العنوان:	أهمية مخاطر نظم المعلومات المحاسبية الإلكترونية دراسة تطبيقية على المنشآت السعودية
المصدر:	مجلة التجارة والتمويل
الناشر:	جامعة طنطا - كلية التجارة
المؤلف الرئيسي:	أبو موسى، أحمد عبدالسلام
المجلد/العدد:	ع 2
محكمة:	نعم
التاريخ الميلادي:	2004
الصفحات:	1 - 54
رقم MD:	332516
نوع المحتوى:	بحوث ومقالات
قواعد المعلومات:	EcoLink
مواضيع:	الحاسبات الإلكترونية ، نظم المعلومات المحاسبية ، الموظفون ، السعودية ، تكنولوجيا المعلومات ، النظم المحاسبية ، أمن المعلومات ، الكوارث الطبيعية ، فيروسات الحاسب
رابط:	http://search.mandumah.com/Record/332516

أهمية مخاطر نظم المعلومات المحاسبية الإلكترونية

دراسة تطبيقية على المنشأت السعودية

دكتور

أحمد عبد السلام أبو موسى

قسم المحاسبة ونظم المعلومات الإدارية

جامعة الملك فهد للبترول والمعادن

أهمية مخاطر نظم المعلومات المحاسبية الإلكترونية
دراسة تطبيقية على المنشآت السعودية*

دكتور

أحمد عبد السلام أبو موسى

قسم المحاسبة ونظم المعلومات الإدارية
جامعة الملك فهد للبترول والمعادن

ملخص البحث:

يهدف هذا البحث إلى التعرف على وإستكشاف وإختبار المخاطر الرئيسية والهامة التي تهدد أمن نظم المعلومات المحاسبية الإلكترونية في المنشآت السعودية. ولقد قام الباحث بعمل دراسة تطبيقية مسحية مستخدماً فى ذلك قائمة إستقصاء معدة خصيصاً لهذا الغرض على عينة شملت ١٢٦ منشأة سعودية. ولقد أوضحت نتيجة الدراسة أن كثيراً من المنشآت التى شاركت فى الدراسة قد عانت من وجود خسائر مالية كبيرة بسبب التعديات على أمن نظم المعلومات المحاسبية بواسطة أشخاص من داخل وخارج تلك المنشآت. وتشير نتائج الدراسة أن أهم المخاطر التى تهدد أمن نظم المعلومات الإلكترونية فى المنشآت السعودية تمتثل فى الإدخال المتعمد وغير المتعمد لبيانات غير سليمة وكذلك التدمير غير المتعمد للبيانات من قبل موظفى المنشأة. كما يعد إشتراك موظفى المنشآت فى إستخدام نفس كلمات السر؛ وإدخال فيروسات إلى النظام المحاسبى؛ وتدمير أو طمس بعض مخرجات النظام المحاسبى؛ والكشف عن بعض المعلومات الهامة لإشخاص غير مرخص لهم بالإطلاع عليها؛ وكذلك توجيه بعض مخرجات الحاسب الألى إلى اشخاص غير مخول لهم بإستلامها والإطلاع عليها من المخاطر الهامة التى تهدد أمن نظم المعلومات الإلكترونية فى المنشآت السعودية. ومن ثم تبدو الحاجة ملحة لتدعيم الضوابط الرقابية على نقاط الضعف فى نظم الرقابة الداخلية المتعلقة بتلك المخاطر. وكذلك زيادة الوعى داخل المنشآت السعودية فيما يتعلق بأمن نظم المعلومات المحاسبية الإلكترونية لكى توفر الحماية الازمة والكافية ضد المخاطر الحالية والمحتملة التى تهدد أمن تلك النظم.

١. طبيعة المشكلة The Nature of the Problem

إن التطور السريع في تكنولوجيا المعلومات والإنتشار الواسع للنظم والبرامج الصديقة للمستخدم؛ بالاضافة إلى رغبة المنشآت في إقتناء وتطبيق أحدث النظم والبرامج الإلكترونية قد جعل من اليسير على تلك المنشآت إستخدام الحاسب الآلي ومكنها من أداء العديد من المهام والوظائف المحاسبية بصورة أسرع وأدق. ولكن على الجانب الأخر فإن هذا

---

* تم إجراء هذا البحث بتمويل من كلية الإدارة الصناعية- جامعة الملك فهد للبترول والمعادن- المملكة العربية السعودية.

التقدم التكنولوجي الهائل قد يحمل بين طياته العديد من المخاطر الهامة المتعلقة بأمن وتكامل النظم المحاسبية الإلكترونية، نظراً لأن التطور في الحاسبات وتكنولوجيا المعلومات لم يصاحبه تطوراً مماثلاً في الممارسات والضوابط الرقابية، كما لم يواكب ذلك تطوراً مماثلاً في معرفة وخبرات ووعي العاملين بتلك المنشآت.

ولقد أشار المعهد القومى للمعايير والتكنولوجيا (١٩٩٥) إلى أن النظم الإلكترونية تعد عرضة للعديد من التهديدات والمخاطر التى قد تصيب المنشأة بأنواع مختلفة من الأضرار والتى ينتج عنها خسائر جوهرية وهامة. وأن تلك الأضرار قد تتراوح بين مجرد الأخطاء التى قد تصيب تكامل قواعد البيانات إلى الحرائق التى قد تدمر مراكز الحاسب الآلى تماماً. وأن الخسائر قد تكون نتيجة حالات الغش والتلاعب من قبل موظفى المنشأت أو من قبل قراصنة المعلومات Hackers من خارج المنشأة؛ أو من الأهمال واللامبالاة Carelessعند إدخال البيانات. ومن ثم فإنه لا يمكن عمل تقديرات دقيقة للخسائر المتعلقة بأمن المعلومات نظراً لأن العديد منها لا يتم إكتشافها؛ والبعض الآخر يتم التكتم والتستر عليه وإخفاءه "Swept under the carpet" لتفادى الأثار غير المرغوبة نتيجة نشر تلك الخسائر للجمهور (National Institute of Standards and Technology, 1995).

إن تهديدات ومخاطر أمن نظم المعلومات المحاسبية يمكن أن تكون فى شكل تحريف المدخلات، سرقة وقت أجهزة الكمبيوتر وإستخدامه فى الأغراض الشخصية، سرقة البيانات / المعلومات، عدم الحفاظ على سرية البيانات، الدخول غير المصرح به للنظم والشبكات، الإستخدام غير المصرح به للبيانات، التلاعبات والإختلاسات، الغش فى إستخدام المعلومات، الخسائر الناتجة عن عدم تكامل المعلومات، التغيير المتعمد وغير المصرح به للبيانات، تخريب وتدمير بعض الملفات، فشل النظام وسقوط شبكة الإتصال، منع الأشخاص المخول لهم بالولوج الى النظام من ممارسة هذا الحقDenial of Services، الكوارث الطبيعية مثل الحرائق والفيضانات أو إنقطاع مصدر الطاقة، الكوارث غير الطبيعية والتى هى من صنع الإنسان مثل الحرائق المفتعلة وغيرها، إدخال فيروس الكمبيوتر للنظام، طمس أو تدمير بنود معينة من مخرجات الحاسب، خلق مخرجات زائفة / غير صحيحة، عمل نسخ غير مصرح (مرخص) بها من مخرجات الحاسب، الكشف (الإظهار) غير المرخص به للبيانات عن طريق عرضها على شاشات العرض أو طبعها على الورق؛ طبع وتوزيع المعلومات بواسطة أشخاص غير مصرح لهم بذلك، توجيه المطبوعات والمعلومات خطأً إلى أشخاص غير مخول لهم / ليس لهم الحق فى الإطلاع عليها أو الحصول على نسخة منها، تسليم المستندات الحساسة إلى أشخاص لا تتوافر فيهم الناحية الأمنية وذلك بغرض تمزيقها أو

التخلص منها، وكذلك مقاطعة تحويل البيانات من أماكن بعيدة (Schweitzer, 1987; OECD, 1992; Loch et al., 1992; Davis, 1996 and 1997; FFIEC, 1996; Henry, 1997; IFAC, 1998; Haugen and Selin,1999; Abu-Musa, 2003).

ويؤكد البعض على أن نظم المحاسبة الإلكترونية تتعرض لكثير من المخاطر والتهديدات ومنها التلاعب فى البيانات بقصد تدميرها سواء بالحذف، أو بالدمج غير الصحيح لبعضها، أو بخلطها ببيانات أخرى غير حقيقية أو تبوبها بشكل خاطىء تفقد معه مدلولها ومعناها؛ وأن ذلك التلاعب يمكن أن يحدث فى إجزاء مختلفة من نظام المعلومات المحاسبى كحسابات التكاليف، أو المخزون، أو النقدية، أو المبيعات، أو المصروفات، أو قد يكون تدمير البيانات ناتجاً عن تغيير (تعديل) فى البيانات(Data Change (Modification بشكل يجعلها لا تعبر عن الحقائق التى نتجت عنها أصلاً. وتتضمن أمثلة التغيير فى البيانات، التلاعب فى حسابات المدينين والدائنين بقصد الغش. وقد يحدث هذا التلاعب فى مراحل مختلفة من النظام مثل المدخلات أو التشغيل أو التخزين أو المخرجات. وأن تدمير البيانات قد يكون جزئياً أو كلياً وفى الحالة الأخيرة قد يصعب تصحيح البيانات أو إستعادتها، 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 إختلاسات فى أصول الشركة. وقد يهدف التلاعب بالنظام إلى الإطلاع على بيانات سرية Disclosure of confidential Data مثل بيانات تخطيط الربحية، أو بيانات الأفراد (الرواتب والترقيات والعلاوات). ويمكن للمتلاعب فى هذه الحالة ليس فقط الإطلاع على البيانات وإساءة إستخدامها بل أيضاً سرقة بعضها أو كلها. ذلك كله قد ينتج عنه خسائر للمنشأت تكون كبيرة فى بعض الحالات (سمير هلال، ١٩٩٢، ص ٥٨-٥٩).

إن مخاطر وتهديدات أمن نظم المعلومات المحاسبية الإلكترونية يمكن تصنيفها وتبويبها من وجهات نظر مختلفة. حيث يمكن تبويب المخاطر من حيث ***مصدرها*** إلى: مخاطر داخلية Internal ومخاطر خارجية External. وتجدر الإشارة إلى أن موظفى المنشأت يمثلون المصدر الرئيسى للمخاطر الداخلية؛ بينما يمثل المغامرون وقراصنة المعلومات Haekers والكوارث الطبيعية Natural Disasters أهم المصادر الخارجية للمخاطر. وتشير معظم الدراسات السابقة إلى خطورة المخاطر والتهديدات الداخلية وجوهرية قيمة الخسائر الناتجة عنها مقارنةً بالمخاطرالخارجية؛ نظراً لأن موظفي المنشأت غير الأمناء يكون لديهم صلاحيات الدخول إلى النظام والوصول إلى البيانات؛ ومن ثم إمكانية تدميرها أو تحريفها أو تعديلها؛ بالإضافة إلى أنهم أكثر درايةً ومعرفةً من غيرهم بنقاط الضعف ونواحى

القصور فى الضوابط الرقابية Controls المطبقة بالمنشأة. أما المخاطر الخارجية فلا تقل أهمية عن المخاطر الداخلية نظراً لأن قراصنة المعلومات عادةً مايستغلون مهاراتهم العالية فى الحاسب الألى وتكنولوجيا المعلومات فى الدخول غير القانونى إلى النظم والبرامج بهدف التلاعب فى البيانات أو تدميرها أو بهدف السرقة والإختلاس، كما أن بعض المنافسين Competitors قد يحاولون إختراق الضوابط الرقابية والأمنية للنظام بهدف الإطلاع على بعض المعلومات السرية مثل بيانات التكاليف والربحية وخطط المنشأة المستقبلية. بينما قد تسفر بعض الكوارث الطبيعية مثل الزلازل والبراكين عن تدمير كلى أوجزئى لأصول المنشأة مثل أجهزة الحاسب الألى والبرامج والبيانات الأدوات المساعدة (Price et al., 1989; Weingartner. and Burton, 1991; Rainer, et al.1991; Loch et al., 1992; Davis, 1996 and 1997; FFIEC, 1996; Henry, 1997; IFAC, 1998; Bandyopadhyay et al., 1999; Haugen and Selin,1999; Abu-Musa, 2003).

بينما يمكن تصنيف المخاطر بناءً على **المتسبب** فيها The Perpetrator إلى مخاطر ناتجة عن **العنصر البشرى** Human Threats ومخاطر ناتجة عن **العنصر غير البشرى** Non-Human. وتجدر الإشارة إلى أن المخاطر الناتجة عن العنصر البشرى قد تكون نتيجة بعض التصرفات البشرية غير المتعمدة (نتيجة الخطأ أو السهو) أو المتعمدة بقصد الغش والتلاعب. أما المخاطر الناتجة عن **العنصر غير البشرى** فتمثل المخاطر التى ليس للإنسان دخل فيها والتى تكون نتيجة الزلازل والبراكين والأعاصير وغيرها من الكوارث الطبيعية.

ويمكن تبويب المخاطر على أساس **العمدية** Intention إلى مخاطر ناتجة عن تصرفات **متعمدة أو مقصودة** Intentional مثل الإدخال المتعمد لبيانات غير صحيحة أو التدمير المتعمد للبيانات؛ أومخاطر نتيجة تصرفات عفوية **وغير متعمدة أو غير مقصودة** Accidental مثل الإدخال أوالتدمير غير المتعمد للبيانات نتيجة السهو أو الخطأ كما سبق الذكر. ويرى البعض "أن غالبية المخاطر الناتجة عن تصرفات غير متعمدة Uninentional على الرغم من إنها تكون مكلفة فى أحيان كثيرة؛ إلا أنها فى معظم الأحيان يمكن تصحيحها Corrected أو تفاديها Avioded بمزيد من التدريب للموظفين وحسن الإشراف عليهم. وعلى الجانب الآخر فإن التصرفات المقصودة أو المتعمدة عادة ما تقصد إلى إرتكاب بعض جرائم الكمبيوتر وتدمير بعض الملفات الهامة أو بعض مكوناتها وبغرض إخفاء أثار حالات الغش والتلاعب وسرقة بعض الأموال أو سرقة بعض البيانات الهامة. وعادةً ما يكون ذلك بإلغاء Deleating أو تعديل وتحريف Altrenting بيانات بعض

السجلات والملفات أو خلق معلومات مضللة وغير صحيحة" (Haugen & Selin 1999).

وتجدر الإشارة إلى أنه يمكن تصنيف المخاطر بناءً على **الآثار الناتجة** عنها Consequences إلى **مخاطر ينتج عنها أضرار مادية** Physical Damage للنظام وأجهزة الحاسب الآلى أو التدمير المادى لوسائل تخزين البيانات مثل الشرائط والأقراص الممغنطة؛ والتى قد تنتج من بعض الظواهر الطبيعية كالفياضانات والزلازل والبراكين أو إنقطاع التيار الكهربائى؛ أومن سقوط النظم أو الشبكات لفترات معينة. أو **مخاطر فنية ومنطقية** Technical or Logical والتى قد تصيب البيانات الموجودة فى ذاكرة الحاسب الآلى أو على الشرائط الممغنطة؛ وقد يكون ذلك بتحريف البرامج وإدخال جراثيم للكمبيوتر والتى قد تؤثر سلبياً على مدى إتاحة البيانات Availability عند الحاجة اليها؛ وذلك بحجبها عن الأشخاص المخول لهم حق الإطلاع عليها أو إستخدامها Denial of use؛ أو الإفصاح عن البيانات السرية لأشخاص غير مخول لهم بالإطلاع عليهاConfidentionlity والتى قد تؤثر على الموقف التنافسى للمنشأة أو التأثير على تكامل Integrity البيانات والبرامج داخل النظام (OECD,1992).

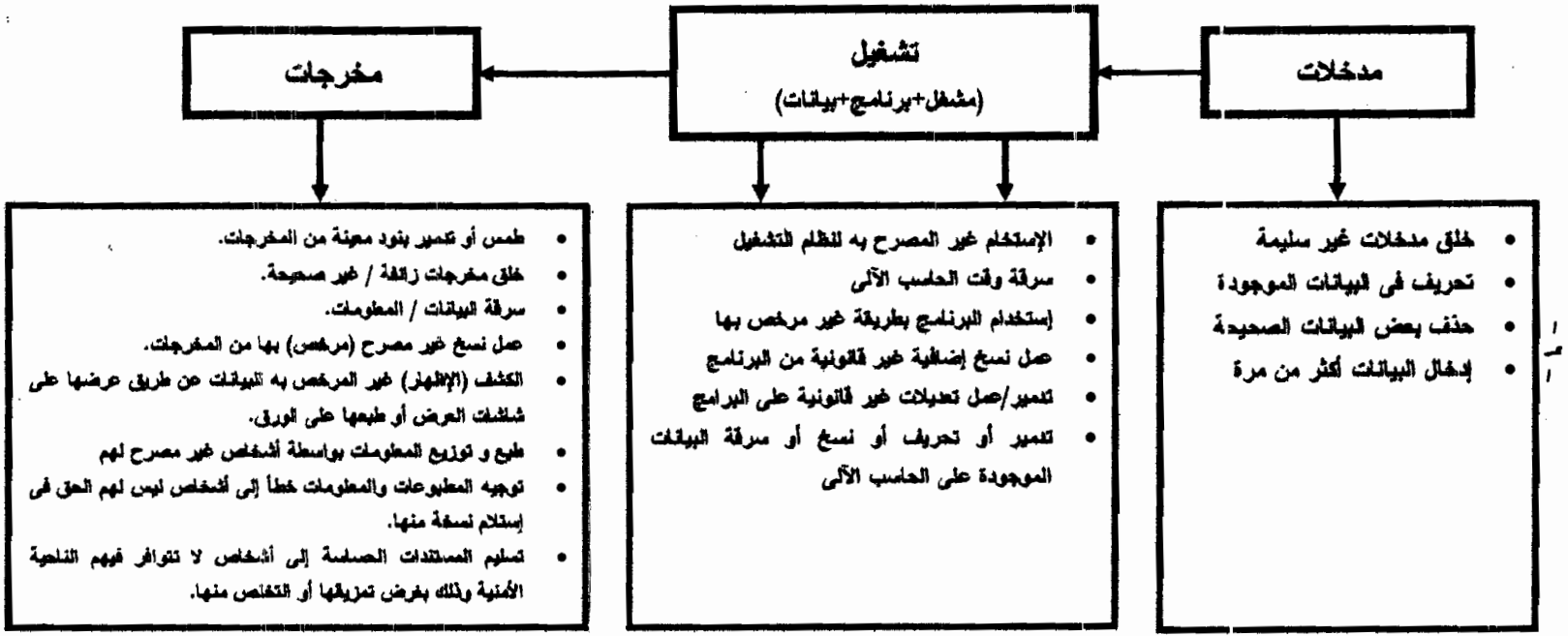
وأخيراً فإنه يمكن تصنيف المخاطر على أساس علاقتها بمراحل النظام إلى: مخاطر المدخلات Input؛ مخاطر التشغيل Processing؛ ومخاطر خاصة بمخرجات Output الحاسب الآلى (شكل ١).

