

استكشاف المخاطر التي تهدد نظم المعلومات المحاسبية المحوسبة في الشركات

الفلسطينية العاملة في قطاع غزة: دراسة تطبيقية

د. عصام محمد البحيصي

قسم المحاسبة - كلية التجارة

الجامعة الإسلامية - غزة - فلسطين

ملخص: تهدف هذه الدراسة إلى بحث المخاطر التي تهدد نظم المعلومات المحاسبية المحوسبة الفلسطينية في قطاع غزة كنموذج لما هو موجود في باقي الدول النامية. ومن أجل تحقيق هذا الهدف تم تنفيذ واستخدام استبيان أعد خصيصاً لهذا الأمر، وقد تم توزيع الاستبيان على عينة من الشركات الفلسطينية وعددها 200 شركة، وقد تم استرجاع 97 منها أي ما يعادل 47% من مجموع مفردات العينة. وقد أظهرت النتائج الإحصائية أن من أهم هذه المخاطر: (1) الإدخال المتعمد للبيانات الخاطئة عن طريق المستخدمين و(2) انقطاع التيار الكهربائي و(3) الإتلاف غير المقصود للبيانات من قبل المستخدمين و(4) اشتراك العاملين في كلمات الدخول للحاسوب و(5) الكوارث من صنع الإنسان و(6) دخول الفيروسات إلى الأنظمة. إضافة إلى ذلك فقد أظهر البحث أن الشركات الفلسطينية تختلف فيما بينها في درجة تكرار وأهمية المخاطر حسب نوعية نظام المعلومات المستخدم وحسب مدى الارتباط بشبكة الانترنت. إلا أنه ليس هناك ارتباط بين نوع المؤسسة (القطاع الذي تنتمي إليه المؤسسة) ودرجة تكرار وأهمية المخاطر التي تتعرض لها الشركات الفلسطينية. كما أن مقارنة نتائج الدراسة مع نتائج الدراسات السابقة، أظهر أن الأخطار التي تتعرض لها الشركات الفلسطينية هي شبيهة إلى حد كبير بالأخطار التي تتعرض لها الشركات في الدول الأخرى، بخاصة النامية منها. ولعل التوصية الأكثر أهمية هنا هي ضرورة زيادة الاهتمام بأمن المعلومات خاصة لدى الشركات التي تستخدم نظام الشبكات والتي ترتبط بشبكة الانترنت. إضافة إلى ذلك فإن الباحث يوصي بضرورة رقابة أداء العاملين ذوي العلاقة المباشرة مع البيانات وتطوير قدراتهم وكفاءاتهم في مجال الحاسوب وذلك لضمان عدم إدخال متعمد للبيانات الخاطئة أو إتلاف غير مقصود للبيانات السليمة. ويشدد الباحث على ضرورة التزام العاملين ذوي العلاقة بالبيانات بعدم إعطاء كلمات الدخول الخاصة بهم لآخرين، وذلك لضمان عدم استخدامها في أمور تزيد من حدة بعض المخاطر التي تتعرض لها أنظمة المعلومات المحاسبية المحوسبة في الشركات.

Exploring the perceived threats of the computerized accounting information system in Palestinian firms at Gaza Strip: Practical Study

Abstract: The objective of this paper is to investigate the significant perceived security threats of computerized accounting information systems (CAIS) in Palestinian organizations at Gaza Strip. An empirical survey using a self-administered questionnaire has been carried out to achieve this objective. The survey results revealed that most of the responded

organizations have suffered from these threats. The statistical results also revealed that accidental and intentional entry of bad data; accidental destruction of data by employees; employees' sharing of passwords; introduction of computer viruses to CAIS; and electricity problems; are the most significant perceived security threats to CAIS in Palestinian organizations. Accordingly, it is recommended to strengthen the security controls over the above weaken security areas and to enhance the awareness of CAIS security issues among Palestinian organizations to achieve better protection to their CAIS.

مقدمة:

إن التطور السريع في تكنولوجيا المعلومات وسهولة الحصول عليها أدى إلى تزايد أعداد مستخدمي هذه التكنولوجيا، سواء من الأفراد أو المؤسسات بشكل هائل . كما أن الرغبة الشديدة لدى المؤسسات لإكتساب وتطبيق النظم والبرامج المحوسبة ساهمت بشكل فعال في الانتشار الواسع لنظم المعلومات. وقد كانت المحاسبة من أهم المجالات التي تأثرت بهذا التغيير حيث شهد النصف الثاني من القرن الماضي تحولاً سريعاً نحو استخدام نظم المعلومات المحاسبية المحوسبة والتي ساهمت بشكل فعال في تطوير الأداء المحاسبي و الإداري خاصة عبر المساهمة في الحصول على معلومات مالية صالحة لإتخاذ القرار في الوقت المناسب. لكن استخدام هذه التكنولوجيا المتقدمة تعرض لمخاطر هامة وعديدة خاصة فيما يتعلق بضمان سلامة وأمن نظم المعلومات المحاسبية المحوسبة . إضافة إلى ذلك فإن التطور الهائل في تكنولوجيا المعلومات لم يصاحبه تطور مماثل في القدرات والكفاءات البشرية من مستخدمي هذه التكنولوجيا، الأمر الذي خلق بدوره نوعاً آخر من المخاطر التي تحد من فاعلية وكفاءة استخدام هذه التقنيات. وتستوجب هذه المخاطر أن تكون المؤسسات أكثر وعياً ومعرفة بالمخاطر الأمنية المحتملة التي تهدد أمن أنظمتها وكفاءة وفعالية استخدامها من أجل العمل على تلافي هذه المخاطر والحد من آثارها السلبية ما أمكن. وعلى الرغم من الجهود المضنية التي تبذل للتخفيف من هذه الخاطر، إلا أنه لا زالت هناك حاجة لبذل المزيد من الجهود من أجل تحقيق هذا الهدف. ويمكننا القول أن دراستنا هذه هي جزء من هذا المجهود الذي يهدف إلى دراسة المخاطر التي تهدد نظم المعلومات المحاسبية المحوسبة في البيئة الفلسطينية كنموذج لمثيلاتها في الدول النامية. ويشتمل البحث بعد المقدمة على أقسام عديدة، في أولها يتم إستعراض مشكلة وأهداف وأهمية وفرضيات ومنهجية البحث وفي ثانيها يتم عرض الأدبيات و الدراسات السابقة حول الموضوع. وفي ثالثها يتم عرض تحليل ونتائج البحث، وفي النهاية يتم تقديم خلاصة البحوث كذلك ما يراه الباحث مناسباً من التوصيات.

استكشاف المخاطر التي تهدد نظم المعلومات المحاسبية المحوسبة

مشكلة الدراسة:

لقد أشارت الدراسات السابقة حول موضوع البحث إلى وجود بعض المخاطر التي تواجه استخدام نظم المعلومات المحاسبية المحوسبة المستخدمة في الشركات في الدول النامية. وتتلخص مشكلة الدراسة في فحص إمكانية وجود مثل هذه المخاطر في الشركات الفلسطينية في قطاع غزة، وتقدير مدى أهميتها. و عليه فإن البحث يحاول الإجابة على الأسئلة التالية:

- 1- ماهي المخاطر التي تهدد نظم المعلومات المحاسبية المحوسبة في الشركات الفلسطينية في قطاع غزة، و ما هي درجة تكرارها و كذلك درجة أهميتها ؟
- 2- معرفة العوامل التي تؤثر على درجة تكرار وأهمية المخاطر التي تهدد نظم المعلومات المحاسبية المحوسبة في الشركات الفلسطينية في قطاع غزة.
- 3- هل المخاطر التي تهدد نظم المعلومات المحاسبية المحوسبة في الشركات الفلسطينية في قطاع غزة تشبه تلك التي تهدد الشركات في الدول النامية ؟

هدف الدراسة:

تهدف هذه الدراسة إلى إستطلاع مدى وجود مخاطر تهدد نظم المعلومات المحاسبية المحوسبة المستخدمة في الشركات الفلسطينية. وما هي أهمية كل نوع منها؟. إضافة إلى معرفة هل المخاطر التي تهدد استخدام نظم المعلومات المحاسبية المحوسبة في فلسطين شبيهة بتلك الموجودة في باقي الدول النامية؟. وما هي سبل الحد منها أو القضاء عليها في حال وجودها ؟

أهمية الدراسة:

تتبع أهمية الدراسة من عاملين أساسيين، أولهما هو الاستخدام المتزايد لنظم المعلومات المحاسبية المحوسبة في فلسطين. و ثانيهما هو ندرة الأبحاث (في حدود علم الباحث) التي تتطرق إلى موضوع البحث في البيئة الفلسطينية، إضافة إلى ندرة مثل الأبحاث بشكل عام. كما أن البحث يمكن أن يكون ذا فائدة عظيمة للشركات في قطاع غزة للإستفادة من نتائجه في التعرف على المشاكل التي تهدد نظمها المحاسبية، و طرق التغلب عليها.

