc...)ولكن عند تشغيله يؤدى وظائف مختلفة لا تخطر ببال المستخدم وتضر بالبيانات المخزونة داخل الحاسب. ومعظم البرامج من هذا النوع لا تترك أثراً لها بعد إلحاق الضرر بالبيانات لأنها تقوم بمسح أو إزالة نفسها من ذاكرة الحاسب مما يصعب معه تعقبها (١٧). وعلى اختلاف مسميات وأنواع البرامج المدمرة فإنها تدخل إلى الحاسب من خلال عمليات البرمجة أواستخدام برامج جاهزة ملوثة.

ويشكل مستخدمو النظام System Users طريقاً آخر لإدخال المخاطر للبيانات والمعلومات والبرامج التى يحتويها نظام المعلومات المحاسبى. وتختلف دوافع المستخدمين للتلاعب بالبيانات والمعلومات والبرامج (١٨) . فالبعض تحركه الدوافع الاقتصادية، أى الرغبة فى الحصول على مكاسب وأموال بأية وسيلة ، مما يدفعه إلى الاختلاس والسرقة عن طريق التلاعب فى بيانات النظام. وقد تكون دوافع المستخدم أيديولوجية فبعض الأفراد يعتقدون أن المنشآت تحقق أرباحا كبيرة وتبالغ فى وصف منتجاتها أو خدماتها للمستهلكين، ودائما تمنح العاملين حقوقا أقل مما تستطيع منحه لهم، وبالتالى فإن هذه المنشآت ،فى نظرهم، تخدع المحيطين بها ولذلك فمن العدالة خداعها بالتلاعب فى نظمها المالية الالكترونية وإيقاع خسائر بها. وهناك دوافع أخرى تتمثل فى محاولات الفرد لإثبات ذاته عن طريق تحدى نظم المعلومات التى تعتقد الشركات والمنشآت أنها فى حماية كاملة. أى أنها دوافع المغامرة لإثبات مدى ذكاء وخبرة المغامر فى التلاعب بالأنظمة مهما كانت الرقابة عليها .وأخيراً فقد يلجأ الموظف، مستخدم النظام، إلى التلاعب بالنظام بغية الثأر من المنشأة إذا أساءت إدارتها التعامل معه أو على الأقل كان لديه شعور بذلك. (١٩)

وأخيرا فمن مداخل الخطرعلى النظام شبكات الاتصال Communication Networks . فاستخدام شبكة الإتصالات التليفونية العامة فى نقل البيانات من وإلى النظام بواسطة طرفيات أو محطات عمل فرعية بعيدة عن مكان الأجهزة الرئيسية يتيح الفرصة للبعض للدخول الى النظام بصورة غير مشروعة . (٢٠)

ثانيا : تعرض (قابلية) النظام للاستجابة للتهديدات والمخاطر Vulnerability

يقصد بتعرض النظام قابلية أو إستجابة عناصره (وظائفه أو عملياته) للاختراق والتلاعب، سواء كانت الأجهزة أو المعدات أوالبرامج، أو إجراءات التشغيل والاستخدام،أو شبكات الإتصال. وهذا المتغير يعبر عن إحدى الخصائص الداخلية للنظام

نفسه .وتتحدد القابلية للاستجابة فى ضوء عاملين أساسية هما كفاية ضوابط الحماية المحيطة بالعنصر والتى صممت لمقاومة هذا الخطر أو التهديد، ثم المعوقات والقيود المؤثرة على كفاءة أو اكتمال هذه الضوابط. ويعتمد نجاح القائم بالتحليل على التفكير كمهاجم للنظام (٢١) وعليه أن يتمثل فى ذلك دوافع الأفراد للتلاعب وأفضل المواضع لإختراق النظام.

ضوابط الحماية (الدفاع) عن النظام Security Controls

تشتمل ضوابط الحماية (الدفاع) عن النظام المحاسبى الالكترونى، كل التصرفات، الإجراءات، الأساليب، والأدوات،التى تستخدم لتقليلمستوى تعرض عناصر النظام وبالتالى تقليل الخسائر المتوقعة للحد الأدنى.