أ. مخاطر المدخلات

وتتمثل المخاطر أو التهديدات المتعلقة بأمن المدخلات فى:-

١. خلق بيانات غير سليمة Creation of Input

ويكون ذلك بخلق بيانات زائفة وغير صحيحة ولكن بإستخدام نماذج ومستندات سليمة وإدخالها خلسة داخل رزم العمليات بدون أن يتم إكتشافها. ومن أمثلة ذلك إدخال مستندات للمصروفات الإضافية داخل رزمة المصروفات الموجودة أو إدخال أمر بيع مباشر مع قيود المبيعات، وقد يصعب إكتشاف ذلك خاصة فى حالة عدم وجود مستندات ورقية للعمليات. وقد يكون ذلك الغش والتلاعب فى البيانات الدائمة Standing Data مثل إدخال أسماء وهمية ضمن كشوف المرتبات مما يترتب عليه صرف مرتبات شهرية لموظفين وهميين؛ أو تعديل فى معدلات الفائدة لبعض العملاء. وقد يكون التلاعب فى بيانات العمليات Transactions Data مثل إدخال فاتورة وهمية بإسم أحد الموردين.



(شكل ١)

(مخاطر أمن نظم المعلومات المحاسبية الإلكترونية طبقاً لمراحل النظام)

٢. تعديل أو تحريف فى بيانات المدخلات Amedment of Input

ويكون ذلك بالتلاعب فى المستندات والمدخلات الأصلية بعد إعتمادها من الشخص المسئول ولكن قبل إدخالها إلى الحاسب الآلى؛ وقد يحدث ذلك بزيادة رقم المصروف الفعلى الموجود بالمستند، أو تغيير إسم أو عنوان مقدم طلب القرض؛ أو تغيير وتعديل معدل الفائدة على بعض العمليات. فعلى سبيل المثال قد تم إكتشاف وجود إتفاق سرى بين أحد مدخلى البيانات وبعض العملاء فى إحدى المنشأت يقوم بمقتضاه الموظف المختص بإدخال البيانات بتخفيض سعر الفائدة على القروض الخاصة بهؤلاء العملاء عند إدخاله لبيانات القروض إلى الحاسب الآلى على أن يتم تقسيم الوفر مناصفة بينه وبين مقدمى طلبات القروض.

٣. حذف بعض المدخلات Deletion of Input

ويكون ذلك بحذف بعض المستندات كلية أو إستبعاد بعض البيانات قبل إدخالها إلى الحاسب الآلى وذلك بحذف المستند من رزمة السجلات Batch of Records أو حتى حذف الرزمة بالكامل. فعلى سبيل المثال قد إعتاد الموظف المسئول عن المرتبات فى منشأة ما على تدمير مذكرات إنهاء تعاقد الموظفين Employee Termination Notices بالمنشأة وتعديل تفصيلات حساب البنك بحيث يدفع المرتب فى حساب خاص بالموظف الذى قام بالتلاعب فى الحسابات (Huntington and Davies ,1994).

٤. إدخال البيانات أكثر من مرة Duplication of Input

ويكون ذلك بإختيار بعض المستندات وإدخال بياناتها أكثر من مرة إلى النظام مثل أوامر الدفع، أو أوامر تسليم المخزون وذلك لتشغيلها أكثر من مرة لصالح القائم بعملية الإختلاس أوالتلاعب؛ ويكون ذلك إما بعمل نسخ إضافية من مستندات المدخلات الأصلية وتقديم كل من الأصل والصورة لإدخالها للحاسب الألى، أو بإعادة إدخال بيانات المستند الأصلى مرة آخرى وذلك فى حالة عدم إلغاء المستندات التى يتم إدخالها والتأشير عليها بما يفيد ذلك. ولقد أشار Huntington and Davies, 1994 إلى أن التلاعب والتحريف Alteration فى البيانات الدائمة Standing Input يكون من الصعب إكتشافه لأن مصدر التلاعب هو عملية واحدة وحدث غير متكرر؛ وذلك بعكس بيانات العمليات المتكررة Transaction Data .

ب. مخاطر تشغيل البيانات

وينصب تأثير تلك المخاطر بصفة أساسية على البيانات المخزنة فى ذاكرة الحاسب والبرامج التى تقوم بتشغيل تللك البيانات. وتتمثل مخاطر تشغيل البيانات فى: تعديل وتحريف Modifing البرامج؛ عمل نسخ غير قانونية من البرامج؛ إستخدام البرنامج بطريقة غيرمصرح أو مرخص بها؛ إدخال القنابل الموقوته Logic Bombs والجراثيم Viruses إلى أجهزة الحاسب الألى؛ تحريف وتعديل البرامج Altering بإستخدام حصان طروادة Trojan Hourse أو إسلوب سلامى salami Technique أو غيرها من الأساليب التى تحتاج إلى خبرات متخصصة فى الحاسب الآلى والبرمجة. فعلى سبيل المثال يمكن إعطاء أوامر للبرنامج بأن لا يسجل أى قيود فى السجلات المالية عندما يتم بيع البضاعة إلى شخص أو إسم معين بالذات أو حساب العمولة Commision على أساس إجمالى المبيعات. وقد يكون ذلك بتحريف البيانات المخزنة فى ذاكرة الحاسب أو تدميرها أوعمل نسخ غير قانونية منها وإستخدامها بطريقة غير مشروعة؛ أو البحث غير القانونى خلالها أو حتى مجرد الإطلاع عليها بدون الحصول على ترخيص مسبق بذلك.

ج. مخاطر مخرجات الحاسب

إن مخاطر مخرجات الحاسب تتمثل فى سرقة مخرجات Stelling الحاسب أو إساءة إستخدامها Misuing أو توجيهها إلى أشخاص غير مصرح لهم بإستلامها أوالإطلاع عليها نظراً لسريتها أو لأنهم غير مخول لهم صلاحيات الإطلاع عليها. ولقد أشار McIntyre 1999 إلى أن واحداً من أضعف الحلقات فى سلسلة أمن المعلومات تتمثل فى إعطاء وتسليم بعض المستندات الهامة إلى أشخاص لا تتوافر فيهم المقومات الأمنية Non-Security Cleared Presonnel وذلك بغرض تمزيقها والتخلص منها Shredding. كما أن كشف البيانات السرية للغير تعد من المخاطر الهامة؛ بالإضافة إلى خلق بيانات زائفة.

ومن ثم فلقد أصبح أمن المعلومات التى تحتويها النظم الإلكترونية، وخاصة المالية والمحاسبية، موضع إهتمام وقلق لإدارات المؤسسات والمنشأت 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 وإحتمالات المخاطر المحيطة بهذه النظم والتى تهدد صحة وموثوقية وسرية وتكامل البيانات المالية والمحاسبية فيها، وذلك نتيجة لعوامل منها:-

- التقدم التقنى فى صناعة الحاسبات، وزيادة وتنوع البرامج المتاحة أدى إلى سهولة نسخ وتعديل وتغيير البيانات والملفات فى أوقات قياسية وبسيطة لا تستطيع ضوابط الحماية (الرقابة) التقليدية متابعتها.
- زيادة خبرة الأفراد، بصفة عامة، فى إستخدام الحاسبات الآلية نتيجة لإنخفاض أسعارها وإنتشارها فى مجالات متعددة، أدى إلى سهولة التغلب على الوسائل التقليدية لتأمين المعلومات فى النظم الإلكترونية.
- إتصال نظم المعلومات الإلكترونية ببعضها البعض من خلال شبكات الإتصال العامة (الهواتف مثلاً)، أتاح فرصة للمغامرين للدخول إلى شبكات معلومات محلية وعالمية، والتلاعب فى بياناتها (سمير هلال ١٩٩٢).

ويهدف هذا البحث إلى التعرف على أهم المخاطر التى تهدد أمن نظم المعلومات المحاسبية الإلكترونية فى المنشأت السعودية؛ وكذلك إختبار جوهرية الفروق فيما يختص بتقييم المنشأت المختلفة لدرجة خطورة تلك التهديدات على أمن نظم معلوماتها المحاسبية. ولتحقيق ذلك الهدف قام البحث بإجراء دراسة تطبيقية على عينة من المنشأت السعودية مستخدماً فى ذلك قائمة إستقصاء أعدت خصيصاً لهذا الغرض. ولقد تضمن الإستقصاء قائمة بأهم المخاطر المحتملة والتى يمكن أن تهدد أمن نظم المعلومات المحاسبية الإلكترونية لإختبارها ميدانياً فى بيئة الأعمال السعودية. وتجدر الإشارة إلى أن قائمة المخاطر المقترحة قد تم تطويرها بناءً على نتائج بعض الدراسات السابقة والبحوث المنشورة فى هذا المجال، كما تضمنت القائمة عدداً من المخاطر المحتملة التى يتم إختبارها للمرة الأولى فى هذا البحث فى المملكة العربية السعودية. ويعد هذا البحث محاولة للإجابة على التساؤلين الآتيين:-

١. ما هى أهم المخاطر التى تواجه أمن نظم المعلومات المحاسبية الإلكترونية فى المنشأت السعودية؟
٢. هل توجد إختلافات جوهرية بين المنشأت السعودية فيما يتعلق بمدى إدراكها وتقديرها لأهمية المخاطر المختلفة التى تهدد أمن نظم معلوماتها المحاسبية الإلكترونية؟

٢. هدف البحث The Research Objective

يهدف هذا البحث إلى التعرف على المخاطر الهامة التى تهدد أمن نظم المعلومات المحاسبية الإلكترونية فى بيئة منشأت الأعمال السعودية؛ وإختبار الفروق الجوهرية بين تلك

المنشآت المختلفة فيما يختص بمدى إدراكها لدرجة أهمية وخطورة تلك التهديدات على حالة الأمن فى نظم معلوماتها المحاسبية الإلكترونية.

٣. أهمية البحث The Importance of the Research

تنبع أهمية هذا البحث من أهمية الموضوع ذاته؛ حيث أن نظم المعلومات المحاسبة الالكترونية قد أصبحت عرضة للعديد من المخاطر التى تهدد صحة Accuracy وموثوقية Reliability ومصداقية Validity وسرية Confidentiality وتكامل Integrity ومدى إتاحية Avaliability البيانات المالية والمحاسبية التى توفرها تلك النظم.. نظراً لأن التطور الكبير في تكنولوجيا المعلومات وصناعة الحاسبات الألية والذى أدى إلى سهولة نسخ وتعديل وتغيير البيانات والملفات المخزنة بذاكرة الحاسب؛ لم يصاحبه تطوراً مماثلاً في الممارسات والضوابط الرقابية المطبقة بتلك المنشآت.

إن مراجعة الأدب المحاسبى والدراسات السابقة المتعلقة بأمن نظم المعلومات المحاسبية الإلكترونية قد أسفرت عن وجود خلط واضح وعدم تمييز بين مخاطر أمن نظم المعلومات Security Threats وعدم كفاية الضوابط الرقابية لأمن تلك النظم Inadequacy of Security Controls فى معظم الدراسات التى تمت فى هذا المجال (إنظر على سبيل المثال Loch et al. 1992; Davis, 1997; Ryan and Bordoloi, 1997; and Henry, 1997). فلقد إعتبرت تلك الدراسات ضعف أو عدم كفاية بعض الأدوات والضوابط الرقابية المتعلقة بأمن نظم المعلومات المحاسبية الإلكترونية على أنها تهديدات أو مخاطر لأمن تلك النظم (على سبيل المثال: ضعف الرقابة على وسائل الإتصال media مثل الشرائط والأقراص الممغنطة؛ ضعف الرقابة على المناولة اليدوية لمدخلات ومخرجات الحاسب؛ ضعف أو عدم كفاية الرقابة المادية على النظام؛ عدم كفاية الرقابة على وسائل حفظ وتحزين المعلومات؛ ضعف الرقابة المادية على الولوج للنظام؛ عدم وجود نظام جيد للمراجعة والفحص؛ عدم عمل نسخ إضافية من البيانات؛ عدم وجود رقابة على قراءة وتحديث وتعديل البيانات؛ عدم وجود حدود واضحة لصلاحيات الوصول إلى بيانات أو ملفات معينة؛ عدم الفصل الجيد بين الوظائف المحاسبية؛ وكذلك عدم الفصل الجيد بين وظائف ومهام نظم المعلومات. ولقد أشار بعض الباحثين (Ryan and Bordoloi, 1997) صراحة إلى أن قائمة المخاطر الواردة فى دراستهم قد إشتملت على بعض البنود التى لايمكن إعتبارها من

مخاطر أمن نظم المعلومات بالمعنى الحرفى أوالدقيق؛ ولكنهم قد ضمنوها فى قائمة المخاطر لإعتقادهم بأهمية تلك البنود لإدارة تكنولوجيا المعلومات وتحسين الممارسات الموجودة.

وتجدر الإشارة إلى أن البحث الحالى قد عالج هذه المشكلة وذلك بالتمييز والفصل الجيد بين المخاطر أو التهديدات Security Threats وضعف وسائل الحماية أو الضوابط الرقابية Security Controls المتعلقة بأمن نظم المعلومات المحاسبية الإلكترونية. حيث إستبعد الباحث البنود والعناصر المتعلقة بضعف وعدم كفاية الأدوات والضوابط الرقابية لأمن نظم المعلومات المحاسبية الإلكترونية من قائمة المخاطر والتهديدات المقترحة والتى تم إختبارها ميدانياً على عينة من المنشأت السعودية. فلقد تضمنت قائمة المخاطر والتهديدات المقترحة عدداً من المخاطر والتهديدات الخاصة بأمن نظم المعلومات المحاسبية الإلكترونية التى تم إختيارها بعناية من بعض الدراسات السابقة (على سبيل المثال: Loch et al., 1992; Davis, 1996 and 1997; FFIEC, 1996; and Henry, 1997) التى تمت فى هذا المجال والتى ينطبق عليها المعنى الدقيق للمخاطر. كما إشتملت القائمة المقترحة على عدد من المخاطر والتهديدات التى يتم إختبارها ميدانياً للمرة الأولى فى بيئة الأعمال السعودية (ملحق ١).

وتجدر الإشارة إلى أن الدراسات السابقة قد ركزت على مخاطر أمن نظم المعلومات المتعلقة بمرحلتى إدخال Input وتشغيل Processing البيانات؛ وأهملت تماماً المخاطر المرتبطة بمرحلة هامة وحيوية من مراحل النظام وهى مخرجات الحاسب الآلى. ومن ثم فلقد تضمنت قائمة المخاطر المقترحة فى هذا البحث عدداً من المخاطر المتعلقة بأمن مخرجات الحاسب الآلى؛ والتى تختبر لأول مرة فى هذا البحث فى بيئة الأعمال السعودية ومنها على سبيل المثال: طمس أو تدمير بنود معينة من المخرجات؛ خلق مخرجات زائفة / غير صحيحة؛ سرقة البيانات / المعلومات؛ عمل نسخ غير مرخص بها من المخرجات؛ الكشف (الإظهار) غير المرخص به للبيانات عن طريق عرضها على شاشات العرض Computer Screens أو طبعها على الورق؛ طبع وتوزيع المعلومات بواسطة أشخاص غير مصرح لهم بذلك؛ توجيه المطبوعات والمعلومات عن طريق الخطأ إلى أشخاص غير مخول لهم / ليس لهم الحق فى إستلام نسخة منها؛ وكذلك تسليم المستندات الحساسة إلى أشخاص لا تتوافر فيهم الناحية الأمنية وذلك بغرض تمزيقها أو التخلص منها (ملحق ١).

وتجدر الإشارة إلى أن البحث الحالى قد إختبر جوهرية وأهمية المخاطر التى تهدد أمن نظم المعلومات المحاسبية الإلكترونية بطريقة مختلفة تماماً عما تم فى الدراسات السابقة. فلقد حاولت الدراسات السابقة تطوير قائمة بمخاطر أمن نظم المعلومات الإلكترونية وإختبار

أهم تلك المخاطر فى بيئات أجهزة الحاسب الألى المختلفة وذلك بسؤال الأشخاص المشاركين فى الإستبيان بأن يقوموا بإختيار وترتيب Ranking أهم ثلاثة مخاطر تواجه أمن نظم المعلومات الإلكترونية من بين بنود قائمة المخاطر المقترحة. ومن ثم فإن عملية ترتيب أهمية تلك المخاطر تعد عملية تقدير شخصى تماماً للشخص المشارك فى الإستبيان، حيث لم تعطى له إى معايير Criteria أو تعليمات واضحة Clear Guidelines يتم على أساسها إجراء عملية الترتيب (على سبيل المثال: معدل تكرار حدوث الخطر، أو قيمة الخسائر الناتجة عن حدوث الخطر إلخ) والتى يمكن أن تساعد فى ترشيد إتخاذ ذلك القرار.

ومن ثم فإن ترتيب أهمية المخاطر فى الدراسات السابقة يمكن أن يختلف من شخص إلى أخر طبقاً لخبراته ومركزه الوظيفى ومدى إتاحة أو توافر البيانات، وكذلك مدى إدراكه الشخصى لطبيعة وأهمية المخاطر، وربما طبيعة الشخص ذاته (متفائل أو متشائم) وكذلك المعايير التى يبنى عليها هذا الشخص تقديره ويتخذ قراره بعمل ترتيب معين للمخاطر. أما فى البحث الحالى فإنه قد تم إختبار أهمية مخاطر أمن نظم المعلومات المحاسبية الإلكترونية على أساس معدل تكرار حدوث تلك المخاطر فى منشأة ما خلال السنوات الماضية. ولقد تم إستخدام معدل تكرار الحدوث كمقياس بديل عن أهمية هذا الخطر وخطورته على أمن نظم المعلومات المحاسبية الإلكترونية.