الدراسات السابقة:

عند استعراض الدراسات السابقة حول موضوع المخاطر التي تهدد نظم المعلومات المحاسبية المحوسبة ، نجد أن هذه الدراسات قليلة نسبياً قياساً بما ينشر حول موضوعات بحثية أخرى وذلك لأن موضوع نظم المعلومات المحاسبية و البحث فيه هو أمر جديد نسبياً قياساً بفروع العلوم الأخرى. كما يتضح أن أغلب هذه الدراسات تدرج تحت مسمى المخاطر الأمنية التي من المحتمل أن تهدد نظم المعلومات المحاسبية المحوسبة في أي مؤسسة. ومن هذه

د. عصام البحيصي

الدراسات دراسة (1999) Dhillon التي ناقشت الخسائر المترتبة على اختراقات أمن المعلومات. ودراسة Siponen (2000) التي ركزت على السيطرة على أمن نظم المعلومات. ودراسة Riner, et. al. (1991) التي تناولت موضوع تحليل مخاطر نظم المعلومات في بيئة الأعمال. إلا أننا سنخصص بالتفصيل بعض الدراسات التي تناولت موضوع البحث بشكل أساسي و مفصل. ومن أهم هذه الدراسات :

دراسة (1992) Lock et. al.:

الذي قام بمحاولة استكشاف لمدى فهم المدراء التنفيذيين لنظم المعلومات الإدارية فيما يتعلق بالمخاطر التي تهدد استخدام جهاز الحاسوب وبيئة الشبكات ، وكان هدف الدراسة هو البحث عن إجابة لسؤالين هما :

1- ما هي المخاطر التي تهدد نظم المعلومات المحاسبية المحوسبة؟

2- وما هي أخطر هذه التهديدات؟؟.

وقد طور Lock et. al قائمة بحوالي 13 خطراً يهدد هذه النظم هي :

1- قيام الموظفين بإدخال عرضي لبيانات خاطئة

2- قيام الموظفين بإدخال متعمد لبيانات خاطئة.

3- قيام الموظفين بتدمير غير مقصود للبيانات.

4- قيام الموظفين بتدمير مقصود للبيانات.

5- قيام الموظفين بدخول غير مفوض (غير مسموح) للبيانات و النظام.

6- مراقبة غير مناسبة على وسائط التخزين (أقراص و أشرطة).

7- الضبط الضعيف على المعالجة اليدوية للمدخلات و المخرجات .

8- دخول للبيانات وللأنظمة من أشخاص خارجيين (قراصنة)

9- الدخول للبيانات والأنظمة من قبل خارجيين (منافسين)

10- دخول فيروسات ومنتسللين في نظام الحاسوب

11 - مراقبة مادية ضعيفة و غير فعالة و غير مناسبة للعمل عبر النظام.

12 - كارثة طبيعية: حريق، فيضان.

13 - انقطاع التيار و الاتصالات.

وقد تم تصميم و تنفيذ و توزيع استبيان على 657 مدير متقاعد في الولايات المتحدة الأمريكية حيث طلب من المشاركين أن يصنفوا أكثر ثلاث مخاطر تهدد النظام ضمن قائمة المخاطر المعطاة لهم ، وقد بلغت نسبة الاستجابة حوالي 20% من العينة. لقد استخدمت هذه الدراسة

استكشاف المخاطر التي تهدد نظم المعلومات المحاسبية المحوسبة

ثلاثة مناهج لتحليل البيانات من أجل تحديد الخطر الذي يهدد نظم المعلومات المحاسبية المحوسبة، وقد أوضحت نتائج الدراسة أن المخاطر الخارجية حصلت على نسبة 37% من الأصوات بينما حصلت المخاطر الداخلية على نسبة 62.4% من مجموع الأصوات وهذا يؤكد مزاعم الخبراء أن المخاطر العظمى تأتي من الداخل وليس من الخارج. وقد كشفت الدراسة أن الإلتلاف غير المقصود للبيانات عن طريق المستخدمين وإدخال البيانات الخاطئة والضبط غير الملائم قد شكلت أهم المخاطر الداخلية التي تهدد هذا النظام ، في حين كانت الكوارث الطبيعية والدخول للأنظمة عن طريق الخارجين (القرصنة) من أهم المخاطر الخارجية التي تهدد أجهزة عملية استخدام النظم المحوسبة .

دراسة Davis (1997):

حاول **Davis** استكشاف المخاطر التي تهدد نظم المعلومات المحاسبية، حيث أجرى دراسته على عينة عشوائية من أعضاء جمعية مدققي الحسابات لنظم المعلومات، والمعهد الأمريكي للمحاسبين القانونيين ، مستخدماً إستبيان يحتوي على قائمة مخاطر مطورة عن تلك التي أعدها (1992) Lock et. al. وقد أشارت النتائج إلى أن 95% ممن المبحوثين يشعرون بأن مستوى هذه المخاطر عادي ، ومعقولة بشكل عام، علاوة على ذلك فإن مدققي حسابات نظم المعلومات أقرروا أن بيانات الحاسوب المختلفة لها مستويات نسبية مختلفة للمخاطر. وقد أظهرت النتائج أن إلتلاف البيانات بصورة غير متعمدة وإدخال المستخدمين للبيانات الخاطئة بصورة متعمدة ودخول فيروسات للحواسيب تعتبر أعلى ثلاث مخاطر، كما أن الدخول غير المصرح به للبيانات أو للنظام وإدخال البيانات الخاطئة بصور غير متعمدة عن طريق المستخدمين والفهم السيئ لواجبات نظام المعلومات قد صنفت على أنها من المخاطر المهمة التي تهدد نظم المعلومات المحاسبية المحوسبة.

دراسة Ryan and Bordoloi (1997):

الذاتان حاولا الكشف عن نفس المخاطر التي تهدد استخدام نظم المعلومات المحوسبة و لكن في ظل بيئتين مختلفتين، إحداهما خاصة باستخدام الحاسوب الشخصي (PC) والأخرى خاصة باستخدام الحاسوب في بيئة الشبكات ووجود السيرفر (Server). وقد استخدم Ryan and Bordoloi نفس قائمة المخاطر التي استخدمها (1992) Lock et. al. في استبيان وزع منه 120 نسخة على حاضري أحد مؤتمرات الفنيين في نظم المعلومات، تم إستعادة 57 منها مكتملة شكلت 47% من العينة. وأستخدم في هذه الدراسة مقياس التصنيف من 1 إلى 10، بحيث كان الرقم 1 يرمز إلى أدنى درجة و الرقم 10 إلى أقصى درجة. علاوة على ذلك فقد طلب من

د. عصام البحيصي

المبوثين تصنيف درجة الحيطة والحذر التي تقوم بها المؤسسة للوقاية من هذه المخاطر واستخدم نفس المقياس (1-10) حيث الرقم 1 تعني أنه لم تؤخذ أي إجراءات فيما الرقم 10 يعني أن الإجراءات قد اتخذت بشكل مرتفع. وأشارت نتائج الدراسة إلى وجود 7 أخطار ذات أهمية عالية و هي :

- 1- الإتلاف غير مقصود للبيانات عن طريق المستخدمين .
- 2- إدخال غير مقصود للبيانات الخاطئة عن طريق المستخدمين .
- 3- الإتلاف المتعمد للبيانات عن طريق المستخدمين .
- 4- إدخال بيانات خاطئة بصورة متعمدة عن طريق المستخدمين .
- 5- الخسارة بسبب الاحتياطات غير الملائمة .
- 6- الكوارث الطبيعية .
- 7- النقطة أحادية للفشل .

كما أظهرت نتائج الدراسة وجود فوارق بين البيئتين محل الدراسة و أن الأخطار كانت في بيئة الشبكة أعلى منها في بيئة الحاسب الشخصي، وأن الشركات اتخذت إجراءات وقاية في حالة الشبكة (Server) أعلى منها في حالة الحاسوب الشخصي (PC)

دراسة Henry (1997):

أجرى هنري دراسةً على 261 شركة في ولاية فرجينيا ، لتحديد طبيعة النظم المحاسبية ومستوى الأمن المتبع لدى هذه الشركات. وقد أشارت نتائج هذه الدراسة إلى أن معظم الشركات (80.3%) تدعم أمن أنظمتها المحاسبية بطريقة أو بأخرى، وأن 74.4% منها يجعل الدخول إلى النظام عبر كلمة دخول سرية وحوالي 43% يستخدم برنامج حماية ضد الفيروسات، فيما أبرزت الدراسة أن حوالي 15% فقط تقوم بتشفير بياناتها وأن حوالي 45% منها أخضعت بياناتها لنوع من التدقيق.

دراسة ابو موسى (2001):

تم في هذه الدراسة بحث أهمية المخاطر التي تهدد نظم المعلومات المحاسبية المحوسبة في البنوك المصرية مستخدماً استبياناً خاصاً تم توزيعه على رؤساء أقسام تدقيق الحسابات الداخلية ورؤساء أقسام الحاسوب في 66 مقراً بنكياً رئيساً في مصر. وقد بلغت نسبة الاستجابة من أقسام الحاسوب 79.3% ومن أقسام الحسابات 56.9%. وقد اشتمل استبيان أبو موسى على قائمة مستمدة من الدراسات السابق ذكرها، و تشتمل على 19 خطراً تهدد نظام الصناعة البنكية في مصر. كما وقد تم استخدام المقياس الخماسي للبحث والتحقق من أهمية هذه المخاطر، و قد كشفت نتائج هذه

استكشاف المخاطر التي تهدد نظم المعلومات المحاسبية المحوسبة

الدراسة أن قيام الموظفين بإدخال غير مقصود لبيانات خاطئة وكذلك قيامهم بتدمير عرضي للبيانات، ودخول فيروسات للنظام والكوارث الطبيعية التي هي من صنع الإنسان تعتبر من أهم المخاطر التي تهدد نظم المعلومات في البنوك المصرية.

دراسة (2002) Waren:

والتي قام فيها بالتعرف على أهم المشاكل التي تواجه نظم المعلومات في عينة من الشركات الأمريكية والانجليزية و الاسترالية و قد توصل فيها إلى أن ضعف إجراءات الأمن التكنولوجي هي أهم مشاكل نظم المعلومات في الشركات الانجليزية و أن ضعف سياسات الأمن التكنولوجي هي أهم مشاكل النظم في الشركات الاسترالية، و أن الإدخال الخاطئ المتعمد للبيانات المالية تمثل أهم مشاكل النظم في الشركات الأمريكية.