وقد تقسم هذه الضوابط حسب هدف الإجراء الرقابى (مثلا إجراء لمنع الخطر Preventive، أو لإحتواء الخطر Containment، أو لإسترجاع الخسائر Recovery) وتمثل هذه الأنواع ثلاث طبقات Layers من الحماية. وهناك تقسيم آخر مرتبط بطبيعة الإجراء الرقابى أو وسيلة الحماية (فنية أو إدارية أو تنظيمية).يمكن أن توصف المجموعة الأولى من هذه الضوابط ، بالضوابط التنظيمية Organizational وتشمل بناء الهيكل التنظيمى وحدود السلطات والمسئوليات ، ونظام التقارير ..الخ. وهذه الضوابط بطبيعتها استراتيجية وتعبر عن السياسة العامة للمنشأة تجاه نظمها وتتضمن وضع سياسات Policy Formulation مكتوبة تتعامل مع المعلومات كأصل من الأصول تكفل له الحماية من خلال خطة تفصيلية لكيفية تحقيق تلك الحماية. كما تتضمن الإلتزام المعلن للإدارة Management Commitment بحماية النظام، ومحاسبة المسئولين عن التقصير في تنفيذ الضوابط الموضوعة.(٢٢). أما ضوابط الحماية المادية Physical Security فتختص بالعوامل البيئية المحيطة بالعناصر المادية للنظام مثل تجهيز مكان للأجهزة والمعدات من مواد تقاوم الحرائق، وتوفير أنواع معينة من معدات الاطفاء لا يسبب استخدامها ضررا لأجهزة الحاسبات . وأيضا تركيب أجهزة تحكم فى التيار الكهربائى UPS، وأجهزة مساندة Standby للاستخدام فى حالة فشل المصدر الرئيسى للتيار حتى لا تضيع بعض البيانات. ومن هذه الضوابط تجهيز المداخل إلى مكان الحاسبات باستخدام الوسائل الالكترونية لتحقيق الشخصية User Identi-fication بحيث يمكن مراقبة دخول وخروج الأفراد (٢٣).

وتسمى الضوابط التى تندرج فى المجموعة الرابعة، ضوابط البيانات Data Controls. وتتضمن هذه المجموعة اجراءات حماية البيانات من الاطلاع عليها، بقصد

أو بدون قصد، بواسطة أشخاص ليس لهم الصلاحية في ذلك، وكذلك حمايتها من أى تعديل أو تدمير يلحقه بها هؤلاء الأشخاص (IBM Corporation 1987). كما تشمل حفظ نسخ إحتياطية Backup وإجراءات الاستعادة Recovery فى حالات حوادث البيانات. ويراعى فى ضوابط حماية البيانات معيارين: الأول هو الخدمة الأدنى Mini-mal Previlege ويقضى بإتاحة القدر المطلوب واللازم فقط من البيانات لأداء عمل المستخدم. أما الثانى فيسمى التعرض الأدنى Minimal Exposure ويقصد به أن المستخدم الذى له صلاحية الاطلاع على معلومات حساسة يكون عليه مسئولية حمايتها بعدم اتاحتها لأشخاص آخرين إلا من تتطلب أعمالهم ذلك وبقدر ما تتطلبه هذه الأعمال (٢٤).

وهناك ضوابط الاتصال Communication Controls التى تختص بتأمين وحماية شبكات الحاسبات من مخاطر الإتصال الخارجي غير المسموح، خاصة من خلال شبكة الهاتف العمومية. ويتضمن ذلك كلمات مرور للدخول إلى النظام من الخارج. بل قد يتحتم إستخدام تليفونات (أرقام) محددة لهذا الإتصال. ثم إن إمكانية الحصول على بيانات معينة بواسطة المتصل من الخارج، قد تعتمد على ما إذا كان لديه أجهزة استقبال Modems مصممة خصيصا ومصرح بها لهذا الغرض. (٢٥) وفى حالة نقل المعلومات لاسلكيا، قدتتم الحماية بإدخال أو صياغة ضوابط ورموز تمنع ترجمة الشفرة المنقولة إلى البيانات الصحيحة إلا بواسطة من لهم تلك الصلاحية. كما قد يتم اختيار ترددات معينة لنقل الشفرة يصعب على الآخرين استقبالها.