ولقد تم ملاحظة أيضاً أن معظم الدراسات السابقة المتعلقة بمخاطر أمن نظم المعلومات المحاسبية الإلكترونية قد تمت فى بعض الدول المتقدمة مثل الولايات المتحدة الأمريكية وبريطانيا، ولذلك فإنه من المتوقع أن يسفر هذا البحث عن نتائج هامة بتطبيقة على المملكة العربية السعودية؛ وذلك للتعرف على المخاطر التى تواجه أمن نظم المعلومات المحاسبية الإلكترونية فى بيئات الأعمال بالدول النامية. وتجدر الإشارة الى أن التعرف على المخاطر التى تهدد أمن نظم المعلومات المحاسبية الإلكترونية يعد خطوة ضرورية وهامة لتشخيص نقاط الضعف فى نظم الرقابة الداخلية؛ ومن ثم وضع مجموعة من الضوابط والأدوات الرقابية الجيدة لحماية تلك النظم ضد تلك المخاطر المحتملة وتخفيض أثارها السلبية المحتملة إلى أقل حد ممكن.

٤. فروض البحث The Research Hypotheses

يعد هذا البحث محاولة للتعرف على مدى إدراك المنشأت السعودية للمخاطر الهامة التى تهدد أمن نظم المعلومات المحاسبية الإلكترونية بها، والتعرف على الإختلافات الجوهرية

فيما يتعلق بدرجة تقييمها لمعدلات تكرار حدوث تلك المخاطر وذلك من خلال إختبار الفرض الإحصائى التالى:

الفرض العدمى: لا توجد إختلافات جوهرية بين المنشأت السعودية فيما يختص بمدى إدراكها لأهمية المخاطر المختلفة التى تهدد أمن نظم معلوماتها المحاسبية الإلكترونية ودرجة تقييمها لمعدلات حدوث تلك المخاطر.

الفرض البديل: توجد إختلافات جوهرية بين المنشأت السعودية فيما يختص بمدى إدراكها لأهمية المخاطر المختلفة التى تهدد أمن نظم معلوماتها المحاسبية الإلكترونية ودرجة تقييمها لمعدلات حدوث تلك المخاطر.

٥. الدراسات السابقة Literature Review

إن مراجعة الدراسات السابقة والبحوث المنشورة المتعلقة بمخاطر أمن نظم المعلومات المحاسبية الإلكترونية يكشف لنا اللثام عن ندرة واضحة فى الأبحاث والدراسات التى تمت فى هذا المجال. ولعل أحد الأسباب المحتملة لتلك الندرة قد يرجع إلى الحداثة النسبية لهذا الموضوع رغم أهميته الحيوية لكثير من المنشأت. وتجدر الإشارة إلى أن الأبحاث القليلة التى تمت فى هذا الموضوع قد إستهدفت التعرف على المخاطر المحتملة التى قد تواجه أو تهدد أمن تلك النظم والتعرف على أسبابها ومحاولة تطوير قائمة تتضمن أهم المخاطر التى قد تواجه أمن النظم المحاسبية الإلكترونية؛ ومن ثم محاولة إختبار مدى جوهرية وأهمية تلك المخاطر فى الواقع العملى من خلال مجموعة من الدراسات الميدانية التى تمت فى هذا الشأن؛ وذلك من خلال التعرف على معدل تكرار حدوثها وحجم الخسائر المالية الناجمة عنها.

وتعد الدراسة التى قام بها Loch وآخرون (١٩٩٢) من الدراسات الأولى والرائدة فى هذا المجال. فلقد قام الباحثون بعمل دراسة مسحية survey إستهدفت إستكشاف مدى إدراك مديرى نظم المعلومات الإدارية فيما يتعلق بالمخاطر الأمنية التى تواجه أمن النظم المحاسبية الإلكترونية فى بيئة الحاسبات الشخصية Microcomputer والحاسبات الكبيرة Mainframe وكذلك شبكة الحاسبات الإلكترونية Network .

ولقد قام الباحثون بتطوير قائمة تضمنت إثنتى عشرة من المخاطر المحتملة التى قد تواجه أمن نظم المعلومات المحاسبية الإلكترونية بناءً على الأبحاث النظرية المتاحة وكذلك

محاولة إختبار مدى وجود وأهمية تلك المخاطر عملياً من خلال البحث الميدانى. ولقد تضمنت تلك القائمة المخاطر التالية:-

١. الإدخال غير المتعمد (غير المقصود) لبيانات غير سليمة بواسطة موظفى المنشأة .
٢. الإدخال المتعمد (المقصود) لبيانات غير سليمة بواسطة موظفى المنشأة.
٣. التدمير غير المتعمد للبيانات بواسطة موظفى المنشأة.
٤. التدمير المتعمد للبيانات بواسطة موظفى المنشأة.
٥. المرور (الوصول) غير المرخص Unauthorized للبيانات / النظام بواسطة موظفى المنشأة .
٦. الرقابة غير الكفاية Inadequate Control على الوسائل Media مثل الأشرطة والأقراص الممغنطة.
٧. الرقابة الضعيفة Poor Control على المناولة اليدوية لمدخلات ومخرجات الحاسب الألى.
٨. الوصول غير المرخص به للبيانات / النظام بواسطة أطراف خارجية (قراصنة المعلومات Hackers).
٩. الوصول غير المرخص به للبيانات / النظام من قبل المنافسون Competitors.
١٠. إدخال فيروسات الكمبيوتر إلى النظام أو البرامج.
١١. الأدوات الرقابية المادية غير الكافية Inadequate Physical Controls .
١٢. الكوارث الطبيعية مثل الحرائق والفيضانات أو إنقطاع مصدر الطاقة وغيرها.

ولقد قام Loch وآخرون (١٩٩٢) بعمل دراسة مسحية Empirical Survey شملت ٦٥٧ من مديرى نظم المعلومات الإدارية فى الولايات المتحدة. ولقد طلب من المشاركين فى الدراسة أن يقوموا بترتيب أهم ثلاث مخاطر فيما يتعلق بأمن نظم المعلومات المحاسبية الإلكترونية من بين بنود القائمة المقترحة للمخاطر. ولقد أوضحت نتائج تلك الدراسة أن الكوارث الطبيعية والأحداث غير المقصودة Accidental Actions لموظفى المنشأة قد تم تصنيفها ضمن الثلاث مخاطر الهامة فى جميع بيئات تكنولوجيا المعلومات. كما أعطى المشاركون فى الدراسة أهمية أكبر للمخاطر الداخلية مقارنة بالمخاطر الخارجية لأمن نظم المعلومات المحاسبية الإلكترونية. كما أظهرت الدراسة أن التدمير غير المتعمد للبيانات والإدخال غير المتعمد لبيانات غير سليمة بواسطة موظفى المنشأة وكذلك الرقابة غير الكافية على الوسائل Media مثل الأشرطة والأقراص الممغنطة تعد أهم ثلاث مخاطر تواجه أمن نظم المعلومات فيما يتعلق بأجهزة الحاسب الشخصية Microcomputer.

بينما أوضحت الدراسة أن أهم ثلاث مخاطر تتعلق بأجهزة الحاسب الألى الكبيرة Mainframe تتمثل فى الإدخال غير المتعمد لبيانات غير سليمة من قبل موظفى المنشأة؛ الكوارث الطبيعية؛ والتدمير غير المتعمد للبيانات بواسطة موظفى المنشأة. بينما أظهرت الدراسة أن الكوارث الطبيعية والدخول غير المصرح به للبيانات / النظام من قبل أطراف خارجية (قراصنة المعلومات) وضعف الأدوات الرقابية المادية تعد أهم ثلاث مخاطر تهدد أمن نظم المعلومات المحاسبية الإلكترونية فى بيئة شبكة الحاسب الآلى Network Enviroment.

ويرى الباحث أنه على الرغم من أن دراسة Loch وآخرون (١٩٩٢) تعد من الدراسات الرائدة فى هذا المجال؛ إلا أنه قد يوجه إليها بعض الإنتقادات الهامة منها أن قائمة المخاطر المقترحة قد تضمنت بعض العناصر التى لايمكن تبويبها وتصنيفها كمخاطر لأمن نظم المعلومات الإلكترونية بصورة دقيقة. فلقد إعتبر Lock ومساعديه ضعف بعض عناصر وأدوات الرقابة ضمن مخاطر أمن النظم (على سبيل المثال ضعف الرقابة على الأقراص الممغنطة والشرائط؛ وكذلك ضعف الرقابة على المناولة اليدوية لمدخلات ومخرجات الحاسب؛ وضعف الرقابة المادية على النظام). ولعل هذا يثير بعض الجدل حول المقولة: أن ضعف البوليس فى حد ذاته لا يخلق الجريمة Weak Policing dose not Itself Create the Crime.

وتجدر الإشارة إلى أن الباحث قد قام بإختيار عدد من مخاطر أمن نظم المعلومات المحاسبية الإلكترونية التى تضمنتها قائمة Loch et. al (1992) لإختبار مدى تكرار حدوثها وأهميتها النسبية فى البيئة السعودية. بينما تم إستبعاد بعض المتغيرات الأخرى (مثل ضعف الرقابة على الأدوات والوسائل الإلكترونية لحفظ وتخزين المعلومات؛ وكذلك ضعف الرقابة على المناولة اليدوية لمدخلات ومخرجات الحاسب الآلى؛ وكذلك ضعف الرقابة المادية) من القائمة المقترحة لمخاطر وتهديدات أمن نظم المعلومات المحاسبية الإلكترونية. كما تضمنت القائمة المقترحة أيضاً عدداً من المخاطر والتهديدات التى يتم إختبارها عملياً لأول مرة فى بيئة الأعمال السعودية.

ونظراً لأن أمن نظم المعلومات المحاسبية الإلكترونية يعد محور إهتمام كثير من الأطراف خاصة مراجعى نظم المعلومات Information Systems Auditors فلقد قام ديفس Davis (1996) بمحاولة إستكشاف حالة أمن نظم المعلومات المحاسبية فى الواقع العملى من خلال دراسة تطبيقية شملت عينة عشوائية من أعضاء جمعية مراقبة ومراجعة نظم المعلومات Information Systems Audit and Control Association

(ISACA) وكذلك أعضاء مجمع المحاسبين القانونين الأمريكى American Institute of Certified Public Accountants (AICPA). ولقد إستخدم Davis نفس قائمة المخاطر المقترحة من قبل Loch et. al. (1992) بعد إضافة أربعة من المخاطر المحتملة عليها وهى:

- عدم الفصل بين الوظائف المحاسبية (إعتماد العمليات – التسجيل – الحفظ).
- عدم الفصل بين الوظائف المتعلقة بنظم المعلومات (البرمجة – التشغيل).
- مقاطعة تحويل البيانات من أماكن متفرقة.
- التطورات التكنولوجية أسرع من التطور فى عناصر وأدوات الرقابة.

ولقد أشارت نتائج دراسة Davis (1996) إلى أن إدخال بيانات غير سليمة بصورة غير متعمدة؛ والتدمير غير المتعمد للبيانات بواسطة موظفى المنشأة؛ وكذلك إدخال فيروسات الكمبيوتر إلى النظام قد تم إعتبارها أهم المخاطر التى تهدد أمن نظم المعلومات المحاسبية الإلكترونية فى بيئة الحاسبات الشخصيةMicrcomputer Environment. بينما يعد الدخول غير المرخص به للبيانات / للنظام بواسطة موظفى المنشأة؛ الإدخال غير المتعمد لبيانات غير سليمة من قبل موظفى المنشأة؛ وعدم الفصل بين المهام والوظائف المتعلقة بنظم المعلومات قد أعتبرت من أهم المخاطر التى تهدد أمن نظم المعلومات فى بيئة الحاسبات الألية الصغيرة Mincomputer Environment.

أما فيما يختص ببيئة الحسابات الألية الكبيرة Mainframe فلقد أظهرت نتيجة الدراسة أن أهم ثلاث مخاطر تواجه أمن نظم المعلومات هى: الإدخال غير المتعمد لبيانات غير سليمة بواسطة موظفى المنشأة؛ وكذلك الكوارث الطبيعية؛ والدخول غير المصرح به للبيانات / النظام بواسطة موظفى المنشأة. بينما يعد الدخول غير المرخص به للبيانات / النظام من قبل موظفى المنشأة وكذلك من قبل قراصنة المعلومات Hackers؛ بالإضافة إلى عدم تطور الممارسات الرقابية بصورة تتواءم مع التطور السريع فى تكنولوجيا المعلومات تعد أهم ثلاث مخاطر تواجه أمن نظم المعلومات ذات الشبكات Network Computer.

وتجدر الأشارة إلى أن دراسة Davis (1996) لم تفرق بين المخاطر Threats وعدم كفاية وفاعلية الأدوات الرقابية المتعلقة بأمن النظم Inadequate or Ineffecient Security Controls. فلقد إعتبر Davis عدم كفاية الرقابة على وسائل حفظ وتحزين المعلومات؛ ضعف الرقابة على المناولة اليدوية لمدخلات ومخرجات الحاسب؛ ضعف الرقابة المادية على الولوج للنظام؛ عدم الفصل بين الوظائف المحاسبية وكذلك عدم الفصل بين وظائف ومهام نظم المعلومات ضمن مخاطر أمن نظم المعلومات. وتجدر الإشارة إلى أن

الباحث قد قام بتنقية وحذف تلك المتغيرات من قائمة المخاطر المقترحة التى سوف يتم إختبارها فى البحث الحالى فيما يتعلق ببيئة الأعمال السعودية.

ولقد قام Ryan and Bordoloi (1997) بعمل دراسة تطبيقية لتقييم مخاطر أمن نظم المعلومات فى النظم المحاسبية الإلكترونية فى المنشأت التى تحولت من نظام أجهزة الكمبيوتر الكبيرة Mainframe إلى نظام خدمة العملاء Client-Server. ولقد قام قام الباحثان بتطوير قائمة شملت خمسة عشر من المخاطر المحتملة التى قد تهدد أمن نظم المعلومات الإلكترونية بناء على الدرسات السابقة والأبحاث التى تمت فى هذا الشأن؛ ولقد قام الباحثان بتوزيع قائمة إستقصاء على مائة وعشرين شركة من الشركات الكبيرة والمتوسطة الحجم فى الولايات المتحدة؛ وتم الحصول على ردود من ٥٢ شركة بما يعادل ٤٧% من عدد الإستبيانات التى تم توزيعها. ولقد طلب من المشاركين فى الإستبيان أن يقوموا بترتيب Rate مدى خطورة وأهمية المخاطر المحتملة لأمن نظم المعلومات المحاسبية الإلكترونية فى بيئة أجهزة الحاسب الألى الكبيرة وكذلك فى نظام خدمة العملاء مستخدمين فى ذلك 10- Point Scale حيث يشير الرقم ١ إلى أن عنصر المخاطر المقترح غير هام بالنسبة للمنشأة بينما يشير الرقم ١٠ إلى أن عنصر المخاطر يعد ذو أهمية كبيرة ومحل إهتمام بالنسبة للمنشأة Very Critical Concern.

وتشير نتائج دراسة Ryan and and Bordoloi (1997) إلى أن هناك فروق جوهرية (عند مستوى معنوية P = 0.05) بين المنشأت التى لديها نظام أجهزة الكمبيوتر الكبيرة وتلك التى تطبق نظام خدمة العملاء فيما يختص بمخاطر أمن نظم المحاسبة الإلكترونية الأتية: التدمير غير المتعمد للبيانات بواسطة موظفى المنشأة؛ الإدخال غير المتعمد لبيانات خاطئة بواسطة موظفى المنشأة؛ التدمير المتعمد للبيانات بواسطة موظفى المنشأة؛ الإدخال المتعمد لبيانات خاطئة بواسطة موظفى المنشأة؛ الخسائر الناجمة على عدم إعداد نسخ إضافية Backups أو الرقابة على ملفات الدخول للنظام Log Files؛ فشل النظام وسقوط الشبكات. وتجدر الإشارة أنه يوجه إلى دراسة(1997) Ryan and Bordoloi نفس الإنتقادات السابقة فيما يختص بعدم الفصل أو التمييز بين المخاطر وضعف أدوات الرقابة المطبقة. ولقد أعترف الباحثان أن قائمة المخاطر المقترحة من قبلهم قد تضمنت بعض العناصر التى لايمكن إعتبارها ضمن مخاطر أمن نظم المعلومات بالمعنى الدقيق. ومن ثم فلقد تم إستبعاد تلك العناصر من القائمة المقترحة للمخاطر فى البحث الحالى؛ حيث تم إختيار ثمانية مخاطر فقط من قائمة Ryan and Bordoloi لإختبارها عملياً فى البيئة السعودية.

ولقد قام Henry (1997) بعمل بحث ميدانى شمل ٢٦١ شركة بولاية فرجينيا بالولايات المتحدة لتحديد وإختبار طبيعة وخصائص أمن نظم المعلومات المحاسبية الإلكترونية المطبقة بتلك الشركات؛ وذلك لدراسة مدى تطابق النظرية مع الممارسات الفعلية. ولقد أشارت نتائج دراسة Henry (1997) إلى أن ٨٠% من الشركات تقوم بعمل نسخ إضافية Backups لبياناتها ونظامها المحاسبى وأن ٧٤,٤% من الشركات التى شاركت فى الدراسة تستخدم كلمات السر لحماية نظامها المحاسبى؛ بيد أن ٤٢,٧% فقط من الشركات نجحت فى توفير الحماية الكافية لنظامها المحاسبى ضد مخاطر فيروسات الكمبيوتر. كما أشارت نتائج الدراسة إلى أن ٤٠% فقط من الشركات توفر الحماية المادية Physical Security اللازمة لنظمها المحاسبية وكذلك فيما يتعلق بتوثيق ومشروعية التغييرات فى نظمها المحاسبية Authorization for Changes to the Systems. وتجدر الإشارة إلى أن ١٥% فقط من الشركات تقوم بتشفير Encryption وتكويد بياناتها. وأن ٤٥% فقط من تلك الشركات لديها نوع من برامج المراجعة على بياناتها وبرامجها المحاسبية الإلكترونية.