دراسة (2005) Hunton et. Al.:

و التي أجرى فيها مقارنة بين وعي المدققين الماليين ومدققي نظم المعلومات بالمخاطر التي تتعرض لها نظم المعلومات المحاسبية في الشركات الأمريكية. و قد توصل في دراسته إلى أن مدققي نظم المعلومات يتفوقون بدرجة كبيرة على المدققين الماليين في اكتشاف المخاطر التي تهدد نظم المعلومات في الشركات الأمريكية و كذلك في تقييم أثر هذه المخاطر على قدرة الشركات على الاستمرار و سلامة مركزها المالي و الإنتاجي.

دراسة أبو موسى (2006):

والتي تناول فيها تقييم المخاطر التي تهدد نظم المعلومات المحاسبية المحوسبة في الشركات في المملكة العربية السعودية. حيث قام بتوزيع إستبيان على عينة من مدراء الشركات و رؤساء أقسام المحاسبة فيها (136 شركة تشمل جميع القطاعات الاقتصادية المختلفة). و قد توصل أبو موسى إلى أن الإدخال الخاطئ المتعمد و غير المتعمد للبيانات و التدمير غير المقصود للبيانات و مشاركة كلمة السر بين الموظفين و دخول الفيروسات للأجهزة هل أهم المخاطر التي تتعرض لها نظم المعلومات المحاسبية المحوسبة في الشركات السعودية. كما توصل أبو موسى إلى أنه لا يوجد اختلاف في هذا الأمر يعزى الى نوع الشركة أو القطاع الاقتصادي الذي تنتمي إليه.

دراسة البحيصي و الشريف (2008):

وهدفت الدراسة الى التعرف على طبيعة المخاطر التي تهدد أمن نظم المعلومات المحاسبية الإلكترونية في بيئة المصارف العاملة في قطاع غزة ومعدلات تكرارها، و أسباب حدوثها، و على إجراءات الحماية التي تتبعها المصارف العاملة في قطاع غزة للحد من المخاطر التي تهدد نظم المعلومات المحاسبية الإلكترونية؛ وكذلك التمييز بين مخاطر أمن نظم المعلومات وعدم كفاية

د. عصام البحيسي

الضوابط الرقابية لأمن تلك النظم. و استخدمت الدراسة نفس المنهجية المستخدمة في هذا البحث، وتوصلت الى مجموعة من النتائج أهمها: اعتماد المصارف العاملة في قطاع غزة في عملها بشكل كبير على النظام الآلي، إلا أن هذا الاعتماد لا يتفق مع عدد موظفي تكنولوجيا المعلومات في المصارف حيث تعتمد الفروع على موظف واحد مهمته تشغيل أنظمة الحاسوب بينما الموظفون المختصون يكون مكانهم في المراكز الرئيسية للفروع وغالبا ما توجد في الضفة الغربية. كذلك كانت تعتبر مخاطر الإدخال غير المتعمد واشتراك الموظفين في كلمة السر وتوجيه البيانات والمعلومات إلى أشخاص غير مصرح لهم بذلك؛ أكثر المخاطر تكرارا حيث قد تحدث أكثر من مرة شهريا إلى مرة أسبوعيا. كما أوضحت الدراسة أن حدوث مخاطر نظم المعلومات المحاسبية الالكترونية ترجع إلى أسباب تتعلق بموظفي البنك نتيجة قلة الخبرة والوعي والتدريب، إضافة إلى أسباب تتعلق بإدارة المصرف نتيجة لعدم وجود سياسات واضحة ومكتوبة وضعف الإجراءات والأدوات الرقابية المطبقة لدى المصرف.

منهجية الدراسة:

في الدراسات السابقة حول الموضوع تم تطوير قائمة للمخاطر التي تهدد عملية استخدام نظم المعلومات المحاسبية المحوسبة وقد تم تحديد هذه القائمة بناءً على أسس علمية ونتائج موضوعية. ومن خلال هذه الدراسة يقوم الباحث بإجراء مسح لعينة من الشركات في فلسطين لمعرفة مدى تأثير هذه الشركات بالأخطار الواردة في هذه القائمة وما هي أهمية كل نوع منها، وهل هناك فروق بين الشركات الفلسطينية فيما يتعلق بهذه المخاطر؟ ويتم ذلك المسح عبر استبيان يوزع على عينة من الشركات ثم تحلل نتائجه فيما بعد باستخدام البرنامج الإحصائي SPSS.

فرضيات الدراسة:

- 1- لا توجد مخاطر تهدد نظم المعلومات المحاسبية المحوسبة المستخدمة في الشركات الفلسطينية
- 2- لا توجد فروقات هامة ذات دلالة احصائية بين مختلف المؤسسات الفلسطينية فيما يتعلق بأهمية التهديدات التي تواجه نظم المعلومات المحاسبية.
- 3- توجد علاقة ذات دلالة احصائية بين نوع النظام المستخدم وبين درجة تكرار الأخطاء الموجودة وأهميتها.
- 4- توجد علاقة ذات دلالة احصائية بين مدى الاتصال بشبكة الانترنت وبين درجة تكرار الأخطاء الموجودة وأهميتها.

استكشاف المخاطر التي تهدد نظم المعلومات المحاسبية المحوسبة

5- لا توجد علاقة ذات دلالة إحصائية بين حجم رأس مال الشركة وبين درجة تكرار الأخطاء الموجودة وأهميتها.

مجتمع وعينة البحث:

نظراً لأنه ليس هناك إحصائية دقيقة للمنشآت والشركات العاملة في قطاع غزة، والتي تستخدم نظم المعلومات المحاسبية المحوسبة، فقد اجتهد الباحث باختيار عينة تتكون من جميع الشركات التي يعلم الباحث من خلال خبرته الشخصية بأنها تقوم باستخدام مثل هذه النظم. ويبلغ عدد مفردات العينة التي تم اختيارها 200 شركة تمثل مختلف القطاعات الاقتصادية الفلسطينية. وقد شملت العينة شركات من مختلف الأشكال القانونية، إلا أن أغلب مفردات العينة من شركات التضامن و التي تمثل غالبية الشركات في قطاع غزة. و ربما كان هذا الأمر مدعاة لتعميم النتائج على قطاع شركات التضامن بشكل أكبر من غيرها من الأنواع الأخرى للشركات.

أداة البحث :

قام الباحث بتصميم إستبيان خاص لتحقيق هدف الدراسة تم توزيعه على جميع مفردات العينة. وقد تكون الإستبيان من قسمين أساسيين هما:

- 1- القسم الخاص بالمعلومات المهنية عن الشركة و الموظف الذي يعبئ الإستبيان
- 2- القسم الخاص بالموضوع محل البحث.

قد تم توزيع إستبيان واحدة على كل شركة من مفردات العينة، على أن يقوم بتعبئتها أحد الأشخاص التالية مسمياتهم الوظيفية (محاسب، رئيس قسم حسابات، مدير مالي، مدير عام) حسب ما هو متوفر في هيكلية الشركة وبعد حوالي شهرين من التوزيع تم جمع 97 إستبيان مكتمل وصالح للإستعمال بنسبة إستجابة تعادل 48.5%، وهذه نسبة جيدة في مثل هذا النوع من الدراسات.

(للإطلاع على أقسام الإستبيان والمقاييس الإحصائية المستخدمة فيه يمكن الرجوع الى الملحق رقم 1)

نتائج البحث:

أظهر التحليل الإحصائي للإستبيان النتائج التالية:

-أولاً/ خصائص العينة

توضح الجداول التالية أهم خصائص العينة محل الدراسة، وتشمل كلاً من خصائص الشركات وخصائص الموظفين الذين قاموا بتعبئة الإستبيان.

د. عصام البحيصي

الجدول رقم (1) يوضح توزيع مفردات العينة حسب القطاعات الاقتصادية التي تتبع لها وكذلك توزيعها حسب حجم رأس المال.

جدول رقم (1)

توزيع مفردات العينة حسب القطاعات الاقتصادية التي تتبع لها وحسب الحجم

| القطاع الاقتصادي | عدد | نسبة |
|--------------------|-----|------------|
| صناعي | 14 | 14.4% |
| تجاري | 29 | 29.9% |
| زراعي | 2 | 2.1% |
| خدمات | 35 | 36% |
| بنوك | 5 | 5.2% |
| شركات تأمين | 3 | 3.1% |
| بناء و تشييد | 9 | 9.3% |
| المجموع | 97 | 100% |
| حجم رأس مال الشركة | عدد | نسبة مئوية |
| اقل من \$10000 | 22 | 22.7% |
| \$100000- 10000 | 45 | 46.4% |
| \$1000000- 100000 | 19 | 19.6% |
| أكبر من \$ 1000000 | 11 | 11.3% |
| المجموع | 97 | 100% |

من الجدول السابق يتضح أن العينة تشتمل على مفردات تمثل جميع القطاعات الاقتصادية في فلسطين سواء كانت خدماتية أو تجارية أو إنتاجية، أو شركات مالية (بنوك و شركات تأمين) أو غير مالية. كما يلاحظ أنه يغلب على مفردات العينة طابع المنشآت التجارية والخدمية، والتي تشكل أغلبية المنشآت على أرض الواقع، الأمر الذي يجعلها تمثل بشكل واقعي إلى حد كبير البيئة الاقتصادية الفلسطينية.