أما النوع التالى من ضوابط الحماية فهى ضد البرامج الجرثومية Anti Virus Controls وهذه الضوابط تكون إما مانعة لا تسمح للمستخدمين بإدخال برامج أو بيانات غير مصرح بها، أو كشفية وعلاجية، للكشف عن أية برامج جرثومية تداخل النظام ومسحها وتنظيف آثارها.

وأخيراً فإن من ضوابط حماية النظام المحاسبى الالكترونى ما يخص الأفراد المتعاملين مع النظام بما فى ذلك طريقة اختيارهم وصفاتهم الشخصية وتأهيلهم المهنى (٢٦). مع مراعاة تغيير كلمات الدخول إلى النظام الخاصة بموظف معين إذا انتهى عمله بالمنشأة لأى سبب، وكذلك إلتزام كتابى من هؤلاء المستخدمين بعدم إتاحة صلاحياتهم فى التعامل مع النظام لآخرين حتى ولو كانوا من مستخدمى النظام.

معوقات حماية نظم المعلومات المحاسبية الالكترونية :

يرجع العامل الأول فى صعوبة حماية البيانات والبرامج فى نظام المعلومات

المحاسبى إلى تعدد مداخل الخطر التى سبق الإشارة إليها وكذلك تعدد مكونات النظام من أجهزة، برامج، بيانات، شبكات إتصال. وفى كل من هذه المواضع تتعدد الطرق التى يمكن بها تهديد النظام (٢٧).

أما العامل الثانى الذى يؤثر فى فعالية اجراءات حماية نظام المعلومات المحاسبى هو إحتمال تشتت المسئولية الإدارية عن النظام ما بين الإدارة المالية فى المنشأة وإدارة التشغيل الالكترونى للبيانات، وكذلك انتشار مستخدميه فى أماكن مختلفة بالمنشأة (٢٨).

ويقلل التقدم التقنى من فعالية ضوابط الحماية، حيث تساعد الإمكانات الفنية المتزايدة فى إختراق حواجز الحماية، مما يجعل من التفكير فى إجراءات حماية جديدة عملاً مستمراً.

ومن العوامل التى تقلل من فعالية ضوابط حماية نظام المعلومات الالكترونى صعوبة بل وعدم توافر معلومات عن بعض جرائم الكمبيوتر إما لرغبة المنشأة فى عدم نشرها أو لعدم اكتشافها أصلا، مما يجعل من الصعب تعقبها والتعرف على مداخلها.

وأخيراً فإن صعوبة تحديد الخسائر المحتمل وقوعها، من المخاطر المحيطة بالنظام، تجعل من تصميم ضوابط (إجراءات) حماية المعلومات فى النظام تكلفة يصعب تقييم جدواها فى ضوء العائد منها Cost ≤ Benefits .

ثالثا : تحديد الأحداث الضارة المتوقعة Expected Harmful Events

يؤدى وجود تهديد أو خطر معين على عنصر أو عملية أو نشاط فى نظام المعلومات المحاسبى، واستجابة هذا العنصر له إلى وقوع حدث ضار بالنظام. وقد يكون الحدث ضاراً بالمكونات المادية للنظام (أجهزة، معدات، توصيلات) مثل السرقة والحريق والتلف. أو قد يكون ضار بالبرامج أو بالبيانات الموجودة بداخله مثل تدمير البيانات أو تغييرها أو سرقتها أو الافصاح عنها لغير المختصين.

وطبقا لحجم ونوع الضرر الناشىء عن ذلك، تكون الخسارة المتوقعة للمنشأة. ورغم صعوبة تقدير هذه الخسارة بشكل منهجى، إلا أنه يمكن بالدراسةالميدانية والملاحظة الفعلية اقتراح شكل تقريبى للدالة الممكن استخدامها فى قياس هذه الخسارة.