وفى دراسة أخرى حديثة قام Abu-Musa (2001) بعمل دراسة تطبيقية لإستكشاف وإختبار المخاطر الهامة التى تهدد أمن نظم المعلومات المحاسبية الإلكترونية فى القطاع المصرفى بجمهورية مصر العربية. حيث قام الباحث بعمل دراسة مسحية شملت جميع البنوك الرئيسية العاملة بجمهورية مصر العربية مستخدماً فى ذلك إستمارة إستقصاء للتعرف على أراء كل من رؤساء أقسام الحاسب الألى ورؤساء أقسام المراجعة الداخلية فيما يختص بالمخاطر الهامة التى تهدد أمن نظم المعلومات المحاسبية الإلكترونية فى البنوك التى يعملون بها. ولقد تم الحصول على ردود تتمثل فى ٧٩ إستمارة إستقصاء من بينها ستة وأربعون إستمارة إستقصاء تم إستيفاء بياناتها من قبل رؤساء أقسام الحاسب الألى؛ وثلاثة وثلاثون تم ملئ بياناتها بواسطة رؤساء أقسام المراجعة الداخلية. ومن ثم كانت نسبة الردود هى ٧٩٠٣% فيما يختص بأقسام الحاسب الألى و ٥٧% فيما يختص بأقسام المراجعة الداخلية.

ولقد قام Abu-Musa (2001) بتطوير قائمة شملت تسعة عشر من المخاطر المحتملة لأمن نظم المعلومات المحاسبية الإلكترونية لإختبار مدى تواجدها وأهميتها فى البيئة المصرية. حيث تم تطوير قائمة المخاطر المقترحة بناءً على الدراسات السابقة التى تمت فى هذا الشأن (على سبيل المثال: Loch et al., 1992; Davis,1996 and1998; FFIEC,1996; and Henry, 1997) كما تضمنت تلك القائمة بعض المخاطر المحتملة

التى تم إختبارها لأول مرة فى تلك الدراسة والتى تتعلق بصفة أساسية بمخاطر أمن مخرجات النظام المحاسبى؛ ولقد تضمنت القائمة المخاطر الأتية:-

١. الإدخال غير المتعمد (غير المقصود) لبيانات غير سليمة بواسطة الموظفين.
٢. الإدخال المتعمد (المقصود) لبيانات غير سليمة بواسطة الموظفين.
٣. التدمير غير المتعمد (غير المقصود) للبيانات بواسطة الموظفين.
٤. التدمير المتعمد (المقصود) للبيانات بواسطة الموظفين.
٥. المرور (الوصول) غير الشرعى (غير المرخص به) للبيانات / النظام بواسطة الموظفين.
٦. المرور غير الشرعى (غيرالمرخص به) للبيانات / النظام بواسطة أشخاص من خارج المنشأة.
٧. إشتراك الموظفين فى كلمة السر.
٨. الكوارث الطبيعية مثل الحرائق، الفيضانات أو إنقطاع مصدر الطاقة.
٩. الكوارث غير الطبيعية والتى هى من صنع الإنسان مثل الحرائق، أو الفياضانات.
١٠. إدخال فيروس الكمبيوتر للنظام المحاسبى.
١١. طمس أو تدمير بنود معينة من المخرجات.
١٢. خلق مخرجات زائفة / غير صحيحة.
١٣. سرقة البيانات / المعلومات.
١٤. عمل نسخ غير مصرح (مرخص) بها من المخرجات.
١٥. الكشف (الإظهار) غير المرخص به للبيانات عن طريق عرضها على شاشات العرضComputer Screens أو طبعها على الورق.
١٦. طبع و توزيع المعلومات بواسطة أشخاص غير مصرح لهم بذلك.
١٧. المطبوعات والمعلومات الموزعة يتم توجيهها خطأ إلى أشخاص غير مخول لهم / ليس لهم الحق فى إستلام نسخة منها.
١٨. المستندات الحساسة يتم تسليمها إلى أشخاص لا تتوافر فيهم الناحية الأمنية وذلك بغرض تمزيقها.
١٩. مقاطعة تحويل البيانات من أماكن بعيدة.

وتشير نتائج الدراسة إلى أن الإدخال غير المتعمد لبيانات غيرصحيحة من قبل موظفى البنوك، التدمير غير المتعمد للبيانات من قبل موظفى البنوك، إدخال فيروس الكمبيوتر إلى النظام، الكوارث الطبيعية والكوارث التى هى من صنع الإنسان، إشتراك بعض

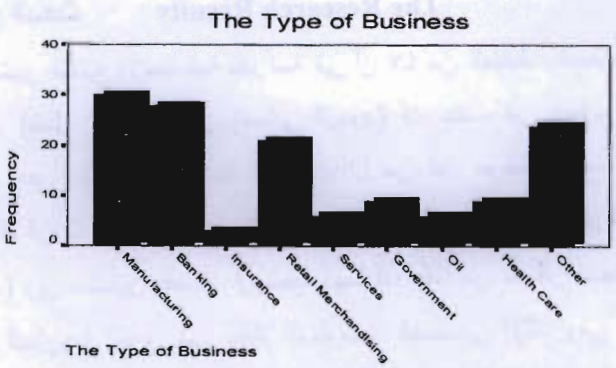
الموظفين فى إستخدام نفس كلمة السر، وكذلك توجية البيانات والمعلومات إلى أشخاص غير مخول لهم بإستلامها تعد من أهم المخاطر التى تواجه أمن نظم المعلومات المحاسبية الإلكترونية فى صناعة البنوك المصرية. وتجدر الإشارة إلى أنه فى جميع الحالات فإن رؤساء أقسام المراجعة الداخلية قد أعطوا تقديرات أعلى لمعدلات حدوث تلك المخاطر فى البنوك التى يعملون بها مقارنة بتقديرات رؤساء أقسام الحاسب الألى. وتشير نتائج الدراسة أنه لا توجد إختلافات جوهرية بين أنواع البنوك المختلفة إلا فيما يختص بالمرور غير المرخص به للبيانات / النظام من قبل أطراف خارجية (قراصنة المعلومات).

٦. منهج البحث Research Methodology

يتمثل منهج هذا البحث فى إجراء دراسة تطبيقية للتعرف على أهم المخاطر التى تهدد أمن نظم المعلومات المحاسبية الإلكترونية؛ وإختبار الفروق الجوهرية بين المنشأت المختلفة فيما يختص بمدى إدراكها لخطورة ومعدلات تكرار حدوث تلك المخاطر فى بيئة الأعمال بالمملكة العربية السعودية؛ مستخدماً فى ذلك إستمارة إستقصاء (ملحق ١) أعدت خصيصاً لتحقيق هذا الغرض. ولقد تم توزيع عدد ٤٠٠ إستمارة إستقصاء على عينة عشوائية من المنشأت السعودية. ولقد شملت عينة البحث عدداً من المنشأت الصناعية؛ البنوك؛ الصحة؛ الوحدات الحكومية؛ تجارة الجملة؛ تجارة التجزئة؛ الخدمات العامة؛ البترول والغاز؛ الدعاية والإعلان؛ شركات التأمين وغيرها من المنشأت الأخرى؛ وذلك فى سبعة مدن سعودية شملت: الرياض؛ جدة؛ الظهران؛ الدمام؛ الثقبة؛ الخبر؛ والجبيل. وبعد المتابعة تم تجميع عدد ٢٠٨ إستمارة إستقصاء؛ ومن ثم فإن معدل الردود المبدئى يمثل ٥٢%. وتجدر الإشارة أنه تم إستبعاد عدد ٣٨ إستمارة إستقصاء من التحليل وهى تمثل المنشأت التى لديها نظم محاسبية يدوية ولا يوجد بها نظم محاسبية إلكترونية. كما تم أيضا إستبعاد ٣٤ قائمة إستقصاء لعدم إكتمال البيانات بها؛ حيث رفضت تلك المنشأت إستكمال بعض بيانات الإستقصاء بحجة أنها بيانات حساسة وسرية للغاية. ومن ثم فإنه بعد إستبعاد قوائم الإستقصاء غير المكتملة Incompleteوغير الصالحة للتحليل Invalid فقد تم الحصول على عدد ١٣٨ قائمة إستقصاء صالحة للتحليل والتى تمثل ٣٤% من إجمالى عدد إستمارات الإستقصاء التى تم توزيعها على مفردات العينة. ويعد هذا المعدل للردود عالياً بالمقارنة بالأبحاث المماثلة التى تمت فى هذا المجال. ولقد تم تحليل البيانات التى تم تجميعها بإستخدام برنامج حزمة البرامج الجاهزة للعلوم الإجتماعية SPSS؛ الطبعة الثانية عشرة (SPSS, Version 12) .

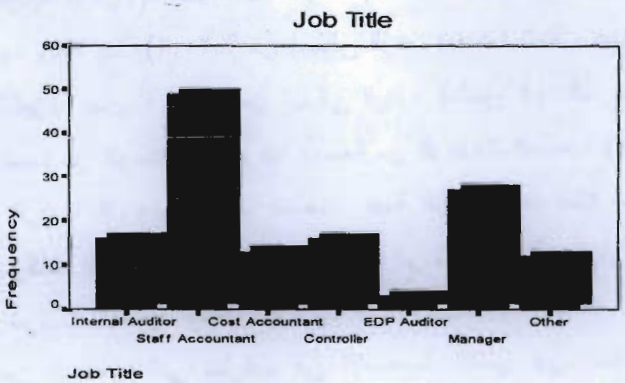
ولقد قام الباحث بإجراء التحليل الوصفى Descriptive Analysis (مثل معدل التكررات والنسب) للبيانات التى تم تجميعها للتعرف على الخصائص الأساسية لعينة البحث ومتغيرات الدراسة. كما تم إجراء بعض الإختبارات اللامعلمية Non-Parametric Tests (مثل إختبار كارسوكال - ولاس Krsukal-Wallis وكذلك إختبار تحليل التباين ANOVA) لإختبار فروض البحث والتعرف على الفروق الجوهرية بين المنشأت المختلفة فيما يتعلق بالمخاطر الهامة التى تهدد أمن نظم المعلومات المحاسبية الإلكترونية بها.

ولقد روعى فى إختيار عينة البحث أن تكون عينة غيرمتحيزة Unbiased وأن تكون ممثلة Represntative للمجتمع الذى سحبت منه. حيث تم إختيار عينة عشوائية من المنشأت السعودية من مختلف أنواع النشاطات والقطاعات من سبع مدن مختلفة فى المملكة العربية السعودية (شكل٢). فلقد شملت عينة البحث ٣٠ منشأة صناعية تمثل ٢٢,١% من إجمالى الردود و٢٨ بنكاً (٢٠,٦% من إجمالى الردود) ؛ كما شمات عينة البحث ٢١ منشأة من تجارة التجزئة تمثل ١٥,٤% من إجمالى الردود (ملحق ٢). كما إشتملت عينة البحث أيضا على تسعة من الوحدات الحكومية وتسعة من الوحدات الصحية والمستشفيات (٦,٦% من إجمالى الردود لكل منهما). كما تضمنت عينة الدراسة عدد ستة منشأت خدمية وعدد مماثل من شركات البترول والغاز. هذا بالأضافة إلى ثلاث منشأت تمثل ٢,٢% من إجمالى الردود من شركات التأمين. وتجدر الإشارة إلى أن هناك ٢٤ منشأة أخرى (١٧,٦% من الإجمالى) من المنشأت التى شاركت فى الإستقصاء تنتمى إلى الفنادق؛ شركات تأجير السيارات؛ شركات الدعاية والإعلان؛ مكاتب المحاسبة؛ شركات الإنشاءات والمقاولات وغيرها من المنشأت الأخرى (شكل ٢).



(شكل ٢: عينة البحث)

وتجدر الإشارة إلى أن ٤٩ من المشاركين فى الإستقصاء (٣٦% من إجمالى الردود) كانوا يعملون محاسبون؛ وأن ٢٧ من المشاركين فى الإستقصاء (٢٠% من إجمالى الردود) كانوا ينتمون إلى فئة المديرين. بينما ١٦ من المشاركين (١٢% من إجمالى الردود) كانوا يعملون كمراجعين داخليين ونسبة مماثلة يعملون كرؤساء أقسام للمحاسبة (ملحق ٢). هذا بالإضافة إلى أن ١٣ مشاركاً كانوا يعملون كمحاسبى تكاليف وثلاثة آخرين كمراجعين لتشغيل البيانات الإلكترونية. ومن ثم فإنه يمكن القول بأن عينة البحث تعد عينة ممثلة للهيكل الوظيفى فى المنشآت السعودية (شكل ٣). وسوف يتم عرض ومناقشة نتائج الدراسة فى الأقسام التالية.



(شكل ٣: عينة البحث)

٧. نتائج البحث The Research Results

تشير النتائج الإحصائية للدراسة إلى أن ٤٧ من المنشآت السعودية التى شاركت فى الإستقصاء (تمثل ٣٤,٦% من إجمالى الردود) قد عانت من وجود خسائر مالية نتيجة التصرفات غير الأمينة Dishonest actions من قبل موظفى المنشأت. وأن ١٣ منشأة (٩,٦%) قد قررت أنها عانت من خسائر نتيجة لأحداث مماثلة من أطراف خارجية (قراصنة المعلومات) وأن منشأتين فقط قد أوضحتا أنهما قد عانتا من خسائر نتيجة كل من التصرفات الداخلية والخارجية لخرق أمن نظام المعلومات المحاسبى الإلكترونى بها فى خلال السنة الماضية (ملحق ٢). ولقد تم ملاحظة أن ٥٠% تقريباً من المنشأت قد عانت من خسائر مالية نتيجة لحدوث بعض التعديات على أمن نظم المعلومات المحاسبية الإلكترونية بها؛ وأن تلك الخسائر قد تراوحت بين ١٠,٠٠٠ ريال سعودى فى بعض المنشأت و ٢٠٠ مليون ريال

سعودى فى المنشأت الأخرى. وتجدر الإشارة أن الإفصاح عن الخسائر يعد من البيانات الحساسة فى هذا البحث؛ حيث أن كثيراً من المنشأت قد ترددت فى الإفصاح عن وجود تلك الخسائر أو الرقم الحقيقى لها خشية أن تؤثر تلك البيانات على سمعتها وأسعار أسهمها فى السوق. ويعرض الباحث فى الجزء المتبقى من البحث لأهم نتائج الدراسة المتعلقة بمدى إدارك المنشأت السعودية لأهمية وخطورة تهديدات أمن نظم المعلومات المحاسبية الإلكترونية؛ وكذلك نتائج إختبارات جوهرية الفروق بين آراء تلك المنشأت فيما يتعلق بمعدل تكرار حدوث تلك المخاطر.

الإدخال غير المتعمد لبيانات غير سليمة بواسطة موظفى المنشأة

Accidental Entry of Bad Data by Employees

لقد تم سؤال المشاركين فى الإستقصاء أن يعبروا عن أرائهم فيما يتعلق بمعدل تكرار حدوث عملية الإدخال غير المتعمد لبيانات غير صحيحة بواسطة موظفى المنشأة إلى النظام المحاسبى؛ وذلك بإختيار رقم واحد من بين خمس إختيارات متاحة لهم (أقل من مرة واحدة سنوياً؛ من مرة سنوياً إلى شهرياً؛ من مرة شهرياً إلى أسبوعياً؛ من مرة أسبوعياً إلى يومياً؛ يومياً أو بصفة متكررة). وتشير نتائج الدراسة إلى أن أكثر من ثلث المشاركين فى الإستقصاء (٣٤,٦%) يعتقدون أن إدخال بيانات غير سليمة بواسطة موظفى المنشأة بطريقة غير متعمدة يحدث ما بين مرة سنوياً إلى شهرياً؛ وأن ٢٠% من المشاركين فى الإستقصاء يعتقدون أن ذلك ربما يحدث ما بين مرة شهرياً إلى أسبوعياً. بينما ١٨,٤% من المشاركين فى الإستقصاء يعتقدون أن الإدخال غير المتعمد لبيانات غير سليمة بواسطة الموظفين تحدث نادراً جداً فى منشأتهم؛ وأن معدل تكرار ذلك لا يتجاوز مرة واحدة سنويا. بينما ١,٥% فقط من إجمالى المشاركين فى الإستقصاء يؤكدون أن ذلك لم يحدث إطلاقاً فى منشأتهم (ملحق ٢).

وعلى الجانب الأخر فإن ٢٢,١% من المشاركين يقررون أن الإدخال غير المتعمد لبيانات غير سليمة من قبل موظفي المنشأة يحدث ما بين مرة أسبوعياً إلى يومياً؛ بينما ٧,٣% من المشاركين فى الإستبيان يعتقدون أن ذلك يحدث يومياً أو بصورة متكررة فى منشأتهم. ولقد أوضحت نتائج إختبارات كارسوكال – ولاس (ملحق ٣) وتحليل التباين (ملحق ٤) عدم وجود إختلافات جوهرية بين المنشأت السعودية فيما يتعلق بمعدل تكرار حدوث إدخال بيانات غير سليمة بصورة غير متعمدة من قبل موظفى المنشأت عند مستوى معنوية P. = 0.05

الإدخال المتعمد لبيانات غيرسليمة بواسطة موظفى المنشأة

Intentional Entry of Bad Data by Employees

فى محاولة للتعرف آراء المشاركين فى الإستقصاء فيما يختص بمدى تكرار حدوث إدخال بيانات غير سليمة بطريقة متعمدة من قبل موظفى المنشأة إلى النظام المحاسبى؛ فقد تم سؤالهم عن معدل تكرار حدوث ذلك الخطر فى منشأتهم. ولقد اشارت نتائج الدراسة أن ما يقرب من نصف المنشأت المشاركة فى الإستقصاء قد أكدت أن ذلك نادراً جداً ما يحدث فى المنشأت التى يعملون بها حيث أن معدل تكرار حدوث ذلك أقل من مرة واحدة فى العام. ويؤكد ٢٣% من المنشأت الأخرى أن ذلك نادر الحدوث أيضاً فى منشأتهم حيث أن ذلك يحدث ما بين مرة سنوياً إلى شهريا. بينما يعتقد ١٠% من المشاركين فى الإستقصاء أن ذلك لم يحدث مطلقاً فى منشأتهم؛ وأعربوا عن رأيهم فى أن ذلك يعد جريمة ونوع من الغش وأن من يرتكبه يجب معاقبته إدارياً وقانونياً.

وعلى الجانب الآخر فإن ستة منشأت (٤,٤%) يعتقدون أن إدخال بيانات غير سليمة بصورة متعمدة من قبل موظفى المنشأة غالباً ما يحدث فى منشأتهم حيث أن ذلك قد يحدث بين مرة إسبوعياً إلى يومياً (ملحق ٢). بينما أربعة منشأت أخرى ٢,٩% يعتقدون أن ذلك يمكن أن يحدث يومياً أو بصورة متكررة فى المنشأت التى يعملون بها؛ وأنهم يعزون إلى ضعف أنظمة الرقابة الداخلية بتلك المنشأت. وتشير نتائج إختبار كارسوكال – ولاس (ملحق ٣) وتحليل التباين (ملحق ٤) إلى أنه لا توجد إختلافات جوهرية بين المنشأت المختلفة (عند مستوى معنوية $P = 0.05$) فيما يتعلق بإدخال بيانات غير سليمة بصورة متعمدة من قبل الموظفين فى المنشأت السعودية.