أما من حيث رأس المال كعامل أساسي في قياس حجم الشركات، فمن الملاحظ أن العينة تشتمل على شركات من أغلب الأحجام (صغيرة، متوسطة و كبيرة). كما أنه يغلب على مفرداتها المنشآت ذات الحجم الصغير والمتوسط والتي تمثل ما يزيد على 69% من مفردات العينة، وهذه

استكشاف المخاطر التي تهدد نظم المعلومات المحاسبية المحوسبة

خاصية معروفة في هيكلية الإقتصاد الفلسطيني الذي يعتمد في أغلبه على الشركات الصغيرة والمتوسطة، والتي تزيد نسبتها في فلسطين عن 95%.

أما الجدول رقم (2) فيوضح نوعية النظم المستخدمة من حيث كونها حواسيب منفصلة أو مرتبطة بشبكات وكذلك مدى إرتباط الشركات بشبكة الإنترنت العالمية.

جدول رقم (2)

خصائص مفردات العينة من حيث النظم المستخدمة والإرتباط بشبكة الانترنت

| نسبة | عدد | نوع الحاسوب المستخدم |
|-------|-----|----------------------------|
| 13.4% | 13 | حاسوب مرتبط بشبكة (Server) |
| 86.6% | 84 | حاسوب شخصي PC |
| 100% | 97 | المجموع |
| نسبة | عدد | الإرتباط بالانترنت |
| 19.6% | 19 | مرتبط بشبكة الانترنت |
| 80.4% | 78 | غير مرتبط بشبكة الانترنت |
| 100% | 97 | الإجمالي |

كما هو ملاحظ فإن الغالبية العظمى من الشركات في مفردات العينة تستخدم أجهزة حاسوب شخصية (PC) في أعمالها، في حين أن قلة لا تكاد تصل إلى 14% هي التي تستخدم حواسيب مرتبطة بشبكات (Server). ولعل هذا مرجعه إلى حجم الشركات الصغير من ناحية و إلى ضعف الوعي بأهمية نظم المعلومات المتطورة لدى الشركات الفلسطينية من ناحية أخرى.

كما يتضح من الجدول السابق أن قلة فقط من الشركات الفلسطينية ضمن مفردات العينة مرتبطة بشبكة الإنترنت، في حين أن أغلب الأغلبية العظمى (80.4%) غير مرتبطة بشبكة الإنترنت، وهذا يعكس واقع هذه الشركات التي غالباً ما لا تكون متصلة بمثل هذا النوع من وسائل الاتصال الحديثة. وربما كانت هذه النتيجة عاملاً مهماً في تحديد أنواع المخاطر التي تتعرض لها نظم المعلومات المحوسبة في الشركات المختلفة، حيث أن هناك مخاطر تظهر فقط في الشركات المتصلة بشبكة الإنترنت، لأن مصدرها هو الإتصال بهذه بالشبكة.

أما الجدول رقم (3) فيوضح إحدى أهم الخصائص المهنية للمبجوثين، وهي مركزه الوظيفي داخل المنشأة وكذلك خبرته المهنية.

الجدول رقم (3)

وظيفة و خبرة معبئ الاستبيان في الشركة

| الوظيفة | عدد | نسبة مئوية |
|-----------------|-----|------------|
| مدير عام | 6 | 6.2% |
| مدير مالي | 17 | 17.5% |
| رئيس قسم حسابات | 25 | 25.8% |
| محاسب | 49 | 50.5% |
| المجموع | 97 | 100% |
| الخبرة | عدد | نسبة مئوية |
| اقل من 5 سنوات | 12 | 12.3% |
| 5- 10 سنوات | 57 | 58.8% |
| 11- 20 سنة | 25 | 25.8% |
| 21- 30 سنة | 3 | 3.1% |
| المجموع | 97 | 100% |

من الجدول السابق (رقم 3) يتضح أن أغلبية المبحوثين هم من ذوي العلاقة المباشرة بموضوع البحث. فقد عبأ الاستبيان حوالي 93.8% من موظفي الدائرة المالية (مدير الدائرة، رئيس قسم الحسابات والمحاسب) وهي الدائرة ذات العلاقة بموضوع البحث. كما أن البقية هم مدراء عامون وهؤلاء غالباً ما يكونون من ذوي علاقة مباشرة بالدائرة المالية و نظم المعلومات المستخدمة فيها.

كما يلاحظ من نفس الجدول أن أغلب الذين عبأوا الاستبيان (84.6%) لديهم مستوى جيد من الخبرة تتراوح ما بين 5- 20 سنة. وهذا يشير إلى وجود قدر كافٍ من الخبرة لدى هؤلاء الموظفين للتعرف على مشاكل استخدام نظم المعلومات المحوسبة في شركاتهم وكذلك تحديد مدى أهمية هذه المخاطر بالنسبة إلى هذه الشركات.

ثانياً النتائج الإحصائية

القسم التالي يناقش النتائج الإحصائية المتعلقة بالمخاطر التي تم التطرق إليها و التي سبق الإشارة إليها. الجدولين رقم (4) و (5) يعرضان درجة تكرار و أهمية تلك المخاطر على التوالي.

استكشاف المخاطر التي تهدد نظم المعلومات المحاسبية المحوسبة

جدول رقم (4)

درجة تكرار المخاطر

| لا ادري | لا يحدث مطلقا | مرة على الأقل سنويا | مرة على الأقل شهريا | مرة على الأقل أسبوعيا | مرة على الأقل يوميا | |
|------------|---------------------|---------------------------|---------------------------|-----------------------------|------------------------|---|
| 0 | 4.1% | 36.1% | 30.9% | 16.5% | 12.4% | الإدخال غير المقصود للبيانات الخاطئة عن طريق المستخدمين |
| 0 | 49.5% | 29.9% | 20.6% | 0 | 0 | الإدخال المتعمد للبيانات الخاطئة عن طريق المستخدمين |
| 0 | 19.6% | 43.3% | 28.9% | 8.2% | 0 | الإتلاف غير المقصود للبيانات من قبل المستخدمين |
| 0 | 78.4% | 21.6% | 0 | 0 | 0 | الإتلاف المتعمد للبيانات عن طريق المستخدمين |
| 0 | 88.7% | 11.3% | 0 | 0 | 0 | الدخول غير المصرح به للبيانات أو النظام عن طريق المستخدمين |
| 0 | 96.9% | 3.1% | 0 | 0 | 0 | الدخول غير المصرح به للبيانات أو النظام عن طريق الدخلاء (القرصنة) |
| 0 | 38.1% | 20.6% | 19.6% | 17.6% | 4.1% | اشترك العاملين في كلمات الدخول للحاسوب |

د . عصام البحيصي

| | | | | | | |
|---|-------|-------|-------|-------|-------|--|
| 0 | 97.9% | 2.1% | 0 | 0 | 0 | أثر الكوارث الطبيعية |
| 0 | 0 | 21.6% | 29.9% | 36.1% | 12.4% | اثر انقطاع التيار الكهربائي |
| 0 | 52.6% | 41.2% | 6.2% | 0 | 0 | أثر الكوارث من صنع الإنسان |
| 0 | 34% | 50.5% | 15.5% | 0 | 0 | دخول الفيروسات إلى الأنظمة |
| 0 | 94.8% | 5.2% | 0 | 0 | 0 | كبت وتخريب المخرجات |
| 0 | 92% | 8% | 0 | 0 | 0 | سرقة البيانات و المعلومات |
| 0 | 96% | 4% | 0 | 0 | 0 | النسخ غير المصرح به للمخرجات |
| 0 | 77.3% | 3.1% | 7.2% | 12.4% | 0 | رؤية الوثائق غير المصرح بها |
| 0 | 100% | 0 | 0 | 0 | 0 | طبع وتوزيع البيانات و المعلومات غير المصرح به |
| 0 | 99% | 1% | 0 | 0 | 0 | تخصيص المطبوعات و توزيع المعلومات على أشخاص غير مؤهلين لإستلامها |
| 0 | 99% | 1% | 0 | 0 | 0 | تسليم المستندات أو الوثائق الحساسة لموظف غير مضمون (مؤتمن) ليمزقها |
| 0 | 87.6% | 6.2% | 4.1% | 2.1% | 0 | حصر أو وقف تحويلات البيانات |

استكشاف المخاطر التي تهدد نظم المعلومات المحاسبية المحوسبة

جدول رقم (5)

أهمية المخاطر

| المتوسط | ضعيفة جدا | ضعيفة | متوسطة | عالية | عالية جدا | الأهمية |
|---------|--------------|-------|--------|-------|--------------|---|
| 1.4 | 75.3% | 13.4% | 6.2% | 3.1% | 2.1% | الإدخال غير المقصود للبينات الخاطئة عن طريق المستخدمين |
| 3.5 | 6.2% | 14.4% | 21.6% | 34% | 23.7% | الإدخال المتعمد للبيانات الخاطئة عن طريق المستخدمين |
| 2.98 | 7.2% | 22.7% | 34% | 30.9% | 4.1% | الإتلاف غير المقصود للبينات من قبل المستخدمين |
| 2.06 | 39.2% | 24.7% | 28.9% | 5.2% | 2.1% | الإتلاف المتعمد للبيانات عن طريق المستخدمين |
| 1.29 | 72.2% | 9.3% | 7.2% | 4.1% | 0 | الدخول غير المصرح به للبينات أو النظام عن طريق المستخدمين |
| 1.04 | 96.6% | 2.1% | 1% | 0 | 0 | الدخول غير المصرح به للبينات أو النظام عن طريق الدخلاء (القرصنة) |
| 2.7 | 12.4% | 36.1% | 28.9% | 13.4% | 9.3% | إشتراك العاملين في كلمات الدخول للحاسوب |
| 1 | 100% | 0 | 0 | 0 | 0 | أثر الكوارث الطبيعية |
| 3.03 | 4.1% | 32% | 32% | 20.6% | 11.3% | أثر انقطاع التيار الكهربائي |