رابعا : قياس الخسائر المتوقعة

يعتمد المقياس المقترح على مفهوم القيمة المتوقعة Expected Value والتى

تعتمد على إحتمال حدوث الحدث وقيمة الخسارة الناتجة فى حالة حدوثه. ولكن المقياس المقترح يأخذ فى الإعتبار أوزان ترجيحية أخرى سنتناولها بالتفصيل فيما بعد.

(أ) متغيرات النموذج (المقياس)

يتضمن النموذج المقترح المتغيرات التالية :

١- المخاطر المحيطة بالنظام Threats (t's)

(أ) تحديد وتقسيم المخاطر الى أنواع رئيسية (مجموعات) وأنواع فرعية:

أول متطلبات النموذج المقترح هى تحديد المخاطر الرئيسية المتوقعة مثل : تدمير البيانات، سرقة البيانات، سرقة المعدات... الخ. و يرمز لكل نوع من هذه المخاطر الرئيسية بالرمز t ، حيث $t = 1,2,.....,T$

(ب) تحديدأهمية نوع الخطر أو التهديد t بالنسبة لباقى الأخطار:

من المهم تحديد الوزن النسبى Weight لكل نوع من المخاطر الرئيسية t للتعبير عن درجة أهمية(خطورة Severity) هذا الخطر بالنسبة للأخطار الأخرى. وهذا الوزن النسبى ضرورى لإ ستخراج مقياس عام لمستوى المخاطر المحيطة بالنظام.ويلاحظ أن مجموع أوزان t's يساوى ١.

(ج) تحديد التهديدات أو المخاطر الفرعية المتسببة فى الخطر t :

يتمتحديد التهديدات أو المسببات لكل نوع من المخاطر الرئيسية، فمثلاالتلاعب فى البيانات هو خطر ينتج من تهديدات مختلفة منها : تلاعب أفراد بقواعد البيانات، أو إدخال برامج جرثومية، أو أخطاء فى أوامر التشغيل ،...الخ . ويمكن التعبير عن كل من هذه التهديدات الفرعيةبالرمز n ، داخل نوع الخطر t حيث: $n = 1,2,.....,N$

وحيث أن الوزن النسبى يرتبط بالحدث الضار المترتب على الخطر أو التهديد، وما دامت التهديدات الفرعية ، على إختلاف أنواعها ، تتسبب فى نفس التهديد (الخطر) الرئيسي، فإنه من المنطقى أن تحدد أوزان للمخاطر الرئيسية ،وليس هناك حاجة لتحديد أوزان للتهديدات الفرعية .

(د) تحديد إحتمالات حدوث كل نوع من المخاطر :

من خلال الملاحظة الميدانية، يجب أن يدرس ويحسب احتمال Probability وقوع كل تهديد n من نوع الخطر t على عنصر النظام أو العملية c محل التقييم.

٢- تقسيم النظام الى عناصر أو أنشطة أو عمليات Components

حيث أن تحليل المخاطر ومستوى التعرض يقاس بالنسبة لكل عنصر Component من عناصر النظام على حده، فمن الضرورى تقسيم النظام الى عناصر أو أنشطة أو عمليات . ويستخدم الرمز c للتعبير عنها. حيث : c = 1, 2, ..., C

٣- مستوى (درجة) تعرض النظام أو قابليته للتلاعب Vulnerability

هذا المتغير مستقل عن إحتمال حدوث الخطر . وهو يعبر عن مستوى ضعف الرقابات المحيطة بعنصر النظام أوالإجراء أو العملية محل التقييم، أى عن قابلية هذا العنصر أو الإجراء للتلاعب أو الإستجابة للتهديد n من نوع الخطر t.

٤- الخسارة المتوقعة Expected Loss

هذه الخسارة يتم تقديرها بالنسبة لكل خطر فرعى n فى مجموعة خطر رئيسى t ، عندما يقع أو يتحقق على عنصر النظام c . ويكون قياس هذه الخسارة المتوقعة فى شكل قيمة مالية.