التدمير غير المتعمد للبيانات بواسطة موظفى المنشأة

Accidental Destruction of Data by Employees

فى محاولة لفهم والتعرف على أراء المنشأت السعودية فيما يختص بخطر التدمير غير المتعمد للبيانات نتيجة الخطأ أوالسهو من قبل موظفى تلك المنشأت؛ فقد تم سؤال الأشخاص المشاركين فى الإستقصاء عن معدل تكرار حدوث ذلك فى المنشأت التى يعملون بها. ولقد أوضحت نتائج الدراسة أن ٣٧,٥% من المنشأت يعتقدون أن التدمير غير المتعمد للبيانات من قبل موظفى المنشأت يعد ظاهرة نادرة الحدوث؛ حيث قد يحدث ذلك أقل من مرة سنويا. وأن ٢٩,٤% من المنشأت يعتقدون أن ذلك يحدث ما بين مرة واحدة سنوياً إلى شهرياً. بينما تؤكد ٩,٦% من المنشأت أن ذلك لم يحدث مطلقاً فى منشأتهم (ملحق ٢). بينما

يعتقد ١٨,٤% من المنشأت أن ذلك يمكن أن يحدث ما بين مرة شهرياً إلى إسبوعياً. ومن ناحية أخرى؛ فإن ٤,٤% من المنشأت التى شاركت فى الإستقصاء يعتقدون أن التدمير غير المتعمد للبيانات من قبل موظفى المنشأة يعد ظاهرة متكررة الحدوث فى منشأتهم؛ حيث يتكرر ذلك ما بين مرة إسبوعياً إلى يومياً. وأن منشأة واحدة تؤكد أن ذلك قد يحدث يومياً أو بصورة متكررة بها. ولقد أظهرت نتائج إختبار كارسوكال – ولاس (ملحق ٣) وإختبار تحليل التباين (ملحق٤) عدم وجود فروق جوهرية بين المنشأت السعودية فيما يختص بإدراكها لمعدل تكرار حدوث التدمير غير المتعمد للبيانات من قبل موظفى المنشأت عند مستوى معنوية P = 0.05.

التدمير المتعمد للبيانات من قبل موظفى المنشأة

Intentional Destruction of Data by Employees

لقد طلب من المنشأت المشاركة فى الإستقصاء أن تعبر عن رأيها فيا يتعلق بمعدل تكرار حدوث التدمير المتعمد للبيانات من قبل موظفى المنشأة. ولقد أوضحت نتائج الدراسة أن ٦٠% من المنشأت تعتقد أن ذلك يحدث نادراً جداً فى منشأتهم؛ نظراً لأنه يحدث أقل من مرة واحدة سنوياً (ملحق ٢). وأن ١٢,٥% من المنشأت يعتقدون أن ذلك من الممكن أن يحدث ما بين مرة واحدة سنوياً إلى شهرياً. وعلى الجانب الأخر فإن الأقلية من المنشأت ٨,٨% قد أشاروا أن ذلك قد يحدث بصورة شبه متكررة؛ فقد يحدث ما بين مرة واحدة شهرياً إلى إسبوعياً. وأن منشأة واحدة قد عبرت عن رأيها أن ذلك ربما يحدث يومياً أو بطريقة متكررة من خلال بعض التلاعبات والإختلاسات الصغيرة من قبل الموظفين. ولقد لوحظ أن معدل تكرار الإتلاف والتدمير المتعمد للبيانات من قبل موظفى المنشأة يعد من الأحداث النادرة الحدوث فى المنشأت السعودية.

وتشير نتائج إختبار كارسوكال – ولاس (ملحق ٣) وكذلك نتائج تحليل التباين (ملحق ٤) إلى وجود دليل قوى على عدم وجود فروق جوهرية بين المنشأت السعودية فيما يختص بمعدل تكرار حدوث تدمير متعمد للبيانات من قبل موظفى المنشأة عند مستوى معنوية P = 0.05.

المرور غير المصرح به للبيانات / النظام بواسطة موظفى المنشأة

Unauthorized Access to the Data / Systems by Employees

فى محاولة للتعرف على معدل حدوث المرور غير المصرح به للبيانات / النظام من قبل موظفى المنشأت فلقد تم سؤال المشاركين فى الإستقصاء عند مدى تكرار حدوث ذلك فى منشاتهم وذلك بالإختيار من بين خمس إختيارات متاحة. ولقد أوضحت نتيجة الدراسة أن أكثر من ثلثى المنشأت المشاركة فى الإستقصاء (٦٧,٦%) يعتقدون أن المرور غير المصرح به إلى بيانات النظام المحاسبى من قبل موظفى المنشأت يعد من الأحداث النادرة جداً؛ حيث أن ذلك قد يحدث أقل من مرة واحدة فى السنة نظراً لوجود نظم رقابة داخلية جيدة. بينما ١١% من المشاركين فى الإستقصاء يعتقدون أن ذلك لم يحدث إطلاقاً فى منشأتهم (ملحق ٢).

وتجدر الإشارة إلى أن عدداً قليلاً من المنشأت المشاركة فى الإستقصاء (١٠,٣%) يعتقدون أن المرور غير المصرح به إلى البيانات / النظام من قبل موظفى المنشأة يمكن أن يحدث ما بين مرة واحدة سنوياً إلى شهرياً. وأن ٩,٦% من تلك المنشأت يعتقدون أن ذلك قد يحدث من مرة شهرياً إلى أسبوعياً؛ بيد أن ١,٥% فقط يعتقدون أن ذلك يحدث مابين مرة أسبوعياً إلى يومياً. ومن ثم فإن ذلك يعطى مؤشراً على إنخفاض معدل المرور غير المصرح به من قبل موظفى المنشأت للبيانات / النظام فى المنشأت السعودية.

ولقد أشارت نتائج إختبارات كارسوكال - ولاس (ملحق ٣) وتحليل التباين (ملحق ٤) على وجود دليل قوى على أنه لا توجد فروق جوهرية بين المنشأت السعودية فيما يتعلق بالمرور غير المصرح به للبيانات / النظام من قبل موظفى المنشأت عند مستوى معنوية P = 0.05 .

المرور غير المصرح به للبيانات / النظام من قبل أطراف خارجية

Unauthorized Access to the Data / Systems by Outsiders

لإختبار معدل تكرار حدوث المرو غير المصرح به إلى البيانات / النظام فى المنشأت السعودية من قبل أطراف خارجية (قراصنة المعلومات) فلقد طلب من المشاركين فى الإستقصاء إعطاء ارائهم فيما يختص بمعدل حدوث ذلك الخطر فى منشأتهم خلال السنوات السابقة. ولقد أشارت نتيجة الدراسة أن غالبية المنشأت (٦٩,١%) يعتقدون أن ذلك نادراً جداً ما يحدث فى منشأتهم (أقل من مرة واحدة فى العام). وأن ١٢,٥% من المنشأت يؤكدون أن ذلك لم يحدث مطلقاً فى منشأتهم (ملحق ٢). بينما يرى ١٠,٣% من المنشأت أن ذلك قد

يحدث من مرة واحدة سنوياً إلى شهرياً. ولعل أحد الأسباب المحتملة وراء تلك النتيجة هى إنخفاض الخدمات الإلكترونية وإرتباط تلك المنشأت مع شبكة الإنترنت والإنخفاض النسبى لعدد المنشأت التى تمارس التجارة الإلكترونية E-Business والتحويل الإلكترونى للأموال Electronic Fund Transfer وغيرها من الخدمات والأعمال الإلكترونية.

وعلى الجانب الآخر فإن ٢,٩% من المنشأت التى شاركت فى الإستقصاء يعتقدون أن المرور غير المرخص به للبيانات / النظام من قبل قراصنة المعلومات والأطراف الخارجية قد يحدث ما بين مرة واحدة شهرياً إلى إسبوعياً؛ وأن ٤ منشأت يعتقدون أن ذلك قد يحدث مابين مرة أسبوعياً إلى يومياً؛ بينما أشارت ٣ منشأت ٢,٢% أن ذلك يحدث بصفة متكررة بها. ولقد أوضحت نتيجة إختبارات كارسوكال - ولاس (ملحق ٣) وإختبار تحليل التباين (ملحق ٤) أنه لاتوجد إختلافات جوهرية بين المنشأت السعودية فيما يختص بالمرور غير المرخص به إلى البيانات / النظام فى تلك المنشأت من قبل أطراف خارجية (قراصنة المعلومات) عند مستوى معنوية P = 0.05 .

- ***إشتراك الموظفين فى إستخدام نفس كلمات السر***

Employees Sharing of Passwords

تشير نتائج الدراسة إلى أن مايقرب من ١٠% من المشاركين فى الإستقصاء يعتقدون أنه كل موظف له كلمة السر الخاصة به؛ وأن الموظفين يحافظون على سريتها ولا يشتركون فى إستخدام نفس كلمات السر على الإطلاق. بينما ٤٤,١% من المشاركين فى الإستقصاء يؤكدون أن إشتراك بعض الموظفين فى إستخدام نفس كلمة السر قد يحدث لتنفيذ بعض المهام؛ بيد أن ذلك يكون فى حدود ضيقة جدا وتحت ضوابط رقابية مشددة (أقل من مرة واحدة سنوياً). وعلى الجانب الأخر فإن ٩% من المشاركين فى الإستقصاء يقررون أن إشتراك الموظفين فى إستخدام كلمة السر يحدث مابين مرة شهرياً إلى إسبوعياً؛ وأن ٨,٨% منهم يعتقدون أن ذلك يحدث بصفة متكررة حيث قد يحدث يومياً فى منشأتهم (ملحق ٢). وتجدر الإشارة أن ٢٧,٢% من المنشأت التى شاركت فى الإستقصاء يعتقدون أن إشتراك الموظفين فى إستخدام كلمة السر يحدث أكثر من مرة واحدة سنوياً إلى شهرياً؛ مما يعطى مؤشراً على إرتفاع معدل حدوث ذلك الخطر فى المنشأت السعودية. ومرة أخرى تؤكد نتائج إختبارات كل من كارسوكال - ولاس (ملحق ٣) وتحليل التباين (ملحق ٤) على عدم وجود إختلافات جوهرية بين المنشأت السعودية فيما يختص بإشتراك الموظفين فى إستخدام نفس "كلمات السر" عند مستوي معنوية P = 0.05.

الكوارث الطبيعية *Natural Disasters*

تؤدى الكوارث الطبيعة مثل الحرائق والزلازل والبراكين والأعاصير والفيضانات إلى خسائر كبيرة بالنسبة لكثير من المنشأت؛ والتى قد تنتج عنها إنقطاع مصدر الطاقة والتدمير الكلى أو الجزئى لأصول المنشأت والتى من بينها أجهزة الحاسب الألى ووسائل حفظ وتخزين المعلومات مثل الشرائط والأقراص الممغنطة؛ بالإضافة إلى سقوط الشبكات والخسائر المالية الناتجة عن عدم إمكانية إستخدام النظام؛ وكذلك تكاليف إصلاح وإستعادة النظام مرة أخرى.

وتشير نتائج الدراسة إلى أن الغالبية العظمى من المنشأت السعودية (٧١,٢%) يؤكدون أن الكوارث الطبيعية تعد ظاهرة نادرة الحدوث فى المملكة. وأن ١٠,٣% يؤكدون أن ذلك لم يحدث مطلقاً فى منشأتهم. بينما ١٢,٥% من المنشأت يعتقدون أن ذلك قد يحدث ما بين مرة واحدة سنوياً إلى شهرياً؛ وأن أقل من ٦% من المنشأت يعتقدون أن الكوارث الطبيعية (مثل إنقطاع مصدر الطاقة) قد يحدث ما بين مرة شهرياً إلى إسبوعياً أو أكثر (ملحق ٢). وتشير نتائج الدراسة إلى عدم وجود فروق جوهرية بين المنشأت السعودية فيما يختص بإدراكهم لمعدل تكرار حدوث الكوارث الطبيعية طبقا لنتائج إختبارات كل من كارسوكال – ولاس وتحليل التباين عند مستوى معنوية $P = 0.05$.

الكوارث غير الطبيعية "من صنع الإنسان"

Disasastre of Human Origin

تتمثل الكوارث غير الطبيعية "من صنع الإنسان" فى الحرائق المفتعلة والإنفجارات وإنقطاع مصدر الطاقة التى قد تسبب فيها الإنسان بصورة متعمدة لإخفاء بعض الإختلاسات والتلاعبات؛ أو بصورة غير متعمدة نتيجة الأخطاء أو السهو أو عدم كفاية الخبرة إلى غيرها من الأسباب. فلقد لوحظ إرتفاع معدلات حدوث مثل تلك الحرائق وغيرها من الكوارث المفتعلة خاصة فى نهاية السنوات المالية وقبل فترة الجرد السنوى للمخازن؛ والتى قد يعزوها البعض إلى وجود ماس كهربائى؛ بيد أن الحقيقة أنها فى معظم الأحيان تكون جرائم وكوارث متعمدة من قبل أشخاص معينين لإخفاء العجز والإختلاسات والتلاعبات فى المخازن أو السجلات والدفاتر المحاسبية.

وتشير نتائج الدراسة إلى أن ٧٠,٣% من مفردات العينة يعتقدون أن معدل حدوث تلك الكوارث يعد نادراً جداً فى منشأتهم (أقل من مرة واحدة سنوياً). كما أن ١٠% أخرون يؤكدون أن ذلك لم يحدث على الإطلاق فى منشأتهم؛ بينما يعتقد ١٢,٣% أن ذلك قد يحدث ما

بين مرة سنوياً إلى شهرياً؛ ومن ثم لايمكن تصنيف ذلك الخطر ضمن المخاطر الهامة التى تهدد أمن نظم المعلومات المحاسبية فى منشأتهم (ملحق ٢). وعلى الجانب الأخر فإن ٥,٩% فقط من المشاركين فى الإستقصاء يعتقدون أن ذلك يمكن أن يحدث ما بين مرة شهرياً إلى إسبوعياً أو أكثر من ذلك. ومن ثم فإن نتائج الدراسة تؤكد إنخفاض معدل تكرار حدوث تلك الكوارث غير الطبيعية (من صنع الإنسان) فى المنشأت السعودية. وتشير نتائج الدراسة إلى عدم وجود إختلافات جوهرية بين المنشأت السعودية فيما يختص بإدراكها وتقييمها لمعدل تكرار حدوث ذلك الخطر طبقاً لنتائج إختبارات كارسوكال – ولاس وتحليل التباين وبمستوى معنوية P = 0.05.

إدخال فيروس الكمبيوتر للنظم المحاسبية

Introduction (Entry) of Computer Viruses to the Systems

تشير نتائج الدراسة إلى أن ما يزيد على نصف عدد المشاركين فى الإستقصاء (٥٢,٢%) يعتقدون أن إدخال فيروس الكمبيوتر إلى النظم المحاسبية الإلكترونية يعد من المخاطر النادرة الحدوث جداً فى المنشأت السعودية نظراً لأنه قد يحدث أقل من مرة سنوياً. وأن ٩,٥% من المنشأت تؤكد عدم حدوث ذلك مطلقاً خلال السنة الماضية؛ كما أن ٢٢,١% من المنشأت تؤكد أن ذلك قد يحدث مابين مرة واحدة سنوياً إلى شهرياً (ملحق ٢). بينما تعتقد ٨,٨% من المنشأت أن ذلك قد يحدث ما بين مرة شهرياً إلى إسبوعياً. وتجدر الإشارة إلى أن سبعة منشأت فقط تمثل (٥,١%) من إجمالى الردود يعتقدون أن إدخال فيروسات الكمبيوتر إلى النظم المحاسبية قد يحدث ما بين إسبوعياً إلى يومياً؛ بينما تؤكد ثلاث منشأت أخرى (٢,٢%) أن ذلك قد يحدث يومياً أو بصفة متكررة. وتجدر الإشارة إلى أن نتائج إختبارات كارسوكال – ولاس وكذلك تحليل التباين لم تظهرا فروقاً جوهريةً بين المنشأت المختلفة فيما يتعلق بمعدل تكرار إدخال فيروسات الكمبيوتر إلى النظم المحاسبية فى المنشأت السعودية بدرجة معنوية P = 0.05.

طمس أو تدمير المخرجات

Suppression or Destruction of Output

تشير نتائج الدراسة أن معظم المشاركين فى الدراسة ٥٩,٦% يرون أن خطر طمس بعض بيانات مخرجات النظام المحاسبى أو تدميرها نادراً ما يحدث ولا يتكرر بإستمرار فى منشأتهم؛ إذ أن معدل حدوثه أقل من مرة واحدة سنويا؛ بينما يؤكد ١١% أخرين على أن ذلك

لم يحدث مطلقاً فى منشأتهم. وأن ١٤% أخرون يعتقدون أن ذلك يعد الأمور نادرة الحدوث فى منشأتهم؛ حيث يتراوح ذلك مابين مرة واحدة سنوياً إلى شهرياً (ملحق ٢).

وعلى الجانب الإخر فإن ٢١ مشارك (١٥,٥%) يعتقدون أن طمس أو تدمير مخرجات النظام بصفة متعمدة يحدث ما بين مرة إسبوعياً إلى شهرياً؛ ومن ثم فإنه طبقاً لتلك النتائج فإن معدل تكرار حدوث ذلك الخطر يعد منخفض نسبياً فى المنشأت السعودية. وتجدر الإشارة إلى أن نتائج إختبارات كارسوكال – ولاس (ملحق ٣) وتحليل التباين (ملحق ٤) لم تفصح عن وجود إختلافات جوهرية بين المنشأت السعودية فيما يتعلق بمعدل تكرار حدوث تدمير أو طمس مخرجات الحاسب الالى عند مستوى معنوية P = 0.05.

خلق مخرجات زائفة / غير صحيحة

Creation of Fictitous / Incorrect Output

تشير نتائج الدراسة إلى أن ما يزيد عن نصف المشاركين فى الإستقصاء ٥٥,١% يعتقدون أن خلق مخرجات زائفة / غير صحيحة نادراً ما يحدث فى منشأتهم (أقل من مرة فى العام). بينما نجد أن ٩,٦% أخرون يؤكدون أن ذلك لم يحدث مطلقاً فى منشأتهم. وتجدر الإشارة إلى أن ٢١,٣% يرون أن خلق مخرجات غير صحيحة / غير زائفة يعد نوعاً من أنواع الغش والتلاعب وأن ذلك قد يحدث ما بين مرة سنوياً إلى شهرياً فى منشأتهم.