د. عصام البحيصي

| | | | | | | |
|------|-------|-------|-------|-------|------|--|
| 2 | 41.2% | 28.9% | 19.6% | 10.3% | 0 | أثر الكوارث من صنع الإنسان |
| 2 | 48.5% | 16.5% | 16.5% | 13.4% | 3.1% | دخول الفيروسات إلى الأنظمة |
| 1.1 | 95% | 1% | 3% | 1% | 0 | كبت و تخريب المخرجات |
| 1.1 | 90.7% | 7.2% | 2.1% | 0 | 0 | سرقة البيانات و المعلومات |
| 1.05 | 96% | 3% | 1% | 0 | 0 | النسخ غير المصرح به للمخرجات |
| 1.3 | 78.4% | 11.3% | 9.3% | 1% | 0 | رؤية الوثائق غير المصرح بها |
| 1 | 100% | 0 | 0 | 0 | 0 | طبع وتوزيع البيانات و المعلومات غير المصرح به |
| 1 | 99% | 1% | 0 | 0 | 0 | تخصيص المطبوعات و توزيع المعلومات على أشخاص غير مؤهلين لاستلامها |
| 1 | 99% | 1% | 0 | 0 | 0 | تسليم المستندات أو الوثائق الحساسة لموظف غير مضمون (مؤتمن) ليمزقها |
| 1.2 | 88.7% | 5.2% | 4.1% | 2.1% | 0 | حصر أو وقف تحويلات البيانات |

ملاحظة: تم استخدام مقياس ليكرت الخماسي في التحليل بحيث تكون الدرجة القصوى 5 و الدرجة الدنيا 1 و المتوسط 3

استكشاف المخاطر التي تهدد نظم المعلومات المحاسبية المحوسبة

1- الإدخال غير المقصود للبيانات الخاطئة عن طريق المستخدمين:

توضح النتائج أن هذا العنصر موجود في أغلب الشركات التي تكون مفردات العينة (95.9%)، إلا أن درجة تكرار هذا العنصر غير عالية حيث تتركز أغلب التكرارات ما بين مرة واحدة سنوياً أو شهرياً. وقد حصل هذا البند على درجة أهمية منخفضة بلغت في المتوسط (1.41)، وربما كان ذلك مرده إلى أن الخطأ يكتشف ويصحح على الفور في التقارير الحسابية النهائية أو النصف سنوية .

2- الإدخال المتعمد للبيانات الخاطئة عن طريق المستخدمين:

من نتائج الإجابة المتعلقة بهذا العنصر والمعروضة بالجدول رقم (4) يتضح أن هذه المشكلة لا تتكرر بشكل كبير في الشركات الفلسطينية. فهي لا تحدث مطلقاً لدى نسبة كبيرة (49.5%) من الشركات التي مثلت مفردات العينة. أما في الشركات التي تحدث فيها، فيتكرر حدوث هذه المشكلة ما بين مرة على الأقل سنوياً و مرة على الأقل شهرياً. و لكن من حيث الأهمية، وكما يظهر في جدول رقم (5)، تعتبر هذه المشكلة من أهم المشكلات التي تواجه الشركات الفلسطينية حيث حصلت على متوسط (3.54).

3- الإتلاف غير المقصود للبيانات من قبل المستخدمين:

كما يظهر في الجدول رقم (4)، فقد لوحظ أن درجة تكرار هذا الخطر غير مرتفعة، حيث كانت أكبر درجة تكرار (43.3%) هي مرة واحدة على الأقل سنوياً. وتراوحت باقي التكرارات ما بين مرة واحدة على الأقل شهرياً أو أسبوعياً. أما بشكل يومي فهو لا يتكرر في أي شركة من مفردات عينة البحث. أما من حيث الأهمية فإن النتائج الظاهرة بالجدول رقم (5) تبين أن هذا الخطر يعتبر متوسط الأهمية لدى الشركات الفلسطينية، حيث بلغ متوسط أهميته (2.98).

4- الإتلاف المتعمد للبيانات عن طريق المستخدمين:

إن الخطر الكامن في الإتلاف المتعمد للبيانات هو أمر غير متكرر نسبياً في الشركات الفلسطينية، حيث أشار أكثر من 78% إلى أن هذا الأمر لا يحدث لديه، في حين أشار الباقي بحدوثه بشكل سنوي ضعيف التكرار (جدول رقم 4). وربما كان الطابع العائلي للشركات الفلسطينية ذا أهمية في عدم تكرار هذا العمل، حيث أن المعرفة الشخصية و العلاقات العائلية تلعب دوراً هاماً في تعيين الموظفين في هذه الشركات. أما من حيث الأهمية، فإن هذا الخطر وكما يتضح من الجدول رقم (5) يعتبر متوسط الأهمية حيث حصل على متوسط قدره (2.06).

5- الدخول غير المصرح به للبيانات أو النظام عن طريق المستخدمين :

كما توضح لنا النتائج الظاهرة في جدول رقم (4) فإن خطر الدخول غير المصرح به عن طريق المستخدمين هو خطر نادر الحدوث، ولا يتكرر بدورية مرتفعة في الشركات الفلسطينية . إضافة إلى ذلك فإنه خطر قليل الأهمية حيث حصل على متوسط قدره 1.29 فقط(جدول رقم 5). ولعل مرجع هذا الأمر هو أن جميع برامج المحاسبة الموجودة و المتداولة في السوق الفلسطيني تقوم بتقسيم صلاحيات الوصول إلى المعلومات بين أكثر من مستوى إداري، الأمر الذي يجعل الدخول إلى النظام والوصول إلى هذه المعلومات بالأمر غير السهل لمن لا يملك مثل هذه الصلاحيات

6- الدخول غير المصرح به للبيانات أو النظام عن طريق الدخلاء (القراصنة):

كما يظهر في جدول رقم (4) يعتبر خطر الدخول غير المصرح به للبيانات أو النظام عن طريق الدخلاء (القراصنة) أحد الإخطار نادرة الحدوث في الشركات الفلسطينية. فقد أفاد حوالي 97% أن هذا الأمر لا يحدث لديهم، في حين أفاد الباقي بأن حدوثه يتكرر بشكل ضعيف (مرة سنوياً). من ناحية أخرى يتضح لنا أن درجة أهمية هذا الخطر هي ضعيفة، حيث لم يحصل إلا على متوسط قدره 1.03(جدول رقم 5). وربما كان احد العوامل الأساسية لندرة تكرار هذا الخطر في الشركات الفلسطينية هو كون قلة قليلة من هذه الشركات مرتبطة بشبكة الإنترنت كما يتضح من جدول رقم (2).

7- إشتراك العاملين في كلمات الدخول للحاسوب :

كما يتضح من الجدول رقم (4) فإن خطر إشتراك العاملين في كلمات الدخول للحاسوب هو من المخاطر التي تتكرر بشكل ملحوظ في الشركات الفلسطينية. فقد أفاد حوالي 62% من الشركات محل البحث بحدوث مثل هذا الأمر لديهم و إن كانوا اختلفوا في درجة تكرار حدوثه. كما أن أهمية هذا الخطر تعتبر أهمية متوسطة، حيث حصل هذا البند على متوسط قدره 2.7 (جدول رقم 5). وربما كانت الصفة العائلية المسيطرة على الشركات الفلسطينية ذات أثر ملحوظ في هذا الموضوع، حيث يتعرف الكثير من الموظفين على كلمات الدخول للحاسوب بصفتهم العائلية والشخصية وليس بصفتهم الوظيفية.

8- الكوارث الطبيعية :

قد تتسبب أحيانا الكوارث الطبيعية (الفيضانات، الرياح، العواصف، الرعد ، البرق و الزلازل) بتخريب كامل أو جزئي لنظم المعلومات. ولمعرفة أثر هذه الكوارث على نظم المعلومات المحاسبية في فلسطين فقد طلب من المشاركين توضيح مدى تكرار حدوثها داخل شركاتهم و كذلك تحديد أهميتها من وجهة نظرهم. ملخص الآراء حول هذا الموضوع يوضحه الجدول رقم

استكشاف المخاطر التي تهدد نظم المعلومات المحاسبية المحوسبة

(4). كما يتضح من الجدول فان الكوارث الطبيعية هي أمر نادر الحدوث بالنسبة للشركات الفلسطينية. فقد أكد حوالي 98% على عدم حدوث ذلك بالنسبة لشركاتهم، في حين أشار الباقي (فقط 2.1%) إلى حدوثها بشكل قليل التكرار (مرة سنوياً على الأقل). من ناحية أخرى فان الجدول رقم (5) يوضح و بشكل صريح الأهمية الضعيفة جداً لهذا العامل كمصدر محتمل للخطر على نظم المعلومات المحاسبية، حيث بلغ متوسطه الحسابي (1) فقط وهي أضعف النسب.

9- انقطاع التيار الكهربائي:

أظهرت النتائج (جدول رقم 4) أن جميع شركات مفردات العينة تعاني من مشكلة انقطاع التيار الكهربائي، و لكنها تختلف في درجة تكرار تلك المعاناة. وقد تركزت درجة تكرار هذا الحدث ما بين مرة على الأقل أسبوعياً (36.1%) إلى شهرياً (29.9%). إضافة إلى ارتفاع درجة التكرار فان أهمية هذا العامل تعتبر متوسطة، حيث حصل العامل على متوسط حسابي قدره 3.03 (جدول رقم 5). و تعتبر هذه النتيجة منطقية في ضوء ظاهرة الانقطاع المتكرر للتيار الكهربائي في الأراضي الفلسطينية و التي تنجم عن العديد من الأسباب منها ما هو متعلق بظروف الإحتلال أو بالقدرات المحدودة لشبكات الطاقة الكهربائية المحلية والتي تؤدي إلى قطع التيار الكهربائي دون سابق إنذار في اغلب الأحوال.