(ب) الصيغة الرياضية للنموذج

يمكن صياغة المقياس العام لخسارة النظام المحاسبى الالكترونى المتوقعة من كافة أنواع المخاطر المحيطة به كالآتى :

$$ETL = \sum_{t=1}^{T} \sum_{n=1}^{N} W_t \sum_{c=1}^{C} P_{tnc} \cdot V_{tnc} \cdot L_{tnc}$$

$$W_t \geq 0, \ \sum_t W_t = 1,$$

$$P_{tnc} \geq 0, \ \sum_n P_{tnc} = 1 \text{ for a given c.}$$

حيث :

ETL = الخسارة الإجمالية المتوقعة من الأخطار المحيطة بالنظام (Expected Total Loss)

t = نوع (مجموعة) الخطر أو التهديد (الرئيسى) Threat

n = نوع الخطر (التهديد) الفرعى الذى يؤدى الى الخطر الرئيسى t

W_t = الوزن النسبى Weight لنوع الخطر t مقارنا بالمخاطر الرئيسية الأخرى.

P_{tnc} = احتمال وقوع المسبب (التهديد) n للخطر t على عنصر النظام c

ويمكن التعبير عن إحتمال الخطأ المقصود بالدالة الآتية:

P_{tnc} = f {P(occurance), Intruder's Skill, No. of people involved}

حيث يعتمد الخطأ المقصود على مهارة المتلاعب ، وعدد المتلاعبين، بالإضافة الى الخطأ (الخطر) العشوائى.ولكن بالنسبة للمخاطر غير المقصودة ، أى العشوائية، فيمكن تقدير احتمالات حدوثها بالصورة البسيطة التالية:

$$P_{tnc} = P \text{ (occurance)}$$

V_{tnc} = درجة تعرض Vulnerability العنصر c ، أو قابليته للاستجابة لنوع الخطر n فى مجموعة الخطر t. وهذه النسبة هى محصلة لمتغيرين هما درجة تعقيد العملية أو العنصر ، ومستوى الرقابات المحيطة به. أى :

$$V_{tnc} = f(\text{complexity of the process, existing controls})$$

L_{tnc} = الخسارة Loss المتوقعة من وقوع الخطر n مسببا للضرر t على عنصر النظام c . وهذه الخسارة تتضمن أربعة عناصر تظهر فى الدالة التالية:

$$L_{tnc} = f(X,Y,Z,K)$$

حيث :

X = تكلفة تصحيح الأضرار الناتجة عن الخطر،

Y = تكلفة إسترجاع البيانات الممسوحة،

Z= قيمة المعلومات التى لا يمكن إسترجاعها .

K = قيمة الضرر الناشىء عن إستخدام معلومات غير صحيحة .

خامسا ، مثال توضيحى Illustravive Example

يتضمن الشكل رقم (٢) جدولا يحتوى على بيانات تم إفتراضها لمثال توضيحى لتحليل وقياس الخسائر المتوقعة من نوع واحد من المخاطر على عنصر واحد(أو عملية واحدة) فى النظام المحاسبى الإلكترونى. وهذا التحليل بالطبع ينطبق على باقى المخاطر وباقى العناصر فى حالة دراسة النظام ككل.

وفيما يلى نتناول خطوات المثال التوضيحى لتطبيق النموذج المقترح:

نوع (إسم) الخطر t / الحدث الضار المتوقع	الوزن النسبي للخطر W_t	عنصر النظام أو العملية محل التقييم c	رقم الخطر الفرعي n	أسباب (مخاطر فرعية) للخطر N_t	إحتمال حدوث الخطر الفرعي P_{tmc}	مستوى تعرض العنصر V_{tmc}	الخسارة الناتجة عن الخطر* L_{tn}
التلاعب فى البيانات/ تدمير البيانات	٤٠٪	عملية إدخال البيانات (طرقيات الإدخال)		**مقصودة:**			
			n = 1	- إدخال بيانات غير حقيقية بواسطة المستخدم	١٥٪	٧٠٪	١٥٠,٠٠٠
			n = 2	- إدخال بيانات غير حقيقية بواسطة شخص غير مخول .	٢٥٪	٢٠٪	٧٥,٠٠٠
			n = 3	- إدخال بيانات غير حقيقية عن طريق أعطال فنية متعمدة فى أجهزة الإدخال	١٠٪	٢٥٪	٢٥,٠٠٠
				غير مقصودة :			
			n = 4	- أخطاء عشوائية فى إدخال البيانات	٣٥٪	٦٠٪	٤٠,٠٠٠
			n = 5	- أعطال فنية غير متعمدة تسببت فى تدمير البيانات عند الإدخال .	١٥٪	١٥٪	٢٠,٠٠٠