ومن ناحية أخرى فإن ١٥% من المنشأت التى شاركت فى الإستقصاء يعتقدون أن خلق مخرجات زائفة / غير صحيحة يمكن أن يحدث أكثر من مرة سنوياً إلى شهرياً. ومن ثم فطبقاً للنتائج المبينة أعلاه فإن الغالبية العظمى من المشاركين فى الإستقصاء يعتقدون أن خلق مخرجات زائفة / غير صحيحة يعد من المخاطر ذات المعدلات المنخفضة الحدوث فى المنشأت السعودية. هذا ولم تفصح نتائج إختبارات كارسوكال – ولاس (ملحق ٣) وتحليل التباين (ملحق ٤) عن وَجود أى فروق جوهرية بين أنواع المنشأت المختلفة فيما يتعلق بمعدل تكرارحدوث هذا الخطر فى المنشأت السعودية عند مستوى معنوية P = 0.05.

سرقة البيانات / المعلومات *Theft of Data / Information*

تشير نتائج الدراسة أن الغالبية العظمى من مفردات العينة (٧٠% تقريباً) يعتقدون أن سرقة البيانات / المعلومات يعد من المخاطر نادرة الحدوث فى منشأتهم؛ وأن معدل تكرار ذلك هو أقل من مرة واحدة فى السنة؛ بينما نجد ٩,٦% أخرون يؤكدون أن ذلك يعد من

الأمور المستحيلة وأنه لم يحدث مطلقاً فى منشأتهم نظراً لوجود نظام رقابة صارم على مخرجات النظام المحاسبى الإلكترونى.

وتجدر الإشارة إلى أن ١٣,٢% من مفردات العينة يعتقدون أن ذلك يمكن أن يحدث ما بين مرة سنوياً إلى شهرياً (ملحق ٢). وأن نسبة قليلة من المنشأت المشاركة فى الإستقصاء (أقل من ٩%) يعتقدون أن سرقة البيانات / المعلومات يحدث أكثر من مرة سنوياً إلى شهرياً. وطبقاً للنتائج الموضحة أعلاه فإن خطر سرقة بيانات / معلومات يمكن إعتباره من المخاطر ذات معدل التكرار المنخفض فى المنشأت السعودية. وتجدر الإشارة إلى أنه لا توجد إختلافات جوهرية بين أنواع المنشأت المختلفة فيما يختص بمعدل تكرار حدوث ذلك الخطر فى المنشأت السعودية طبقاً لنتائج إختبار كارسوكال – ولاس وكذلك تحليل التباين عند مستوى معنوية P = 0.05.

عمل نسخ غير مصرح (مرخص) بها من المخرجات

Unauthorized Copying of Output

لقد أوضحت نتائج الدراسة أن أكثر من ثلثى المشاركين فى الإستقصاء (٦٦,٩%) يعتقدون أن عمل نسخ غير مصرح بها من المخرجات يعد من الإحداث النادرة جداً (أقل من مرة سنوياً)؛ بينما يرى ١١% من المنشأت أن ذلك لم يحدث مطلقاً نظراً لوجود نظام رقابة داخلية جيد على مخرجات الحاسب الألى فى منشأتهم. كما تشير نتائج الدراسة إلى أن ١٣,٢% من المنشأت يعتقدون أن ذلك يحدث ما بين مرة سنوياً إلى شهرياً.

ومن ناحية اخرى فإن ١٢ منشأة فقط تمثل أقل من ٩% من إجمالى الردود يعتقدون أن عمل نسخ غير مصرح (مرخص بها) من البيانات والمعلومات يحدث أكثر من مرة سنوياً إلى شهرياً (ملحق ٢). ومن ثم فإن عمل نسخ غير مصرح بها من البيانات والمعلومات يعد من المخاطر ذات معدلات الحدوث المنخفضة فى بيئة الأعمال السعودية. وبناءً على نتائج إختبار كارسوكال – ولاس وإختبار تحليل التباين يبدو أنه لايوجد إختلاف جوهرى بين المنشأت السعودية فيما يتعلق بذلك الخطر عند مستوى معنوية P = 0.05.

الكشف (الإظهار) غير المصرح به للبيانات / المعلومات

Unauthorized Document Visibility

تشير نتائج الدراسة إلى أن ٦٠% تقريباً من المنشأت المشاركة فى الإستقصاء قد عبروا عن رأيهم بأن الكشف (الإظهار) غير المصرح به للبيانات / المعلومات عن طريق

عرضها على شاشات العرض Computer Screen أو طبعها على الورق نادراً ما قد يحدث فى منشأتهم (أقل من مرة واحدة سنويا)؛ بينما يؤكد البعض الأخر (٦,٦% من إجمالى الردود) أن ذلك يعد من الأمور الصعبة؛ ولم يحدث قط فى منشأتهم نظراً لوجود نظام رقابة جيد على مخرجات الحاسب الألى. بينما يعتقد ١٦,٢% من المشاركين فى الإستقصاء أن حدوث مثل ذلك يعد من الأحداث النادرة فى منشأتهم حيث قد يحدث ما بين مرة سنوياً إلى شهرياً؛ وأن ٨,٨% أخرون يعتقدون أن ذلك قد يحدث ما بين مرة شهرياً إلى إسبوعياً (ملحق ٢).

وعلى الجانب الأخر فإن ٦% من المنشأت يرون أن الكشف أو الإظهار غير المصرح به للبيانات أو المعلومات لأشخاص غير مرخص لهم بذلك قد يحدث ما بين مرة أسبوعياً إلى يومياً؛ وأن ٣,٧% فقط من المنشأت المشاركة فى الإستقصاء يعتقدون أن ذلك يمكن أن يحدث يومياً أو بصفة متكررة (ملحق ٢). ومن ثم يمكن القول بأن الكشف عن بيانات / المعلومات غير المرخص به يعد من المخاطر غير عالية الحدوث فى بيئة الأعمال السعودية. ولم تظهر نتائج تحليل كارسوكال – ولاس (ملحق ٣) وتحليل التباين (ملحق ٤) فروقاً جوهريةً بين المنشأت السعودية فيما يختص بمدى إدراكها لمعدل تكرار حدوث عنصر **المخاطر المشار إليه عاليه بدرجة معنوية P = 0.05 .**

طبع و توزيع البيانات / المعلومات من قبل أشخاص غير مصرح لهم بذلك
Unauthorized Printing and Distribution of Data / Information

فيما يتعلق بخطر طبع وتوزيع البيانات / المعلومات من قبل أشخاص غير مصرح لهم بذلك؛ تشير نتائج الدراسة إلى أن غالبية المشاركين فى الإستقصاء (٦٥,٣%) قد أشاروا إلى أن ذلك يعد من الأمور نادرة الحدوث جداً (أقل من مرة سنوياً) فى منشأتهم؛ بينما يقرر ١٠,٣% من المشاركين أن ذلك لم يحدث البته فى منشأتهم. كما أن ما يقرب من ١٧% من المشاركين فى الإستقصاء يعتقدون أن ذلك قد يحدث ما بين مرة واحدة سنوياً إلى شهرياً.

ومن ناحية أخرى فإن ما يقرب من ٦% من المنشأت المشاركة فى الإستقصاء يعتقدون أن طبع وتوزيع بيانات / معلومات من قبل أشخاص غير مرخص لهم بذلك قد يحدث ما بين مرة شهرياً إلى أسبوعياً؛ وأن ٣% فقط من المشاركين فى الإستقصاء قد قرروا أن ذلك قد يحدث ما بين مرة أسبوعياً إلى يومياً؛ بينما ٣,٧% أخرون يعتقدون أن ذلك قد يحدث يومياً أو بصفة متكررة فى منشأتهم (ملحق ٢). ومن ثم يمكن القول أن طبع وتوزيع بيانات / معلومات من قبل أشخاص غير مرخص لهم بذلك يعد من عناصر المخاطر غير

متكررة الحدوث فى المنشأت السعودية. وطبقاً لنتائج إختبار كارسوكال – ولاس (ملحق ٣) و تحليل التباين (ملحق ٤) فإنه لا توجد فروق جوهرية بين المنشأت فيما يختص بمعدل تكرار حدوث ذلك الخطر فى المنشأت السعودية عند مستوى معنوية P = 0.05.

توجيه المطبوعات و المعلومات إلى أشخاص غير مخول لهم بإستلام نسخة منها

Directing Prints and Distributed Information to People not entitled to receive.

تشير نتائج الدراسه إلى أن ٥٥,١% من المشاركين فى الإستقصاء يرون أن توجيه المطبوعات والبيانات عن طريق الخطأ إلى أشخاص غير مخول لهم بإستلامها يعد من الأحداث النادرة جداً فى منشأتهم؛ حيث قد يحدث أقل من مرة واحدة سنوياً. بينما ٨,١% من المنشأت المشاركة فى الإستقصاء يقررون أن ذلك لم يحدث مطلقاً فى منشأتهم؛ وأن ٢٢,١% يرون أن ذلك قد يحدث ما بين مرة سنوياً إلى شهرياً (ملحق ٢). وعلى الجانب الأخر فإن ٨,١% من المشاركين فى الإستقصاء قد أشاروا إلى أن ذلك يحدث مابين مرة شهرياً إلى أسبوعياً؛ وأن منشأة واحدة تعتقد ان ذلك يحدث من مرة أسبوعياً إلى يومياً. وتجدر الإشارة إلى أن ثمانية من المشاركين فى الإستقصاء (٥,٦%) يعتقدون أن التوجيه الخاطىء للبيانات والمعلومات إلى أشخاص غير مخول لهم بإستلام تلك المعلومات يعد من الأحداث المتكررة فى المنشأة؛ حيث قد يحدث ذلك يومياً فى منشأتهم. وتشير نتائج إختبارات كل من كارسوكال – ولاس (ملحق ٣) وتحليل التباين (ملحق ٤) إلى عدم وجود فروق جوهرية بين المنشأت فيما يختص بمعدل تكرار عنصر المخاطرة المشار إليه عاليه فى المنشأت السعودية عند مستوى معنوية P = 0.05 .

تسليم المستندات الحساسة إلى أشخاص لا تتوافر فيهم الناحية الأمنية لتمزيقها أو التخلص منها

Sensitive Documents are handled to Non-Security Cleared Personnel for Shredding

تشير نتائج الدراسة إلى أن ٦١% من المشاركين فى الإستقصاء يرون أن تسليم مستندات حساسة إلى أشخاص لا تتوافر فيهم النواحى الأمنية لتمزيقها أو التخلص منها يعد نادراً جداً؛ حيث أن ذلك قد يحدث أقل من مرة واحدة فى السنة. بينما يؤكد ٨,٨% من المشاركين فى الإستقصاء أن ذلك لم يحدث مطلقاً فى المنشأت التى يعملون بها؛ وأن ١٩% آخرين يعتقدون أن ذلك قد يحدث من مرة سنوياً إلى شهرياً؛ بما يمكن إعتباره من الأحداث

النادرة وغير المتكررة. بينما نجد أن نسبة ضئيلة من المشاركين فى الإستقصاء (١١% من إجمالى الردود) يعتقدون أن ذلك يمكن أن يحدث أكثر من مرة واحدة سنوياً إلى شهرياً (ملحق ٢). ومن ثم فإن النتائج الموضحة عالية تعطى مؤشراً قوياً على إنخفاض معدل تكرار تسليم مستندات حساسة إلى أشخاص لا تتوافر فيهم النواحى الأمنية بهدف تمزيقها أو التخلص منها. وتجدر الإشارة إلى أن إختبارات كارسوكال – ولاس (ملحق ٣) وتحليل التباين (ملحق ٤) لم تظهر أى إختلافات جوهرية بين المنشأت السعودية فى هذا الشأن عند مستوى معنوية P= 0.05.

مقاطعة تحويل البيانات من أماكن متفرقة

Interception of Data Transmision

تشير نتائج الدراسة إلى أن ٦٠% من المشاركين فى الدراسة يعتقدون أن مقاطعة تحويل البيانات من أماكن متفرقة يعد من الأمور النادرة الحدوث جداً وغير المتكررة فى منشأتهم؛ حيث قد يحدث ذلك أقل من مرة واحدة سنوياً. وأن ١١% من المشاركين فى الإستقصاء يرون ذلك لم يحدث مطلقاً فى منشأتهم. بينما يعتقد ١٧,٦% من المشاركين أن ذلك يحدث ما **بين مرة سنوياً إلى شهرياً مما يمكن إعتباره حدثاً غير متكرر الحدوث فى** المنشأت التى يعملون بها. وتجدر الإشارة أن إثنتين فقط من المنشأت ترى أن ذلك يمكن أن يحدث ما بين مرة شهرياً إلى إسبوعياً. وأن ٤,٤% فقط من المشاركين فى الدراسة يعتقدون أن مقاطعة تحويل وإرسال البيانات من أماكن متفرقة يعد من المخاطر الهامة حيث قد يحدث ذلك يومياً أو بصفة متكررة فى منشأتهم (ملحق ٢). ومن ثم يمكن القول أن مقاطعة إرسال تحويل البيانات من أماكن متفرقة لا يعد من المخاطر عالية الحدوث فى المنشأت السعودية. ومرة أخرى لم تظهر نتائج إختبارات كارسوكال – ولاس (ملحق ٣) وتحليل التباين (ملحق ٤) أى فروق جوهرية بَين المنشأت السعودية فيما يتعلق بخطر مقاطعة تحويل البيانات من قبل قراصنة المعلومات عند مستوى معنوية P= 0.05.

٧. مناقشة نتائج الدراسة Discussion of the Results

لقد أظهرت نتائج الدراسة أن نسبة عالية من المنشأت التى شاركت فى الإستقصاء قد عانت من وجود خسائر مالية كبيرة نتيجة بعض التعديات على أمن نظم المعلومات المحاسبية بها سواءً من قبل أطراف داخلية (موظفى المنشأة) أو أطراف خارجية (قراصنة المعلومات)؛ وأن تلك الخسائر قد تراوحت ما بين ١٠٠,٠٠٠ ريال سعودى و٢٠٠ مليون

ريال سعودى. وتجدر الإشارة إلى أن الإفصاح والتقرير عن الخسائر المالية الناجمة عن التعديات على أمن نظم المعلومات المحاسبية يعد من الأمور الحساسة فى هذا الإستقصاء؛ حيث أن كثيراً من المنشأت قد تتردد فى الإفصاح عن رقم خسائرها الفعلية خشية الأثار السلبية التى قد تنتج عن ذلك والتى قد تنعكس على سمعة المنشأة وأسعار أسهمها فى السوق. كما أوضحت الدراسة أن كثيراً من تلك التلاعبات والإختلاسات والتعديات على أمن نظم المعلومات المحاسبية قد تم إكتشافها عن طريق الصدفة نتيجة لعدم كفاية وفعالية الأدوات والضوابط الرقابية المطبقة فى تلك المنشأت. وأن معظم الإختلاسات والتلاعبات التى تم إكتشافها قد تم تسويتها داخلياً ولم يتم الإفصاح أو التقرير عنها للجمهور حفاظاً على سمعة الشركة وتحسين صورتها فى السوق. وتتفق النتائج التى تم الحصول عليها الدراسة الحالية مع نتائج الدراسات السابقة التى تمت فى هذا المجال (أنظر على سبيل المثال: Abu-Musa, 2001; KPMG, 2000; Corbitt, 1996; Mau and Catlin,1993; EDPACS, 1992; Feeney,1993; Meall,1992; Rockwell,1990; Doost, 1990;).

أما فيما يختص بمدى إدراك المنشأت السعودية للمخاطر الهامة التى تهدد نظم المعلومات المحاسبية ومعدلات تكرار حدوث تلك المخاطر بها؛ فلقد أوضحت نتيجة الدراسة إلى أن الإدخال غير المتعمد لبيانات غير سليمة والتدمير غير المتعمد للبيانات من قبل موظفى المنشأة يعد من المخاطر الهامة والمتكررة الحدوث فى المنشأت السعودية. ولعل أحد التفسيرات المحتملة لإرتفاع معدل تكرار حدوث تلك المخاطر فى المنشأت السعودية قد يرجع إلى كثرة الأخطاء الناتجة عن عدم توافر الخبرة اللازمة والتدريب الكافى والخلفية العلمية والمهارات المطلوبة لتنفيذ تلك الأعمال من قبل موظفى تلك المنشأت. وتتفق نتائج الدراسة مع النتائج التى تم الحصول عليها فى بعض الدراسات السابقة ومنها على سبيل المثال: Ryan .& Bordoloi 1997, Davis 1996 , Loch et al. 1992, Abu-Musa, 2001

كما أظهرت نتيجة الدراسة إلى أن الإدخال المتعمد لبيانات غير سليمة من قبل موظفى المنشأة بهدف الإختلاس والتلاعب فى الأرقام المحاسبية يعد من الأمور المتكررة الحدوث فى بيئة الإعمال السعودية والتى قد تهدد أمن نظم المعلومات المحاسبية بها. وقد يعزو البعض تلك الظاهرة إلى ضعف نظم الرقابة الداخلية فى تلك المنشأت وعدم فعاليتها؛ وإشتراك بعض الموظفين فى إستخدام نفس كلمات السر؛ وعدم الفصل بين المهام والوظائف المحاسبية وكذلك المتعلقة بنظم المعلومات؛ وعدم وجود سياسات وبرامج محددة ومكتوبة لأمن نظم المعلومات المحاسبية بتلك المنشأت؛ وعدم إلزام الموظفين بأخذ أجازتهم الدورية؛ وعدم الإهتمام الكافى بفحص التاريخ الوظيفى والمهنى للموظفين الجدد؛ وعدم الإهتمام

بدراسة المشاكل الإقتصادية والإجتماعية والنفسية لموظفي تلك المنشأت. وتتفق نتائج البحث الحالى مع نتائج دراسة Ryan & Bordoloi 1997 بينما تختلف تلك النتيجة مع النتائج التى تم الحصول عليها فى بعض الدراسات الأخرى مثل: Abu-Musa 2001; Davis 1996; Loch et.al 1992 .