10- كوارث من صنع الإنسان:

نقصد هنا بالكوارث التي يحدثها الإنسان الحرائق ، الانفجارات. الحرائق التي قد تحدث نتيجة لأعمال الإنسان غير مقصودة و المقصودة مثل " النصب ، الاحتيال ، الاختلاس ، والسرقة. و الانفجارات سواء كان مصدرها المواطن الفلسطيني أو قصف قوات الاحتلال الإسرائيلي، وللتحقق حول حدوث هذه الكوارث فقد طلب من المشتركين تحديد حدوثها في شركاتهم. كما يتضح من الجدول رقم (4) فان الكوارث التي يتسبب بها الإنسان هي أمر موجود في الشركات الفلسطينية، إلا أن درجة تكراره محدودة نسبياً. فقد أشارت الأغلبية (52.6%) إلى عدم تأثرها بمثل هذا الحدث، في حين تركزت أغلب الإجابات التي أفادت بحدوث هذا الأمر (41.2%) حول تكرار حدوثه مرة واحدة في السنة على الأقل. في حين كانت قلة فقط (6.2%) من الشركات التي أكدت حدوث هذا الأمر مرة واحدة شهرياً على الأقل. و في رأي الباحث أن الأمر الذي يتكرر لدى الشركات الفلسطينية هو تعرضها لأضرار ناتجة عن القصف الإسرائيلي بشكل أكبر بكثير من حدوث أضرار أو أحداث مفتعلة. من ناحية أخرى فان النتائج أيضاً تظهر أن هذا العامل يعتبر من العوامل ذات الأهمية الضعيفة نسبياً في تأثيرها على نظم المعلومات المحاسبية في الشركات الفلسطينية حيث حصل على متوسط حسابي قدره 2 فقط (جدول رقم 5).

11- دخول الفيروسات إلى الأنظمة:

يلاحظ من الجدول رقم (4) أن دخول الفيروسات لأنظمة المعلومات هو خطر متكرر نسبياً في الشركات الفلسطينية، حيث لوحظ وجوده لدى حوالي 65% من مفردات العينة. إلا أن أهمية هذا الخطر غير مرتفعة، فقد بلغ المتوسط الحسابي لأهمية هذا الخطر رقم 2 الذي يرمز إلى درجة أهمية ضعيفة (جدول رقم 5). وربما كان السبب وراء ضعف أهمية هذا الخطر هو عدم ارتباط أغلبية الشركات الفلسطينية بشبكة الانترنت الأمر الذي لا يساهم في دخول الفيروسات الحديثة دائماً. إضافة إلى أن أغلب الشركات لديها برامج مضادة للفيروسات.

12- كبت وتخريب المخرجات :

كما يتضح من النتائج الظاهرة بالجدول رقم (4) فإن كبت وتخريب المخرجات يعتبر خطر نادر الحدوث في الشركات الفلسطينية، فقد أفادت أغلبية تقارب 95% من مفردات العينة بعدم وجود هذا الخطر لديهم، في حين أشار الباقي إلى تكراره بنسبة مرة واحدة سنوياً على الأقل. إضافة إلى أهميته المتواضعة جداً، فلم يتجاوز متوسطه الحسابي رقم 1.1 جدول رقم (5). وربما كان ذلك عائداً إلى أن أغلب الشركات الفلسطينية هي ذات طابع عائلي والتوظيف فيها يكون بالمعرفة الشخصية في أغلب الحالات، وبالتالي فإن الموظف ونتيجة لهذه العلاقة الشخصية لا يقدم على ارتكاب هذا الأمر وخاصة أن هذا الخطر لا يتم إلا بشكل متعمد.

13- سرقة البيانات والمعلومات:

كما يظهر من النتائج الظاهرة في الجدول رقم (4)، فإن سرقة البيانات والمعلومات هي خطر لا يكاد يحدث في المنشآت الفلسطينية. فقد أفاد 92% من مفردات العينة بعدم حدوث هذا الأمر لديهم ، أما الباقي فقد أفادوا بوجوده ويتكرر حدوثه مرة واحدة فقط سنوياً. أما من حيث الأهمية، فإن هذا الخطر يعتبر ذا أهمية ضعيفة جداً فلا يكاد يتجاوز متوسطه الحسابي الواحد الصحيح (جدول رقم 5). ولعل هذا الأمر أيضاً يرجع إلى عائلية الشركات ودور العلاقات الشخصية في مجتمع وبيئة الأعمال الفلسطينية من ناحية، وإلى عدم ربط أغلبية تلك الشركات بشبكة الإنترنت، الأمر الذي يحول دون عمليات السرقة عبر الشبكة.

14- النسخ غير المصرح به للمخرجات:

أما من حيث النسخ غير المصرح به للمخرجات فإن هذا الأمر يعتبر من أندر المخاطر حدوثاً في بيئة الشركات الفلسطينية. فهذا الخطر لا يوجد إلا لدى 4% من مفردات عينة البحث، ولا يتكرر لديها إلا مرة واحدة سنوياً (جدول رقم 4). ويعتبر أيضاً من أقل المخاطر أهمية من حيث التأثير على تلك الشركات، فقد بلغ متوسطه الحسابي 1.05 فقط (جدول رقم 5). وفي تفسيرنا لذلك،

استكشاف المخاطر التي تهدد نظم المعلومات المحاسبية المحوسبة

فإننا نعتقد أن خاصية عائلية الشركات والعلاقات الشخصية التي تحكم عمليات التوظيف في بيئة الأعمال الفلسطينية تلعب دوراً بارزاً في التخفيف من حدة وأهمية هذا الخطر.

15- رؤية الوثائق غير المصرح بها:

حسب ما يعرضه الجدول (18) فإن رؤية الوثائق غير المصرح بها هو خطر موجود في بيئة الأعمال الفلسطينية، حيث أفاد ما يزيد على 22% من مفردات العينة بحدوث هذا الخطر في شركاتهم. وتتراوح دورية تكرار حدوث هذا الخطر من مرة واحدة أسبوعياً حتى مرة واحدة على الأقل سنوياً. ألا أنه وعلى الرغم من ذلك فإن هذا الخطر يعتبر ضعيف الأهمية، فلم يزيد متوسطه الحسابي عن 1.3.

16- طبع وتوزيع البيانات والمعلومات غير المصرح به:

أما طبع وتوزيع البيانات والمعلومات غير المصرح بها، فإنه الخطر الوحيد الذي لا يحدث في بيئة الأعمال الفلسطينية. فقد أفاد جميع مفردات العينة بعدم حدوث هذا الخطر في شركاتهم. وأيضاً هنا فإننا نعتقد بأن خاصية عائلية الشركات والعلاقات الشخصية التي تحكم عمليات التوظيف في بيئة الأعمال الفلسطينية تلعب دوراً بارزاً في التخفيف من حدة وأهمية هذا الخطر.

17- تخصيص المطبوعات وتوزيع المعلومات على أشخاص غير مؤهلين لاستلامها:

أما فيما يتعلق بتخصيص المطبوعات وتوزيع المعلومات على أشخاص غير مؤهلين لاستلامها، فإن النتائج المدرجة بالجدول رقم (4) توضح بما لا يدع مجالاً للشك بان هذا الخطر هو من أقل المخاطر حدوثاً في بيئة الأعمال الفلسطينية. فلم يفد إلا 1% فقط من مفردات العينة بوجود هذا الخطر وبدورية تكراره مرة واحدة سنوياً. من ناحية أخرى فإن هذا الخطر يكاد يكون عديم الأهمية أيضاً.

18- تسليم المستندات أو الوثائق الحساسة لموظف غير مضمون (مؤتمن) ليمزقها:

الجدول رقم (4 و5) توضح أن خطر تسليم المستندات أو الوثائق الحساسة لموظف غير مضمون (غير مؤتمن) ليمزقها ينطبق عليه نفس ما ينطبق على خطر تخصيص المطبوعات وتوزيع المعلومات على أشخاص غير مؤهلين لاستلامها سواء من حيث عدم الحدوث تقريباً أو من حيث ضعف درجة الأهمية.

19- حصر أو وقف تحويلات البيانات:

أما فيما يتعلق بحصر أو وقف تحويلات البيانات، فالنتائج الظاهرة بالجدول رقم (4 و5) تظهر أن هذا الخطر موجود لدى جزء بسيط من مفردات العينة وبنسبة تكرار تختلف من شركة إلى أخرى، ولكن تتركز أغلبها في مرة واحدة سنوياً أو شهرياً. فلم تتجاوز نسبة الشركات التي

د. عصام البحيسي

أقرت بوجود هذا الخطر لديها نسبة 12.4% إلا قليلاً. إضافة إلى ذلك فإن نسبة أهمية هذا الخطر ضعيفة جداً ولم يتجاوز متوسطه الحسابي 1.2.

ثالثاً: اختبار فرضيات الدراسة

1- الفرضية الأولى

لا توجد مخاطر تهدد نظم المعلومات المحاسبية المحوسبة المستخدمة في الشركات الفلسطينية. الجداول السابقة (رقم 4 ، 5) تفيد بما لا يدع مجال للشك أن هناك مخاطر عديدة ومتنوعة تهدد نظم المعلومات المحاسبية المحوسبة المستخدمة في الشركات الفلسطينية، حيث توضح هذه الجداول وجود مثل هذه المخاطر وبدرجات تكرر متفاوتة وكذلك درجات أهمية متفاوتة. كما يتضح من هذه الجداول أن الإدخال المتعمد للبيانات الخاطئة عن طريق المستخدمين وانقطاع التيار الكهربائي والإتلاف غير المقصود للبيانات من قبل المستخدمين واشتراك العاملين في كلمات الدخول للحاسوب والكوارث من صنع الإنسان ودخول الفيروسات إلى الأنظمة هي أهم تلك المخاطر. الأمر الذي يعني رفض الفرضية الأولى، الفائلة بأنه لا توجد مخاطر تهدد نظم المعلومات المحاسبية المحوسبة المستخدمة في الشركات الفلسطينية.