(ب) قياس إجمالى الخسائر المتوقعة (ETL)

اجمالى الخسائر المتوقعة (ETL) = ٤٠٪ [(١٥٠,٠٠٠)(,٧٠)(,١٥) + (٧٥,٠٠٠)(,٢٠)(,٢٥) + (٢٥,٠٠٠)(,٢٥)(,١٠)

+ (٤٠,٠٠٠) (,٦٠)(,٣٥) + (٢٠,٠٠٠)(,١٥)(,١٥)]

= ٤٠٪ (٢٨٩٧٥) = ١١,٥٩٠ دولار.

* الخسائر يمكن تقديرها بمستوى ثقة معين (± ٪)

١- تحديد نوع الخطر t

تم تعريف الخطر محل التحليل بأنه التلاعب فى البيانات المدخلة الى النظام.

٢- تقدير الوزن النسبى للخطر t ، أى W_t

يفترض هذا المثال نسبة ٤٠٪ للتعبير عن الأهمية النسبية لخطر التلاعب بالبيانات بالنسبة لباقى الأخطار المحيطة بالنظام. وقد يبدو هذا الوزن عاليا، ولكنه فى الحقيقة يرتبط بخطر يؤثر بصورة جوهرية على نتائج العمل فى النظام. وفى الواقع العملى يعتمد تحديد الأوزان النسبية على خبرة المنشأة بأنواع المخاطر المختلفة وما قد ينتج عنها من أضرار وخسائر. كما يتأثر هذا التقدير بقدرة المنشأة على تصحيح أو إستعادة البيانات التى تم التلاعب فيها.

٣- تعريف c :

وهى العنصر أو الوظيفة أو العملية من النظام التى ستكون ضوابط حمايتها محل التحليل والتقييم. لهذا الغرض تم تقسيم النظام المحاسبى الإلكترونى إلى مراحل (مدخلات ، تشغيل، تخزين، مخرجات). ثم أختيرت مرحلة المدخلات وأعيد تقسيمها إلى عمليات أو وظائف (تجميع بيانات، تجهيز بيانات، إدخال بيانات) وأخيرا تم إختيار عملية إدخال البيانات (عبر وسيلة الإدخال) لتكون هى العملية محل التقييم ،أى c . وقد تتعلق البيانات المدخلة بأى نشاط مثل المبيعات ، المخزون، المصروفات ..الخ.

٤- تحديد المسببات أو المخاطر الفرعية N للخطر t

من الإطلاع على بعض الدراسات السابقة فى موضوع أمن المعلومات [٢٩] ، يمكن إفتراض خمسة مسببات أو مخاطر فرعية تعتبر تلاعبا فى البيانات أو تؤدى الى ذلك. وتتضمن المخاطر **المقصودة** : إدخال بيانات غير حقيقية بواسطة المستخدم ، أو بواسطة أشخاص غير مستخدمين للنظام عن طريق تلاعبهم بكلمات المرور ، أو أعطال فنية مقصودة فى أجهزة الإدخال تتسبب فى إدخال البيانات بصورة خاطئة. أما الأسباب **غير المقصودة** فتتضمن : الأخطاء العشوائية فى إدخال البيانات ،نتيجة لجهل المستخدم ، أو أعطال فنية غير مقصودة فى أجهزة الإدخال تتسبب فى إدخال البيانات بصورة خاطئة.

