



بحث أمن المعلومات والبيانات

بحث أمن المعلومات والبيانات



جامعة ميدأوشن

بكالوريوس إدارة المشاريع

د. منى مصطفى العشري

الطالب : ماجد عوض الحازمي

الرقم الجامعي : 2021202046

بحث أمن المعلومات والبيانات

ملخص البحث

يهدف هذا البحث إلى محاولة معرفة أثر إدارة أمن المعلومات على نجاح برنامج أمن المعلومات ، ولقد قدم البحث إطاراً نظرياً لأهم العوامل والمتغيرات التي تؤثر على فعالية إدارة أمن المعلومات وأثرها على نجاح برنامج أمن المعلومات ، وذلك باستخدام قائمة الاستقصاء التي تم تصميمها خصيصاً لهذا الغرض. ولقد تم تجميع البيانات اللازمه لاختبار الفروض الإحصائية باستخدام البرنامج الإحصائي SPSS، وعمل التحليل الإحصائي الوصفي وكذلك الاختبارات الإحصائية المعلمية لاختبار الفروض، وقد توصلت نتائج الدراسة إلي أن إدارة أمن المعلومات لها تأثير جوهري وإيجابي على نجاح برنامج أمن نظم المعلومات ، كما أوصت بضرورة اهتمام منظمات الأعمال بإدارة أمن المعلومات باعتبارها عنصراً هاماً وضرورياً لنجاح برنامج أمن المعلومات

1- الإطار العام للبحث

1/1 مقدمة

أدى تطور تكنولوجيا المعلومات والاتصالات إلى إحداث تطور كبير في مجال المعلومات الذي زامنه ظهور تهديدات كبيرة ومتنوعة تهدد أمن نظم المعلومات وسلامة المعلومات التي تتضمنها، ولضمان أمن المعلومات تقوم المنظمات عادة بإدخال سياسات ومبادئ توجيهية تتاح لجميع الأعضاء (Rotvold,) 2008، ومع ذلك لاتزال هناك تهديدات وحوادث أمنية ونقاط ضعف ومخاطر تعصف بالعديد من المنظمات لذلك أصبح أمن المعلومات واحداً من أهم التحديات التي تواجه المنظمات في الوقت الراهن، والتي تتطلب من إدارات المنظمات الإدارة الجيدة لأمن نظم المعلومات، والتي تعرف بأنها نهج أمني مستمر ومنظم لإدارة حماية معلومات المنظمة من التعرض للخطر من قبل الأطراف المسؤولة ولضمان بقاء المعلومات آمنة (Zammani & Razali, 2016).

وتختلف إدارة أمن المعلومات عن حوكمة أمن المعلومات حيث تهتم حوكمة أمن المعلومات بتأسيس بيئة رقابية مع ضمان توفير الحماية اللازمة للأصول المعلوماتية من المخاطر المختلفة، وكذلك وضع خطة للتطوير المستمر لإدارة المخاطر، وعلى الرغم من هذا الاختلاف فإن كلاهما يسعى لتخفيف المخاطر التي تواجه نظم المعلومات المحاسبية الإلكترونية.

بحث أمن المعلومات والبيانات

2/1 مشكلة البحث

أصبح حماية المعلومات في عصر العولمة أمراً بالغ الأهمية من أجل ضمان استمرارية الأعمال، حيث إن التصدي للتهديدات الأمنية لنظم المعلومات أصبح تحدياً يواجه العديد من المنظمات، فأمن المعلومات لا يعني تأمين المعلومة والحفاظ على سرية ونزاهة المعلومات وتوافرها فقط ولكن أيضاً تأمين البنية التحتية التي تسهل استخدامها من أجهزة وبرمجيات وعوامل بشرية ومادية.

واعتراحاً بذلك بذلت المنظمات جهوداً كبيرة في إدارة ومعالجة أمن المعلومات، وأصبح من الضروري عليها أن تهتم بوضع نظم وإجراءات تعمل على الحد من تلك المخاطر، ووضع نظام جيد لإدارتها والعمل على نجاح برنامجها الأمني.