ولقد أوضحت نتيجة الدراسة الحالية أن إدخال فيروسات الكمبيوتر إلى النظام المحاسبى يعد من المخاطر الهامة التى تهدد أمن نظم المعلومات المحاسبية فى المنشأت السعودية؛ والذى قد يرجعه البعض إلى عدم توفر الحماية الكافية ضد مخاطر فيروسات الكمبيوتر فى تلك المنشأت؛ نظراً لعدم تحميل برنامج ضد الفيروسات على أجهزة الكمبيوتر أو عدم تحديثها؛ أو عدم الوعى الكافى لدى الموظفيين بضرورة فحص أى البرامج أو الأقراص الممغنطة الجديدة عند إدخالها إلى أجهزة الكمبيوتر وذلك بتمريرها على برامج الفيروساتِAnti-Virues؛ أو إستخدام برامج غير أصلية وتتفق تلك النتيجة مع نتائج دراسة Davis 1996 ودراسة Henry 1997.

كما أظهرت نتائج الدراسة إلى أن طمس أو تدمير مخرجات الحاسب الآلى؛ والكشف غير المرخص به للبيانات والمعلومات عن طريق عرضها على شاشات العرض أو طبعها على الأوراق، وكذلك توجيه المطبوعات والمعلومات إلى أشخاص غير مخول لهم بإستلام تلك المعلومات تعد من المخاطر الهامة التى تهدد أمن نظم المعلومات المحاسبية فى المنشأت السعودية؛ والذى قد يرجع إلى ضعف وعدم كفاءة النظم الرقابية المطبقة على مخرجات الحاسب الآلى؛ وعدم وجود سياسات واضحة ومكتوبة فيما يختص بأمن نظم المعلومات المحاسبية فى تلك المنشأت؛ وكذلك عدم التوصيف الدقيق للهيكل الوظيفى والإدارى الذى يحدد المسئوليات والصلاحيات لكل شخص داخل الهيكل التنظيمى بتلك المنشأت؛ بالإضافة إلى عدم الفصل الدقيق بين الوظائف. وتجدر الإشارة إلى أن تلك المخاطر المتعلقة بأمن مخرجات الحاسب الآلى تعد من المخاطر التى يتم إختيارها لأول مرة فى بيئة الأعمال السعودية.

ولقد أشارت نتائج الدراسة أن الكوارث الطبيعية لا تعد من المخاطر الهامة التى تهدد أمن النظم المحاسبية فى المنشأت السعودية نظراً لأن المملكة العربية السعودية ليست من المناطق النشطة فيما يختص بالزلازل والبراكين. كما أنها ليست من المناطق التى تتعرض للفياضات والأعاصير وغيرها من الكوارث الطبيعية. كما إظهرت نتائج الدراسة أن التدمير المتعمد للبيانات من قبل موظفى المنشأة يعد من الإحداث النادرة وغير متكررة الحدوث فى المنشأت السعودية نظراً لأن التدمير المتعمد للبيانات بهدف التلاعب فى السجلات والدفاتر

المحاسبية والغش فى القوائم المالية يحتاج عادةً الى مهارات عالية وخبرات متخصصة فى مجال الحاسب الألى وتكنولوجيا المعلومات حتى يتم هذا التدمير بطريقة لاتسمح بإكتشافه من خلال الأدوات والضوابط الرقابية العادية؛ ومن ثم محاولة إتخاذ كافة الإحتياطات والتدابير الازمة لإخفاء الأثار المحتملة الناتجة عن تدمير تلك البيانات. ومن ثم فإن تقرير المنشأت السعودية عن إنخفاض معدل حدوث التدمير المتعمد للبيانات بها قد يرجع الى ضعف أنظمة الرقابة الداخلية المطبقة فى تللك المنشأت وعدم قدرتها على إكتشاف مثل هذه التلاعبات والإختلاسات؛ أو عدم توافر المهارات والخبرات الازمة لدى موظفى تلك المنشأت لإحداث التدمير المتعمد للبيانات بطريقة يصعب إكتشافها؛ أو لعدم رغبة تلك المنشأت فى التقرير عن حالات التدمير المتعمد لبيانتها فى حالة حدوث ذلك إما لعدم جوهرية الأثار المالية الناجمة عنها؛ أو لخوف تلك المنشأت من التأثير السلبى للتقرير عن مثل هذه الأحداث على سمعة المنشأة لدى مستخدمى القوائم المالية.

وتجدر الإشارة إلى أن إنخفاض معدل تكرار حدوث المرور غير المصرح به للبيانات / النظام من قبل موظفى المنشأت فى الدراسة الحالية قد يرجع بصفه أساسيه إلى عدم إشتراك الموظفين فى إستخدام نفس كلمات السر للولوج إلى النظام لتنفيذ الأعمال والمهام المنوطة اليهم؛ نظراً لأن كل موظف لديه كلمة سر خاصة به لتنفيذ أعمال ومهام محدده على برنامج المحاسبة؛ والتى قد لا تسمح له بالمرور لتنفيذ غيرها من المهام الأخرى. ومن ثم فإن إشتراك الموظفين فى إستخدام نفس كلمات السر لم يظهر ايضاً ضمن قائمة المخاطر الهامة التى تهدد أمن نظم المعلومات المحاسبية فى بيئة الأعمال السعودية.

أما فيما يختص بمخاطر أمن نظم المعلومات المتعلقة بمخرجات الحاسب الآلى فى المنشأت السعودية؛ فلقد أشارت الدراسة إلى أن خلق مخرجات زائفة أو غير صحيحة؛ سرقة البيانات والمعلومات؛ عمل نسخ غير مصرح بها من المخرجات؛ وكذلك تسليم المستندات الهامة والحساسة إلى أشخاص لا تتوافر فيهم الناحية الأمنية بهدف تمزيقها أو التخلص منها يعد من الأحداث نادرة الحدوث نسبياً فى المنشأت السعودية. وقد يرجع ذلك إما لكفاءة وفعالية الضوابط الرقابية المطبقة على مخرجات الحاسب الآلى فى تلك المنشأت؛ أو لعدم إدراك تلك المنشأت لمدى خطورة ذلك على أمن نظم المعلومات المحاسبة بها؛ خاصة فى حالة عدم قدرة أنظمة الرقابة الداخلية المطبقة فى تلك المنشأت على إكتشاف تلك المخاطر فى حالة حدوثها.

كما أشارت نتيجة الدراسة إلى أن مقاطعة تحويل البيانات من أماكن متفرقة قد لا يعد من المخاطر الهامة التى تهدد أمن نظم المعلومات فى المنشأت السعودية نظراً لإنخفاض نسبة المنشأت التى تمارس الخدمات والأعمال الإلكترونية مثل التجارة الإلكترونية والتحويل

الإلكترونى للأموال؛ كما أن عدداً كبيراً من المنشأت التى شاركت فى الإستقصاء ليست مرتبطة مع شبكة الإنترنت. وتجدر الإشارة إلى أن نتائج الإختبارات الإحصائية اللامعملية مثل إختبار كارسوكال – ولاس وتحليل التباين لم تظهر أى إختلافات جوهرية بين المنشأت السعودية التى شاركت فى الإستقصاء فيما يختص بمدى إدراكها لأهمية المخاطر المشار إليها أعلاه والتى تهدد أمن نظم المعلومات المحاسبية الإلكترونية ودرجة تقييمها لمعدلات تكرار حدوث تلك المخاطر فى بيئة الأعمال السعودية.

٨. خلاصة وتوصيات البحث

Conclusion and Recommendations for Future Research

لقد إستهدف هذا البحث التعرف على المخاطر الهامة التى تهدد أمن نظم المعلومات المحاسبية الإلكترونية فى المنشأت السعودية؛ وكذلك إختبار الفروق الجوهرية بين المنشأت المختلفة فيما يختص بتقييمها لمعدلات تكرار حدوث تلك المخاطر ومدى إدراكها لدرجة خطورة تلك التهديدات على أمن نظم معلوماتها المحاسبية الإلكترونية. ولقد تم تطوير قائمة بأهم المخاطر المحتملة لأمن نظم المعلومات المحاسبية الإلكترونية بالإعتماد على الأبحاث والدراسات السابقة ومنها على سبيل المثال: Davis, 1992. Henry Loch et al., 1996 and Abu-musa 2001 1997 والأبحاث الأخرى المتاحة فى هذا المجال. كما تضمنت القائمة المقترحة عدداً من المخاطر المحتملة التى تم إختبارها عملياً للمرة الأولى فى بيئة الأعمال السعودية. ولقد تم أجراء دراسة تطبيقية على عينة ممثلة وغير متحيزة شملت ١٢٦ منشأة تنتمى إلى قطاعات وأنشطة إقتصادية مختلفة؛ والتى تم إختيارها عشوائيا من سبعة مدن مختلفة بالمملكة العربية السعودية.

ولقد أشارت نتائج الدراسة إلى أن أهم المخاطر التى تهدد أمن نظم المعلومات المحاسبية الإلكترونية فى المنشأت السعودية هى: الإدخال المتعمد وغير المتعمد لبيانات غير صحيحة بواسطة موظفي المنشأت؛ إدخال فيروسات الكمبيوتر إلى النظام المحاسبى؛ مشاركة الموظفين فى إستخدام نفس كلمات السر؛ طمس أو تدمير مخرجات الحاسب الألى؛ الكشف (الإظهار) غير المرخص به للبيانات والمعلومات عن طريق عرضها على شاشات العرض أو طبعها على الأوراق؛ وكذلك توجية المطبوعات والمعلومات إلى أشخاص غير مخول لهم بإستلام تلك المعلومات أو الإطلاع عليها. ولم تظهر نتائج إختبارات كارسوكال – ولاس وتحليل التباين أى إختلافات جوهرية بين المنشأت المختلفة فيما يختص بتقديرها لأهمية المخاطر التى تهدد أمن نظم المعلومات المحاسبية الإلكترونية فى بيئة الأعمال السعودية.

وتجدر الإشارة أنه يمكن تطوير هذا البحث وإعتباره نقطة إنطلاق لمزيد من الأبحاث المستقبلية للتعرف على أراء المراجعين الخارجيين مقارنةً بأراء المراجعين الداخليين فيما يختص بالمخاطر الهامة التى تهدد أمن نظم المعلومات المحاسبية الإلكترونية. وكذلك إختبار الفروق الجوهرية بين أراء المحاسبين والمراجعين الداخليين ومراجعى نظم المعلومات بأقسام الحاسب الألى فيما يتعلق بتقييمهم لمعدلات حدوث ومدى خطورة تلك التهديدات وأثارها السلبية المحتملة على النظم المحاسبية الإلكترونية. ويمكن إجراء دراسات مماثلة على بعض دول مجلس التعاون الخليجى للتعرف على أرائهم ودرجة إدراكهم لمدى خطورة تلك التهديدات على نظم المعلومات المحاسبية الإلكترونية؛ والتعرف على خططهم المستقبلية لمواجهة تلك التحديات؛ كما يمكن أيضا عمل دراسات مقارنة لإختبار الفروق الجوهرية بين معدلات حدوث تلك المخاطر فى تلك الدول ومقارنتها بمثيلاتها بالدول المتقدمة.

REFERENCES

د. سمير رياض هلال (١٩٩٢) "محددات إعادة إستخدام البرامج فى نظم المعلومات المحاسبية: حالة عملية فى الوحدات الحكومية بدولة الإمارات العربية"، ***مجلة التجارة والتمويل***، المجلة العلمية لكلية التجارة – جامعة طنطا، العدد الملحق الأول للعدد الثانى، ص ص٤٩-٧٤.

Abu-Musa, Ahmad A. (2001), Evaluating The Security of Computerized Accounting Information Systems: An Empirical Study on Egyptian Banking Industry", ***PhD. Thesis***, Aberdeen University, UK.

Abu-Musa, Ahmad A. (2003), "The Perceived Threats to the Security of Computerized Accounting Information Systems", ***The Journal of American Academy of Business, Cambridge, USA***, Vol. 3, No.1, September, pp. 9- 20.

Bandyopadhyay, Kakoli, Peter P. Mykytyn and Kathleen Mykytyn (1999), "A Framework for Integrated Risk Management in Information Technology", ***Management Decision,*** (Vol. 37, Iss. 5).

Collier, Paul, Rob Dixon and Claire Marston (1991), "The Role of Internal Auditor in the Prevention and Detection of Computer Fraud", ***Public Money and Management,*** (Winter), pp. 53 - 61.

Corbitt, Terry (1996), "Stop, Thief", ***Accountancy Age***, (Feb), p. 20

Dougan, Jim (1994), "Internal Control Checklist for Hospitality Computer Systems", ***Bottom Line,*** (Vol. 9, Iss. 5), pp. 8 - 11.

Davis, Charles E. (1996), "Perceived Security Threats to Today's Accounting Information Systems: A Survey of CISAs", ***IS Audit & Control Journal,*** (Vol. 3), pp. 38 - 41.

Davis, Charles E. (1997), "An Assessment of Accounting Information Security", ***The CPA Journal,*** New York (Vol. 67, Iss. 3), pp. 28 - 34.

Doost, Roger K. (1990), "Accounting Irregularities And Computer Fraud", ***National Public Accountant,*** (Vol. 35 Iss. 5), pp. 36 - 39.

EDPACS (1992), "A major International Organisation Ignores Computer Security", ***EDPACS: The EDP Audit, Control, & Security Newsletter,*** (Vol. 20, Iss. 4), pp. 18-19.

FFIEC (1996) ***IS Examination Handbook, Chapter, 14, Security- Physical And Data.***

Feeney, Kevin (1993), "How To Deal With Computer Fraud", ***Connecticut CPA Quarterly***, (March), pp. 10-11.

Grundy, Emma, Collier, Paul and Spaul, Barry (1994), "Auditing Personnel: A Human Resource Approach to Information System Control", ***Managerial Auditing Journal,*** (Vol. 9), pp. 10-16.

Haugen Susan and J. Roger Selin (1999), "Identifying and Controlling Computer Crime and Employee Fraud", ***Industrial Management and Data Systems,*** (Vol. 99, Iss. 8).

Henry, Laurie (1997), "A Study of the Nature and Security of Accounting Information Systems: The Case of Hampton Roads, Virginia", ***The Mid-Atlantic Journal of Business,*** (Vol. 33, Iss. 63), pp. 171 - 189.

Hood, Keith L. and Jie-Win Yang (1998), "Impact of Banking Information Systems Security on Banking in China: The Case of Large State-Owned Banks in Shenzhen Economic Special Zone - An Introduction", ***Journal of Global Information Management,*** (Vol. 6, No. 3), pp. 5 - 15.

Huntington, Ian and David Davies (1994), ***Fraud Watch,*** The Institute of Chartered Accountants in England and Wales, London.

International Federation of Accountants (IFAC), Information Technology Committee, (1998), ***International Information Technology***

Guidelines: Managing Security of Information, The (January), New York.

Jenkins, Brian, Peter Cooke and Peter, Quest (1992), ***An Audit Approach to Computers,*** Institute of Chartered Accountants In England And Wales, London.

KPMG (2000), ***Information Security Survey 2000, Executive Summary***, April, KPMG, London

Leinicke, Linda Marie, W. Max Rexroad and Jon D. Ward (1990), "Computer Fraud Auditing: It Works", ***Internal Auditor,*** (Vol. 47 Iss. 4), pp. 26 - 33.

Levi, Philip (1993), "PC security for accountants - What's Hot and What's New", ***Accounting Technology,*** (Feb. / Mar.), pp. 26-30.

Loch, Karen D., Houston H. Carr and Merrill E. Warkentin (1992), "Threats to Information Systems: Today's Reality, Yesterday's Understanding", ***MIS Quarterly,*** (June), pp. 173 - 186.

National Institute of Standards and Technology (1995), Technology Administration, U.S. Department of Commerce, ***An Introduction to Computer Security: The NIST Handbook***, Special Publication 800-12. October 1995

Mau, Sonya and Jack, Catlin (1993), "Systems Security In 90's", ***Interpreter,*** (January), pp. 8-9

Meall, Lesley (1992), "Computer Crime: Foiling the Fraudsters", ***Accountancy,*** (November), pp. 56-57.

OECD (Organisation for Economic Co-operation and Development) (1992), ***Guidelines for the Security of Information Systems***, The Council of the OECD, 26 November.

Parker, Donn B. (1976), ***Crime By Computer,*** Charles Scribner's sons, New York.

Price, R. Leon, John S. Cotner and Warren L. Dickson (1989), "Computer Fraud In Commercial Banks: Management's Perception of Risk", ***Journal of Systems Management,*** October, (Vol. 40, No. 10), pp. 28 - 34.

Rainer, Kelly Rex, Charles A. Snyder and Houston H. Carr (1991) "Risk Analysis For Information Technology", ***Management Information Systems,*** (Vol. 8, Iss. 1), pp. 129 - 147.

Rockwell, Robin (1990), "The Advent of Computer Related Crimes", ***Secured Lender***, (Jul /Aug), pp. 40 – 42.

Roufaiel, Nazik S. (1990), "Computer Related Crimes: An Educational And Professional Challenge", ***Managerial Auditing Journal,*** (Vol. 5, Iss. 4), pp. 18 - 25.

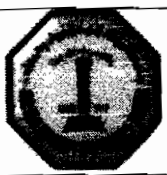
Ryan, S. D. and B. Bordoloi (1997), "Evaluating Security Threats in Mainframe and Client / Server Environments", ***Information & Management,*** (Vol. 32, Iss. 3), pp. 137 - 142.

Schweitzer, James A. (1987), ***Computers, Business, and Security,*** Butterworth Publishers, London.

Weingartner, A. and Maggie Burton (1991), "PC Security - Don't Be Caught Out", ***Computer Security Guide,*** pp. 33 - 35.

(ملحق: ١)
(قائمة الإستقصاء)

جامعة الملك فهد للبترول والمعادن
كلية الإدارة الصناعية
قسم المحاسبة و نظم المعلومات



أهمية مخاطر نظم المعلومات المحاسبية الإلكترونية:
دراسة تطبيقية على المنشأت السعودية

السيد الفاضل / السيدة الفاضلة

يهدف هذا الإستبيان إلى التعرف عل أرائكم فيما يختص بالمخاطر الهامة التى تواجه أمن نظم المعلومات المحاسبية الإلكترونية فى المنشأت السعودية؛ لذلك نرجو منكم التكرم بملىء بيانات الإستبيان المرفق. ونود أن نؤكد على أن البيانات التى سوف يتم تجميعها فى هذا الإستبيان سوف تكون سرية ولن تستخدم إلا فى أغراض البحث العلمى. ونظراً لأن إجاباتكم سوف تكون على قدر عالٍ من الأهمية بالنسبة لهذا البحث، لذا نرجو التكرم بمراعاة الدقة فى إستيفاء بيانات هذا الإستبيان. ونشكر لكم مشاركتكم فى هذا الإستبيان.