٥- تحديد إحتمالات حدوث التهديدات (المخاطر الفرعية) P_{tnc}

فى هذه الخطوة تستخدم الدوال التعريفية لهذه الإحتمالات كما سبق بيانه فى النموذج. ويجب الإشارة هنا إلى الحاجة لبيانات ميدانية تمكن من وضع هذه الدوال فى شكل معادلات يمكن بها تحديد هذه الإحتمالات. وفى هذا المثال ولأغراض التوضيح

سنفرض الإحتمالات الموجودة فى الجدول الموضح فى شكل رقم (٣). لاحظ أن هذه الإحتمالات مستقلة عن مستوى (إحتمال) تعرض العنصر أو العملية فى النظام. ولقد روعى فى الأرقام المفترضة مايلى :

- تساوى مجموع إحتمالات المخاطر المقصودة مع غير المقصودة
- المخاطر التى ترجع الى تعطل الأجهزة أقل إحتمالا من التى ترجع الى أخطاء العنصر البشرى
- مجموع إحتمالات المخاطرالفرعية n لنفس الخطر t علي العنصر الواحد c=١.

٦- تقدير مستوى إستجابة العنصر للمخاطر V_{tnc}

هذه التقديرات محصلة عاملين هما: مدى تعقيد العملية التى يقوم بها العنصر،، ومستوى أداء ضوابط الحماية المصممة لها. ولأغراض المثال فقد تم إفتراض هذه النسب كما فى العامود المختص من الجدول الموضح فى شكل (٢). وقد بنيت هذه النسب (الإحتمالات) الإفتراضية على :

- أن الإستجابة للتلاعب المقصود أكبر منها لغير المقصود
- أنه ليس هناك إستجابة كاملة للتلاعب فى كافة البيانات ، حيث عادة ما تصمم برامج الإدخال بضوابط معينة . وقد تم إفتراض حد أدنى لفعالية هذه الضوابط (٣٠٪).
- إحتمال معرفة كلمات المرور لغير المستخدمين لا يزيد عن ٢٠٪
- إستجابة النظام للأخطاء العشوائية فى إدخال البيانات يتحدد بما لا تكتشفه برامج الإدخال من أخطاء

٧- تحديد الأحداث الضارة المتوقعة

فى هذا المثال تم تحديد الحدث الضار بأنه تدمير أو تخريب البيانات.وعموما فمن المفضل إعداد دليل للأحداث الضارة المتوقعة والناتجة عن المخاطر المحتملة بحيث يتضمن هذا الدليل وصفا للحدث الضار وموقعه والخسائر المتوقعة منه.

٨- تحديد الخسائر L_{tnc}

يتم تقدير الخسارة التى تنتج عن التلاعب فى البيانات الناتج من عملية الإدخال ،لكل سبب على حده، ولكن لمدة دورة كاملة فى النظام. وإذا كانت القوائم المالية تستخرج من بيانات النظام المحاسبى عن سنة، فيكون تقدير الخسارة الإحتمالية من الخطأ عن سنة. وعموما فان هذا التقدير يحتاج أيضا الى ملاحظات ميدانية لتقدير

عناصر الخسارة بما فى ذلك تكلفة تصحيح وإسترجاع وستخدام بيانات خاطئة. وفى هذا المثال تم إفتراض الخسائر على« أساس الصعوبة النسبية المتوقعة فى إحتواء وإسترجاع خسائر البيانات الناتجة عن المخاطر غير المقصودة، عنها فى حالة خسائرالبيانات المقصودة ويلاحظ أن الخسائر قد تحدد فى شكل مدى range ، أى بمستوى ثقة يجعل لها فى التطبيق العملى حدا أقصى وحدا أدنى.

ويتضح من نتائج المثال التوضيحى الواردة فى شكل (٢) أن الخسائر المتوقعة من خطر التلاعب فى البيانات ، من خلال عملية الإدخال فقط عبر طرفية الإدخال، وطبقا للأرقام المفترضة فى المثال هى ١١.٥٩٠ دولار. ويستفيدالمراجع الداخلى من هذا الرقم فى النظر إليه كسقف لتكلفة أية ضوابط حماية إضافية مقترحة ضد خطر التلاعب في البيانات عند نقطة الإدخال.كما يستفيد المراجع الخارجى به فى الحكم على جوهرية الخسارة المحتملة، والتى يمكن أن يستنبط منها مدى ضعف الرقابة وبالتالى ضرورة توسيع نطاق الفحص.