2- الفرضية الثانية

لا توجد فروقات هامة بين مختلف المؤسسات الفلسطينية فيما يتعلق بأهمية التهديدات التي تواجه نظم المعلومات المحاسبية. من أجل إختبار مدى صحة هذه الفرضية تم إجراء أختبار مربع كاي لمعرفة درجة الترابط بين نوع المؤسسة وبين أهمية المخاطر التي تتعرض لها المؤسسات. وقد أظهرت نتيجة الاختبار عدم وجود أي علاقة ذات دلالة إحصائية عند مستوى (0.05) بين المتغيرين مما يعني قبول الفرضية¹.

3- الفرضية الثالثة

توجد علاقة بين نوع النظام المستخدم ونوع الأخطار الموجودة ودرجة تكرارها وأهميتها. من أجل اختبار هذه الفرضية تم إجراء مربع كاي بين نوع النظام المستخدم (حاسوب شخصي أو سيرفر مع شبكة) ومدى ارتباط الشركة بشبكة الانترنت من ناحية ودرجة تكرار وأهمية كل واحد

¹ لم يضع الباحث نتائج تحليل مربع كاي نتيجة عدم وجود علاقة بين أي من المخاطر والعامل محل البحث و اكتفى فقط بالإشارة إلى النتيجة الإجمالية

استكشاف المخاطر التي تهدد نظم المعلومات المحاسبية المحوسبة

من المخاطر التي تمت دراستها، وقد تبين لنا وجود علاقة ذات دلالة إحصائية عند مستوى (0.05) بين نوع النظام المستخدم (حاسوب شخصي أو سيرفر) ودرجة تكرار واهمية المخاطر التالية:

- 1- اشتراك العاملين في كلمات الدخول للحاسوب
 - 2- الإلتلاف غير مقصود للبيانات من قبل المستخدمين
 - 3- رؤية الوثائق غير المصرح بها
- الجدول رقم (6)² يعرض العلاقة بين المتغير التابع (نوع النظام) و التغيرات المستقلة (المخاطر) التي وجد أنها ترتبط بعلاقة ذات دلالة إحصائية مع المتغير التابع.

جدول رقم (6)

تحليل مربع كاي لدرجة تكرار و أهمية المخاطر المذكورة مع نوع النظام المستخدم

| الأهمية | | درجة التكرار | | العوامل |
|---------|-------|--------------|-------|---|
| Sig | | Sig | | |
| 0.001 | 0.988 | 0.000 | 1.345 | اشتراك العاملين في كلمات الدخول للحاسوب |
| 0.000 | 1.305 | 0.000 | 1.271 | الإلتلاف غير المقصود للبيانات من قبل المستخدمين |
| 0.000 | 1.977 | 0.000 | 2.113 | رؤية الوثائق غير المصرح بها |

وبعد إجراء إختبار التكرار المتقاطع (cross tabulation) اتضح أن هذه المخاطر تزداد بشكل واضح في المنشآت التي تستخدم نظام الشبكات والسيرفر عن تلك التي تستخدم أجهزة حاسوب منفصلة. وتعتبر هذه النتائج أساسا يستند عليه في قبول الفرضية الثالثة.

جدول رقم (7)

تحليل التكرار المتقاطع للمخاطر ذات العلاقة مع نوع النظام المستخدم

| نوع النظام | | المخاطر |
|------------|---------------|---|
| حاسوب شخصي | سيرفر مع شبكة | |
| 23% | 77% | اشتراك العاملين في كلمات الدخول للحاسوب |
| 34% | 68% | الإلتلاف غير المقصود للبيانات من قبل المستخدمين |
| 19% | 81% | رؤية الوثائق غير المصرح بها |

² اقتصر الجدول على المخاطر التي أظهر التحليل بأنها ذات علاقة معنوية فقط دون باقي المخاطر.

د. عصام البحيصي

5- الفرضية الرابعة

توجد علاقة بين مدى الاتصال بشبكة الانترنت ونوع الأخطار الموجودة ودرجة تكرارها وأهميتها.

من أجل اختبار هذه الفرضية تم إجراء مربع كاي بين مدى إرتباط الشركة بشبكة الإنترنت من ناحية ودرجة تكرار وأهمية كل واحد من المخاطر التي تمت دراستها، وقد تبين لنا وجود علاقة ذات دلالة إحصائية عند مستوى (0.05) بين ربط الشركة بشبكة الانترنت وخطر دخول الفيروسات إلى الأنظمة³ فقط. وقد بين اختبار الجداول المتقاطعة (cross tabulation) أن هذا الخطر يزداد بشكل كبير في الشركات المرتبطة بشبكة الانترنت. أما خطر الدخول غير المصرح به للبيانات النظام عن طريق الدخلاء (القرصنة) فهو خطر لا يوجد إلا في الشركات التي ترتبط بشبكة الانترنت. وعليه فإننا نقبل الفرضية الرابعة.

جدول رقم (8)

تحليل مربع كاي لخطر دخول الفيروسات مع خاصية الاتصال بشبكة الانترنت

| الاهمية | | درجة التكرار | | دخول الفيروسات إلى الأنظمة |
|---------|-------|--------------|-------|----------------------------|
| Sig. | | Sig. | | |
| 0.000 | 1.041 | 0.000 | 1.162 | |

جدول رقم (9)

تحليل التكرار المتقاطع لخطر دخول الفيروسات مع خاصية الاتصال بشبكة الانترنت

| الاتصال بشبكة الانترنت | | العوامل |
|------------------------|------|----------------------------|
| غير متصل | متصل | دخول الفيروسات إلى الأنظمة |
| 37% | 63% | |

³ اقتصر الجدول على الخطر الذي اظهر التحليل بأنه ذا علاقة مع المتغير التابع، دون باقي العوامل و التي لم تظهر لها علاقة بهذا المتغير

استكشاف المخاطر التي تهدد نظم المعلومات المحاسبية المحوسبة

6- الفرضية الخامسة

لا توجد علاقة ذات دلالة احصائية بين حجم رأس مال الشركة وبين درجة تكرارها الأخطار الموجودة وأهميتها.

وقد أظهر تحليل الترابط (correlation) عند مستوى (0.05) عدم وجود علاقة ذات دلالة إحصائية بين حجم رأس المال و درجة تكرار و أهمية كل واحد من المخاطر محل البحث، مما يعني قبول الفرضية المذكورة⁴.

الخاتمة والتوصيات :

إن هدف هذه الورقة هو للتعرف على أهم المخاطر التي تهدد أمن نظم المعلومات المحاسبية المحوسبة من خلال تكرار حدوثها في الشركات الفلسطينية ، لقد طورت هذه الدراسة بناءً على دراسات سابقة عن طريق (لوك , آخرين 1992 ، هنري 1997 ، ودافيز 1996، أبو موسى 2001، 2006) وأظهرت النتائج أن من أهم المخاطر التي تواجه النظام في الشركات الفلسطينية هي:

1- الإدخال المتعمد للبيانات الخاطئة عن طريق المستخدمين

2- انقطاع التيار الكهربائي

3- الإلتلاف غير المقصود للبيانات من قبل المستخدمين

4- اشتراك العاملين في كلمات الدخول للحاسوب

5- الكوارث من صنع الإنسان

6- دخول الفيروسات إلى الأنظمة

أما باقي المخاطر التي تمت دراستها فهي وإن وجدت، فهي ذات أهمية ضعيفة في بيئة الأعمال الفلسطينية.

من ناحية أخرى فقد تبين لنا أن الشركات الفلسطينية تختلف فيما بينها في درجة تكرار وأهمية المخاطر حسب نوعية نظام المعلومات المستخدم وحسب مدى الارتباط بشبكة الانترنت. إلا أنه ليس هناك ارتباط بين نوع المؤسسة (القطاع الذي تنتمي إليه المؤسسة) ودرجة تكرار وأهمية المخاطر التي تتعرض لها الشركات الفلسطينية و هذا يتفق مع دراسة أبو موسى 2006. من جانب آخر فقد أظهرت نتائج البحث وبعد مقارنتها بنتائج الدراسات السابقة، أن الأخطار التي

⁴ لم يضع الباحث نتائج تحليل الترابط نتيجة عدم وجود علاقة بين اي من المخاطر و العامل محل البحث و اكتفى فقط بالإشارة الى النتيجة الاجمالية

د. عصام البحيصي

تتعرض لها الشركات الفلسطينية هي شبيهة إلى حد كبير بالأخطار التي تتعرض لها الشركات في الدول الأخرى، وخاصة النامية منها. ولعل التوصية الأكثر أهمية هنا هي ضرورة زيادة الاهتمام بأمن المعلومات خاصة لدى الشركات التي تستخدم نظام الشبكات والتي ترتبط بشبكة الانترنت. إضافة إلى ذلك فإن الباحث يوصي بضرورة:

- 1- تطوير أداء العاملين فيما يتعلق بنظم المعلومات المحاسبية المحوسبة وطرق التعامل معها، وذلك عبر توفير دورات تدريبية لهم في هذا المجال.
- 2- رقابة أداء العاملين ذوي العلاقة المباشرة مع البيانات وذلك لضمان عدم إدخال متعمد للبيانات الخاطئة أو إتلاف غير مقصود للبيانات السليمة.
- 3- على ضرورة التزام العاملين ذوي العلاقة بالبيانات بعدم إعطاء كلمات المرور الخاصة بهم لآخرين، وذلك لضمان عدم استخدامها في أمور تزيد من حدة بعض المخاطر التي تتعرض لها الشركات.