الباحث
د/ أحمد عبد السلام أبو موسى
أستاذ مساعد بقسم المحاسبة ونظم المعلومات
كلية الإدارة الصناعية
جامعة الملك فهد للبترول والمعادن

Dr. Ahmad A. Abu-Musa
Department of Accounting and MIS
College of Industrial Management
King Fahd University of Petroleum and Minerals
P O Box 1755, Dhahran, 31261, Saudi Arabia
Phone: 00966-3-860-1420
Fax: 00966-3-860-3489
mailto:abumusa@kfupm.edu.sa

معلومات عامة

من فضلك ضع علامة "√" على المربع الذى تختاره لكل سؤال على حدة

١- هل تعمل حالياً فى:-

- ☐ منشأة صناعية
- ☐ تجارة الجملة
- ☐ بنك
- ☐ تجارة التجزئة
- ☐ شركة تأمين
- ☐ وحدة حكومية
- ☐ منشأة صحية
- ☐ آخرى. من فضلك حددها.....

٢- كم عدد المحاسبين الذين يعملون حالياً بالمنشأة؟

- ☐ ١ - ٥
- ☐ ٦ - ١٠
- ☐ ١١ - ١٥
- ☐ ١٦ - ٢٠
- ☐ أكثر من٢٠

٣- كم عدد المتخصصين فى نظم المعلومات الذين يعملون حالياً بالمنشأة؟

- ☐ ١ - ٥
- ☐ ٦ - ١٠
- ☐ ١١ - ١٥
- ☐ ١٦ - ٢٠
- ☐ أكثر من٢٠

٤- ماهو المسمى الوظيفى لعملك الحالى بالمنشأة؟

- ☐ محاسب مالى
- ☐ مراجع لنظم المعلومات الإلكترونية
- ☐ مراجع داخلى
- ☐ رئيس قسم
- ☐ محاسب تكاليف
- ☐ مير عام
- ☐ مراقب عام

٥- كم عدد سنوات الخبرة التى قضيتها فى مزاولة عملك الحالى؟.....

٦- النظام المحاسبى فى المنشأة التى تعمل فيها:

- ☐ يدوى لا يستخدم الحاسبات الألية
- ☐ خليط من العمل اليدوى، والتشغيل الإلكترونى بالكمبيوتر
- ☐ يعتمد بدرجة كبيرة على الكمبيوتر (شديد الألية)

تقييم تهديدات أمن نظام المعلومات المحاسبى

من فضلك ضع علامة "√" على المربع الذى تختاره فى عمود التكرارات المناسب لكل تهديد على حدة.

تهديدات أمن نظام المعلومات المحاسبية الإلكترونية	أقل من مرة واحدة سنوياً	من مرة سنوياً إلى شهرياً	من مرة شهرياً إلى سنوياً	من مرة إسبوعياً إلى يومياً	يومياً أو بصفة متكررة
١. الإدخال غير المتعمد (غير المقصود) لبيانات غير سليمة بواسطة الموظفين.					
٢. الإدخال المتعمد (المقصود) لبيانات غير سليمة بواسطة الموظفين.					
٣. التدمير غير المتعمد للبيانات بواسطة الموظفين.					
٤. التدمير المتعمد (المقصود) للبيانات بواسطة الموظفين.					
٥. المرور (الوصول) غير الشرعى (غير المرخص به) للبيانات / النظام بواسطة الموظفين.					
٦. المرور غير الشرعى (غيرالمرخص به) للبيانات / النظام بواسطة أشخاص من خارج المنشأة.					
٧. إشتراك الموظفين فى كلمة السر .					
٨. الكوارث الطبيعية مثل الحرائق، الفيضانات او إنقطاع مصدر الطاقة.					
٩. الكوارث غير الطبيعية والتى هى من صنع الإنسان مثل الحرائق، أو الفياضانات.					
١٠. إدخال فيروس الكمبيوتر للنظام المحاسبى.					
١١. طمس أو تدمير بنود معينة من المخرجات.					
١٢. خلق مخرجات زائفة / غير صحيحة.					
١٣. سرقة البيانات / المعلومات.					
١٤. عمل نسخ غير مصرح (مرخص) بها من المخرجات.					
١٥. الكشف غير المرخص به للبيانات عن طريق عرضها على شاشات العرض أو طبعها على الورق.					
١٦. طبع و توزيع المعلومات بواسطة أشخاص غير مصرح لهم بذلك.					
١٧. المطبوعات والمعلومات الموزعة يتم توجيهها خطأ إلى أشخاص غير مخول لهم / ليس لهم الحق فى إستلامها نسخة منها.					
١٨. تسليم المستندات الحساسة إلى أشخاص لاتتوافر فيهم الناحية الأمنية بغرض تمزيقها أو التخلص منها.					
١٩. مقاطعة تحويل البيانات من أماكن بعيدة.					

(ملحق: ٢)
(التحليل الوصفى للنسب والتكرارت)

The Type of Business

The Type of Business	Frequency	Percent	Valid Percent	Cumulative Percent
Manufacturing	30	22.1	22.1	22.1
Banking	28	20.6	20.6	42.6
Insurance	3	2.2	2.2	44.9
Retail Merchandising	21	15.4	15.4	60.3
Services	6	4.4	4.4	64.7
Government	9	6.6	6.6	71.3
Oil	6	4.4	4.4	75.7
Health Care	9	6.6	6.6	82.4
Other	24	17.6	17.6	100.0
Total	**136**	**100.0**	**100.0**	

Job Title

Job Title	Frequency	Percent	Valid Percent	Cumulative Percent
Internal Auditor	16	11.8	11.8	11.8
Staff Accountant	49	36.0	36.0	47.8
Cost Accountant	13	9.6	9.6	57.4
Controller	16	11.8	11.8	69.1
EDP Auditor	3	2.2	2.2	71.3
Manager	27	19.9	19.9	91.2
Other	12	8.8	8.8	100.0
Total	**136**	**100.0**	**100.0**	

Experience

Experience	Frequency	Percent	Valid Percent	Cumulative Percent
1-5	70	51.5	51.5	51.5
6-10	36	26.5	26.5	77.9
11-15	8	5.9	5.9	83.8
16-20	10	7.4	7.4	91.2
21-25	5	3.7	3.7	94.9
< 25 years	7	5.1	5.1	100.0
Total	**136**	**100.0**	**100.0**	

Security Losses

Security Losses	Frequency	Percent	Valid Percent	Cumulative Percent
Actions of employees	47	34.6	34.6	34.6
Actions of outsiders.	13	9.6	9.6	44.1
Nothing	74	54.4	54.4	98.5
Actions of both insiders and outsiders	2	1.5	1.5	100.0
Total	**136**	**100.0**	**100.0**	

Accidental entry of bad data by employees

Accidental entry of bad data by employees	Frequency	Percent	Valid Percent	Cumulative Percent
Less than Once a year	25	18.4	18.4	18.4
Once a year to monthly	47	34.6	34.6	52.9
Once a month to weekly	27	19.9	19.9	72.8
Once a week to daily	30	22.1	22.1	94.9
daily or more frequently	5	3.7	3.7	98.5
Never	2	1.5	1.5	100.0
Total	**136**	**100.0**	**100.0**	

Intentional entry of bad data by employees

Intentional entry of bad data by employees	Frequency	Percent	Valid Percent	Cumulative Percent
Less than Once a year	67	49.3	49.3	49.3
Once a year to monthly	31	22.8	22.8	72.1
Once a month to weekly	14	10.3	10.3	82.4
Once a week to daily	6	4.4	4.4	86.8
daily or more frequently	4	2.9	2.9	89.7
Never	14	10.3	10.3	100.0
Total	**136**	**100.0**	**100.0**	

Accidental destruction of data by employees

Accidental Destruction of Data by Employees	Frequency	Percent	Valid Percent	Cumulative Percent
Less than Once a year	51	37.5	37.5	37.5
Once a year to monthly	40	29.4	29.4	66.9
Once a month to weekly	25	18.4	18.4	85.3
Once a week to daily	6	4.4	4.4	89.7
daily or more frequently	1	.7	.7	90.4
Never	13	9.6	9.6	100.0
Total	**136**	**100.0**	**100.0**	

Intentional destruction of data by employees

Intentional destruction of data by employees	Frequency	Percent	Valid Percent	Cumulative Percent
Less than Once a year	81	59.6	59.6	59.6
Once a year to monthly	22	16.2	16.2	75.7
Once a month to weekly	12	8.8	8.8	84.6
Once a week to daily	3	2.2	2.2	86.8
daily or more frequently	1	.7	.7	87.5
Never	17	12.5	12.5	100.0
Total	**136**	**100.0**	**100.0**	

Unauthorized access to the data and / or system by employees

Unauthorized access to the data and / or system by employees	Frequency	Percent	Valid Percent	Cumulative Percent
Less than Once a year	92	67.6	67.6	67.6
Once a year to monthly	14	10.3	10.3	77.9
Once a month to weekly	13	9.6	9.6	87.5
Once a week to daily	2	1.5	1.5	89.0
Never	15	11.0	11.0	100.0
Total	**136**	**100.0**	**100.0**	

Unauthorized access to the data and / or system by outsider

Unauthorized access to the data and / or system by outsiders	Frequency	Percent	Valid Percent	Cumulative Percent
Less than Once a year	94	69.1	69.1	69.1
Once a year to monthly	14	10.3	10.3	79.4
Once a month to weekly	4	2.9	2.9	82.4
Once a week to daily	4	2.9	2.9	85.3
daily or more frequently	3	2.2	2.2	87.5
Never	17	12.5	12.5	100.0
Total	**136**	**100.0**	**100.0**	

Employees' sharing of passwords

Employees' sharing of passwords	Frequency	Percent	Valid Percent	Cumulative Percent
Less than Once a year	60	44.1	44.1	44.1
Once a year to monthly	26	19.1	19.1	63.2
Once a month to weekly	12	8.8	8.8	72.1
Once a week to daily	13	9.6	9.6	81.6
daily or more frequently	12	8.8	8.8	90.4
Never	13	9.6	9.6	100.0
Total	**136**	**100.0**	**100.0**	

Natural disaster

Natural disaster	Frequency	Percent	Valid Percent	Cumulative Percent
Less than Once a year	97	71.3	71.3	71.3
Once a year to monthly	17	12.5	12.5	83.8
Once a month to weekly	1	.7	.7	84.6
Once a week to daily	4	2.9	2.9	87.5
daily or more frequently	3	2.2	2.2	89.7
Never	14	10.3	10.3	100.0
Total	**136**	**100.0**	**100.0**	

Human- made disasters

Human- made disasters	Frequency	Percent	Valid Percent	Cumulative Percent
Less than Once a year	96	70.6	70.6	70.6
Once a year to monthly	18	13.2	13.2	83.8
Once a month to weekly	2	1.5	1.5	85.3
Once a week to daily	3	2.2	2.2	87.5
daily or more frequently	3	2.2	2.2	89.7
Never	14	10.3	10.3	100.0
Total	**136**	**100.0**	**100.0**	

Introduction (entry) of computer viruses to the system

Introduction (entry) of computer viruses to the system	Frequency	Percent	Valid Percent	Cumulative Percent
Less than Once a year	71	52.2	52.2	52.2
Once a year to monthly	30	22.1	22.1	74.3
Once a month to weekly	12	8.8	8.8	83.1
Once a week to daily	7	5.1	5.1	88.2
daily or more frequently	3	2.2	2.2	90.4
Never	13	9.6	9.6	100.0
Total	**136**	**100.0**	**100.0**	

Suppression or destruction of output

Suppression or destruction of output	Frequency	Percent	Valid Percent	Cumulative Percent
Less than Once a year	81	59.6	59.6	59.6
Once a year to monthly	19	14.0	14.0	73.5
Once a month to weekly	13	9.6	9.6	83.1
Once a week to daily	3	2.2	2.2	85.3
daily or more frequently	5	3.7	3.7	89.0
Never	15	11.0	11.0	100.0
Total	**136**	**100.0**	**100.0**	

Creation of fictitious / incorrect output

Creation of fictitious / incorrect output	Frequency	Percent	Valid Percent	Cumulative Percent
Less than Once a year	75	55.1	55.1	55.1
Once a year to monthly	29	21.3	21.3	76.5
Once a month to weekly	10	7.4	7.4	83.8
Once a week to daily	7	5.1	5.1	89.0
daily or more frequently	2	1.5	1.5	90.4
Never	13	9.6	9.6	100.0
Total	**136**	**100.0**	**100.0**	

Theft of data / information

Theft of data / information	Frequency	Percent	Valid Percent	Cumulative Percent
Less than Once a year	95	69.9	69.9	69.9
Once a year to monthly	12	8.8	8.8	78.7
Once a month to weekly	8	5.9	5.9	84.6
Once a week to daily	4	2.9	2.9	87.5
daily or more frequently	4	2.9	2.9	90.4
Never	13	9.6	9.6	100.0
Total	**136**	**100.0**	**100.0**	

Unauthorized copying of output

Unauthorized copying of output	Frequency	Percent	Valid Percent	Cumulative Percent
Less than Once a year	91	66.9	66.9	66.9
Once a year to monthly	18	13.2	13.2	80.1
Once a month to weekly	4	2.9	2.9	83.1
Once a week to daily	4	2.9	2.9	86.0
daily or more frequently	4	2.9	2.9	89.0
Never	15	11.0	11.0	100.0
Total	**136**	**100.0**	**100.0**	

Unauthorized document visibility

Unauthorized document visibility	Frequency	Percent	Valid Percent	Cumulative Percent
Less than Once a year	80	58.8	58.8	58.8
Once a year to monthly	22	16.2	16.2	75.0
Once a month to weekly	12	8.8	8.8	83.8
Once a week to daily	8	5.9	5.9	89.7
daily or more frequently	5	3.7	3.7	93.4
Never	9	6.6	6.6	100.0
Total	**136**	**100.0**	**100.0**	

Unauthorized printing and distribution of information

Unauthorized printing and distribution of information	Frequency	Percent	Valid Percent	Cumulative Percent
Less than Once a year	82	60.3	60.3	60.3
Once a year to monthly	23	16.9	16.9	77.2
Once a month to weekly	8	5.9	5.9	83.1
Once a week to daily	4	2.9	2.9	86.0
daily or more frequently	5	3.7	3.7	89.7
Never	14	10.3	10.3	100.0
Total	**136**	**100.0**	**100.0**	

Prints and distributed information are directed to people who are not entitled to receive .

Prints and distributed information are directed to people who are not entitled to receive it.	Frequency	Percent	Valid Percent	Cumulative Percent
Less than Once a year	75	55.1	55.1	55.1
Once a year to monthly	30	22.1	22.1	77.2
Once a month to weekly	11	8.1	8.1	85.3
Once a week to daily	1	.7	.7	86.0
daily or more frequently	8	5.9	5.9	91.9
Never	11	8.1	8.1	100.0
Total	**136**	**100.0**	**100.0**	

Sensitive documents are handed to non- security cleared personnel for shredding

Sensitive documents are handed to non- security cleared personnel for shredding.	Frequency	Percent	Valid Percent	Cumulative Percent
Less than Once a year	83	61.0	61.0	61.0
Once a year to monthly	26	19.1	19.1	80.1
Once a month to weekly	6	4.4	4.4	84.6
Once a week to daily	5	3.7	3.7	88.2
daily or more frequently	4	2.9	2.9	91.2
Never	12	8.8	8.8	100.0
Total	**136**	**100.0**	**100.0**	

Interception of data transmissions from remote locations

Interception of data transmissions from remote locations	Frequency	Percent	Valid Percent	Cumulative Percent
Less than Once a year	81	59.6	59.6	59.6
Once a year to monthly	24	17.6	17.6	77.2
Once a month to weekly	8	5.9	5.9	83.1
Once a week to daily	2	1.5	1.5	84.6
daily or more frequently	6	4.4	4.4	89.0
Never	15	11.0	11.0	100.0
Total	**136**	**100.0**	**100.0**	

(ملحق: ٣)
(تحليل كارسوكال - ولاس)
Kruskal-Wallis Test

	Accidental entry of bad data by employees	Intentional entry of bad data by employees	Accidental destruction of data by employees	Intentional destruction of data by employees	Unauthorized access to the data and / or system by employees
Chi-Square	8.009	10.748	15.009	15.290	8.474
df	8	8	8	8	8
Asymp. Sig.	.433	.216	.059	.054	.389

	Unauthorized access to the data and / or system by outsiders	Employees' sharing of passwords	Natural disaster	Human-made disasters	Introduction (entry) of computer viruses to the system
Chi-Square	5.771	2.649	8.367	5.677	8.169
df	8	8	8	8	8
Asymp. Sig.	.673	.954	.398	.683	.417

	Suppression or destruction of output	Creation of fictitious / incorrect output	Theft of data / information	Unauthorized copying of output	Unauthorized document visibility
Chi-Square	7.569	12.381	10.723	6.998	4.886
df	8	8	8	8	8
Asymp. Sig.	.477	.135	.218	.537	.770

	Unauthorized printing and distribution of information	Prints directed to people who are not entitled to receive it.	Sensitive documents are handed to non-security cleared personnel for shredding.	Interception of data transmissions from remote locations
Chi-Square	5.383	8.280	7.769	7.342
df	8	8	8	8
Asymp. Sig.	.716	.407	.456	.500

a **Kruskal Wallis Test**
b **Grouping Variable: The Type of Business**

CAIS Security Threats		Sum of Squares	df	Mean Square	F	Sig.
Theft of data / information	Between Groups	21.595	8	2.699	1.009	.433
	Within Groups	339.750	127	2.675		
	Total	361.346	135			
Unauthorized copying of output	Between Groups	9.154	8	1.144	.385	.927
	Within Groups	377.486	127	2.972		
	Total	386.640	135			
Unauthorized document visibility	Between Groups	9.844	8	1.231	.516	.843
	Within Groups	303.148	127	2.387		
	Total	312.993	135			
Unauthorized printing and distribution of information	Between Groups	6.088	8	.761	.262	.977
	Within Groups	368.728	127	2.903		
	Total	374.816	135			
Prints are directed to people who are not entitled to receive	Between Groups	12.072	8	1.509	.588	.786
	Within Groups	325.663	127	2.564		
	Total	337.735	135			
Sensitive documents are handed to non-security cleared personnel for shredding.	Between Groups	13.427	8	1.678	.659	.726
	Within Groups	323.213	127	2.545		
	Total	336.640	135			
Interception of data transmissions from remote locations	Between Groups	18.087	8	2.261	.771	.628
	Within Groups	372.317	127	2.932		
	Total	390.404	135			