سادسا : محددات تطبيق النموذج Model Limitations

تتوقف دقة نتائج تحليل الخطر على مدى **تعقيد بيئة التحليل** Environment Complexity . وتتضمن المتغيرات التى تساهم فى تعقيد بيئة النظام المحاسبى الالكترونى، ما يلى:

١ - كبر حجم المنشأة وتعدد أماكن نشاطها.
٢ - كبر حجم النظام وتنوع معداته وأماكن استخدامه
٣ - زيادة عدد مستخدمى النظام وإنتشارهم فى أماكن متباعدة
٤ -إتساع شبكة المعلومات المتصلة بالنظام
٥ - مستوى التقنية المستخدم فى النظام
٦ - طريقة إعداد البرامج وصلاحيات التغيير والتعديل فيها.

ومن المتوقع أنه كلما زادت مساحة استخدام النظام ، وتعدد مستخدموه، وكثرت وتباعدت المواقع التى تمتد اليها طرفياته وأجزائه ، وتقادمت التقنية المستخدمه فى معداته وبرامجه، فان ذلك سوف يؤدى الى جهد وتكلفة أكبر فى تحليل وتقييم كافة ضوابط الحماية فيه [٣٠]. أما التوازن بين التكلفة والعائد فهى إحدى القواعد الهامة التى يجب مراعاتها عند تطبيق نموذج تحليل الخطر،من حيث الموارد المطلوبة لإجراء التحليل، أو من حيث دورية إجرائه، أو توافر الخبرات اللازمة لذلك.

خلاصـــة البحث

تناول هذا البحث مشكلة تقييم أمن المعلومات المحاسبية فى النظام الإلكترونى، عن طريق تحليل محددات هذا الأمن وهى المخاطر المحيطة بالنظام والضوابط المصممة لمقاومتها.. وقد إقترح البحث نموذجا كميا يعتمد على تحديد أنواع هذه المخاطر ومسبباتها الفرعية، ودرجة إستجابة النظام لها، والأحداث الضارة المتوقعة من ذلك والخسائر المقدرة من هذه الأضرار.

وهذا النموذج يشكل أداة منهجية لمساعدة الإدارة فى الحكم على أداء ضوابط الحماية (وسائل الرقابة) فى نظام المعلومات المحاسبى الإلكترونى، ومدى مقبولية الخسائر الناتجة عن ضعف هذه الحماية. ،وكذلك جدوى إنشاء ضوابط جديدة لزيادة مأمونية المعلومات. كما يساعد المراجع على تحديد نطاق المراجعة فى ضوء مستوى المخاطر ومستوى أداء الضوابط. و النموذج المقترح فى هذا البحث يرتكز على تحليل الخطر كمدخل أساسى لتقييم الحاجة الى ضوابط إضافية لتحقيق أمن المعلومات. ولتوضيح إجراءات تطبيق النموذج، فقد قدم البحث مثالا بأرقام إفتراضية تتعلق بنوع واحد من المخاطر على عنصر أو عملية واحدة من عمليات النظام و تم قياس خسائر المعلومات المتوقعة فيها.

على أننا يجب أن ننوه أن هذا النموذج يحتاج الى بيانات فعلية تنتج عن دراسة ميدانية تهدف للتعرف على سلوك عناصر النظام تحت التهديدات المختلفة وملاحظة مدى تكرارية هذه التهديدات، ، وتحديد مدى الضرر الناشىء عنها. وقد تكون الدراسة الميدانية المطلوبة موضوعا ملائما لبحث آخر فى هذا المجال.

هوامش ومراجع البحث :

1. O'Donoghue, J. "Computer Crime is Usually an Inside Job", **Digital Review**, 21, July 1986.

2. Parker, D. B. "Consequential Loss From Computer Crime" In **Security and Protection in Information Systems** , A. Grissonanche, ed., Elsevier, 1986 pp. 379-380.

3. Wilson, J. L., E. Turban, and M. Zviram "Information Systems Security : A Managerial Perspective", **International Journal of Information Management**, Vol 12, 1992, pp. 105-119.