المراجع

المراجع العربية

1. البحيصي، عصام و الشريف، حرية. مخاطر نظم المعلومات المحاسبية الالكترونية: دراسة تطبيقية على المصارف الفلسطينية. *مجلة الجامعة الإسلامية - العلوم الانسانية* - 16(2)، 2008، 895-924.

المراجع الأجنبية

2. Abu Mousa, Ahmed. Evaluating the security of computerized accounting information system: An empirical study of Egyptian banks industry. Ph.D thesis, **University of Aberdeen**. U.K. 2001.
3. Abu Mousa, Ahmed. Investigating the perceived threats of computerized accounting information systems in developing countries: An empirical study on Saudi organizations. **King Fahd University Journal**, Computer and Information Science, 2006, 18, 1-26.
4. Davis, Ch. E. An assessment of accounting information system security. **The CPA Journal**, 1997, 67 (3), 38-34.
5. Dhillon, G. Managing and controlling computer misuse. **Information Management and Computer Security**, 1999. 7 (4), 71-175.
6. Henry. L. A study of the nature and security of accounting information system: The case of Hampton Roads, Virginia. **The Mid-Atlantic Journal of Business**, 1997, 33 (63), 171-189.

استكشاف المخاطر التي تهدد نظم المعلومات المحاسبية المحوسبة

7. Hunton, J.; A. Wright; and S. Wright. Business and Audit Risks Associated With ERP Systems: Knowledge Differences between Information Systems Audit Specialists and Financial Auditors. **Journal of Information Systems**, 2005, Forthcoming.
8. Loch, K.; Houston, H. C.; and Merrill, E. W. Threats to information system: Today's reality and yesterday's understanding. **MIS Quarterly**, 1992, June, 173-186.
9. Riner, K. R.; Snyder, Ch. A. ; and Houston , H. C. Risk analysis for information technology. **Management Information System**, 1991. 8 (1), 129.147.
10. Ryan. S. D. and Bordoloi. B. Evaluating security threats in mainframe client /server environment". **Information and Management**, 1997, 32, (3), 137-142.
11. Siponen, M. T. " A conceptual foundation for organizational information security awareness" **Information Management and Computer Security**, 2000, 8 (8), 31-44.
12. Warren, M. J. Security practice: survey evidence from three countries, **Logistics Information Management**, 2002,15 (5/6), 347-351.

ملحق رقم (1)

الاستبيان

الأخ الفاضل:

الإستبيان المرفق يشكل مصدر معلومات لبحثنا الموسوم " المخاطر التي تهدد نظم المعلومات المحاسبية المحوسبة في الدول النامية - دراسة تطبيقية على الشركات الفلسطينية". والبحث يهدف إلى التحقق من وجود ودرجة أهمية هذه المخاطر في بيئة الشركات الفلسطينية ، سوف أكون ممتناً لكم إذا أكملت هذا الإستبيان، علماً بان المعلومات التي تجمع من خلال هذا الإستبيان هي بيانات سرية وسوف تستخدم لأغراض البحث العلمي فقط لا غير. إجاباتك هي مساهمة مشكورة في دعم البحث العلمي في بلدنا. جزاكم الله كل خير

ملاحظة:

يرجى أن يعبئ الاستبانة احد الأشخاص التالية مسمياتهم الوظيفية (محاسب، رئيس قسم حسابات، مدير مالي أو مدير عام)

أخوكم د. عصام البحيصي

قسم المحاسبة كلية التجارة

الجامعة الإسلامية بغزة

د. عصام البحيصي

الرجاء وضع علامة (X) أمام العيارة التي تختارها

القسم الأول: معلومات مهنية

1- مؤسستكم تتبع القطاع:

| | | | | | |
|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|
| صناعي | تجاري | خدمات | بناء و مقاولات | البنوك | التأمين |
| <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |

2- يبلغ رأس مال شركتكم:

| | |
|---------------------|--|
| أقل من \$10000 | |
| \$ 100000 - 10000 | |
| \$ 1000000 - 100000 | |
| أكثر من \$ 1000000 | |

3- الوظيفة الحالية

| | |
|-----------------|--|
| مدير عام | |
| مدير مالي | |
| رئيس قسم حسابات | |
| محاسب | |
| أخرى | |

4- سنوات الخبرة

| | | | | |
|----------------|--------------|-------------|-------------|----------------|
| أقل من 5 سنوات | 5 - 10 سنوات | 11 - 20 سنة | 21 - 30 سنة | أكثر من 30 سنة |
| | | | | |

5- نوع الحاسوب المستخدم في العمل

| | |
|----------------------------|--|
| حاسوب شخصي PC | |
| حاسوب مرتبط بشبكة (Server) | |

6- ترتبط منشاتكم بشبكة الانترنت

| | |
|--------------------------|--------------------------|
| نعم | لا |
| <input type="checkbox"/> | <input type="checkbox"/> |

استكشاف المخاطر التي تهدد نظم المعلومات المحاسبية المحوسبة

القسم الثاني: تقييم للمخاطر التي يتعرض لها نظام المعلومات المحاسبية

الهدف الرئيسي من هذا القسم استكشاف المخاطر و التهديدات الأساسية التي تواجه فعلياً أمن النظام المحاسبي المحوسب في البنوك السعودية ومدى اتصالها المادي لكل تهديد على حد :

7-الرجاء تحديد تكرار كل تهديد حسب ما هو حادث في مؤسستكم :

| الرقم | التهديدات | مرة على الأقل في السنة | مرة على الأقل شهريا | مرة على الأقل أسبوعيا | مرة على الأقل يوميا | لا تحدث |
|-------|---|------------------------|---------------------|-----------------------|---------------------|---------|
| 1 | الإدخال غير المقصود وحضور للبيانات عن طريق العاملين | | | | | |
| 2 | الإدخال المعتمد للبيانات الخاطئة عن طريق العاملين | | | | | |
| 3 | الهلاك غير المقصود للبيانات عن طريق العاملين | | | | | |
| 4 | الهلاك المعتمد للبيانات عن طريق العاملين | | | | | |
| 5 | الدخول غير المصرح به للبيانات أو النظام | | | | | |
| 6 | الدخول غير المصرح به للبيانات عن طريق القرصنة | | | | | |
| 7 | اشتراك العاملين في كلمات الدخول | | | | | |
| 8 | الكوارث الطبيعية | | | | | |
| 9 | الكوارث من صنع الإنسان | | | | | |
| 10 | دخول فيروسات إلى النظام | | | | | |

د . عصام البجيصي

| | | | | | | |
|--|--|--|--|--|----|---|
| | | | | | 11 | كبت وهلاك المخرجات |
| | | | | | 12 | خلق الخيال /مخرجات غير صحيحة |
| | | | | | 13 | سرقة البيانات أو المعلومات |
| | | | | | 14 | النسخ غير المصرح به للمعلومات |
| | | | | | 15 | رؤية الوثائق غير المصرح بها عن طريق عرضها طبعتها |
| | | | | | 16 | طبوع وتوزيع المعلومات عن طريق شخص غير مضمون |
| | | | | | 17 | طبوع وتوزيع المعلومات الأشخاص غير مؤهلين لاستلامها |
| | | | | | 18 | وثائق مهمة وحساسة تسلم لشخص غير مضمون لتمزيقها |
| | | | | | 19 | حصر ووقف تحويل البيانات من بعيد . |

8- الرجاء تحديد أهمية المخاطر التالية بالنسبة لشركتكم

| درجة الأهمية | | | | | التهديدات | الرقم |
|------------------------|-----------------|--------------|-------------|--------------------|---|-------|
| أهمية منخفضة جدا | أهمية منخفضة | أهمية متوسطة | أهمية عالية | أهمية عالية جدا | | |
| | | | | | الإدخال غير المؤمن وحضور للبيانات عن طريق العاملين | 1 |

استكشاف المخاطر التي تهدد نظم المعلومات المحاسبية المحوسبة

| | | | | | | |
|--|--|--|--|--|---|----|
| | | | | | الإدخال المعتمد للبيانات الخاطئة عن طريق العاملين | 2 |
| | | | | | الهلاك غير المقصود للبيانات عن طريق العاملين | 3 |
| | | | | | الهلاك المعتمد للبيانات عن طريق العاملين | 4 |
| | | | | | الدخول غير المصرح به للبيانات أو النظام | 5 |
| | | | | | الدخول غير المصرح به للبيانات عن طريق القرصنة | 6 |
| | | | | | اشتراك العاملين في كلمات الدخول | 7 |
| | | | | | الكوارث الطبيعية | 8 |
| | | | | | الكوارث من صنع الإنسان | 9 |
| | | | | | دخول فيروسات إلى النظام | 10 |
| | | | | | كبت وهلاك المخرجات | 11 |
| | | | | | خلق الخيال /مخرجات غير صحيحة | 12 |
| | | | | | سرقة البيانات أو المعلومات | 13 |
| | | | | | النسخ غير المصرح به للمعلومات | 14 |
| | | | | | رؤية الوثائق غير المصرح بها عن طريق عرضها طبعها | 15 |
| | | | | | طبع وتوزيع المعلومات عن طريق شخص غير مضمون | 16 |
| | | | | | طبع وتوزيع المعلومات للأشخاص غير مؤهلين لاستلامها | 17 |
| | | | | | وثائق مهمة وحساسة تسلم لشخص غير مضمون لتمزيقها | 18 |
| | | | | | حصر ووقف تحويل البيانات من بعيد . | 19 |