وبذلك يمكن صياغة مشكلة البحث في السؤال البحثي التالي:

ما مدى تأثير إدارة أمن المعلومات على نجاح برنامج أمن نظم المعلومات ؟

ويمكن الإجابة على السؤال البحثي الرئيسي من خلال الإجابة على الأسئلة البحثية الفرعية التالية:

6. ما المقصود ببرنامج أمن المعلومات؟ وما الفرق بين إدارة أمن المعلومات وحوكمة أمن المعلومات؟

2. هل يؤثر التنفيذ المستمر للسياسات المتعلقة بأمن المعلومات على نجاح برنامج أمن نظم المعلومات ؟

3. هل يؤثر وجود إجراءات لتنفيذ عمليات وأنشطة سياسات أمن المعلومات على نجاح برنامج أمن نظم المعلومات ؟

4. هل يؤثر وجود فريق متخصص في إدارة أمن المعلومات على نجاح برنامج أمن نظم المعلومات ؟

5. هل يؤثر وجود فريق تنسيق لإدارة أمن المعلومات حيث التواصل بفعالية مع جميع المستويات بالمنظمة على نجاح برنامج أمن نظم المعلومات ؟

1. هل يؤثر وجود فريق مسئول عن ضمان ضوابط الرقابة على نجاح برنامج أمن نظم المعلومات ؟

1. هل يؤثر التقييم الجيد لإدارة أمن نظم المعلومات على نجاح برنامج أمن نظم المعلومات ؟

بحث أمن المعلومات والبيانات

3/1 هدف البحث

يتمثل الهدف الرئيسي للبحث في "دراسة مدى تأثير إدارة أمن المعلومات على نجاح برنامج أمن نظم المعلومات"

ويمكن تحقيق هذا الهدف من خلال تحقيق الأهداف الفرعية التالية:

1. تحديد المفاهيم الأساسية المرتبطة ببرنامج أمن المعلومات، ودراسة أوجه الاختلاف بين إدارة أمن المعلومات وحوكمة أمن المعلومات.
2. دراسة أثر التنفيذ المستمر للسياسات المتعلقة بأمن المعلومات على نجاح برنامج أمن نظم المعلومات.
3. دراسة أثر وجود إجراءات لتنفيذ عمليات وأنشطة سياسات أمن المعلومات على نجاح برنامج أمن نظم المعلومات.
4. دراسة أثر وجود فريق متخصص في إدارة أمن المعلومات على نجاح برنامج أمن نظم المعلومات.
5. دراسة أثر وجود فريق تنسيق لإدارة أمن المعلومات يعمل على التواصل بفعالية مع جميع المستويات بالمنظمة على نجاح برنامج أمن نظم المعلومات.
6. دراسة أثر وجود فريق مسئول عن ضمان ضوابط الرقابة على نجاح برنامج أمن نظم المعلومات.
7. دراسة أثر التقييم الجيد لإدارة أمن نظم المعلومات على نجاح برنامج أمن نظم المعلومات.

4/1 أهمية البحث

تتمثل أهمية البحث في الأهمية العلمية والعملية على النحو التالي:

1/4/1 الأهمية العلمية

تتمثل في محاولة إلقاء الضوء على تنوع وتعدد المخاطر التي تتعرض لها نظم المعلومات ، وكذلك توضيح المحاولات التي تقوم بها المنظمات للحد من تلك المخاطر عن طريق إدارة أمن المعلومات وحوكمة أمن المعلومات.

بحث أمن المعلومات والبيانات

2/4/1 الأهمية العملية

- قد يساعد البحث العاملين في مجال أمن نظم المعلومات في اتخاذ القرارات ووضع الخطط والبرامج والسياسات التي تعمل على التخفيف من حدة المخاطر التي تتعرض لها نظم المعلومات وأمن نظم المعلومات .
- يساعد البحث على الفهم الجيد لإدارة أمن برامج نظم المعلومات وكيفية تطبيقها وتنفيذها في منظمة الأعمال.

5/1 منهج البحث

اعتمد الباحثون على المنهج العلمي بشقيه الاستقرائي والاستنباطي، وذلك على النحو التالي:

1/5/1 المنهج الاستنباطي Deductive Approach

اعتمد الباحثون على المنهج الاستنباطي Deductive Approach لدراسة والتعرف على إدارة أمن المعلومات ودورها في نجاح برنامج أمن نظم المعلومات في منظمات الأعمال ، وفي إطار ذلك قام الباحثون بدراسة وتحليل الدراسات والمقالات والبحوث العلمية والعملية المختلفة التي لها صلة بموضوع البحث بهدف اشتقاق الفروض الإحصائية التي سيتم اختبارها في الدراسة الميدانية.

2/6/1 المنهج الاستقرائي Inductive Approach

اعتمد الباحثون على المنهج الاستقرائي Inductive Approach في إجراء الدراسة الميدانية للتعرف على مدى تأثير إدارة أمن المعلومات علي نجاح برنامج أمن نظم المعلومات ، واختبار الفروق الجوهرية بين الوظائف المختلفة فيما يختص بمدى إدراكها لأهمية إدارة أمن المعلومات في بيئة الأعمال عن طريق قائمة الاستقصاء Questionnaire التي أعدت خصيصاً لتحقيق هذا الغرض، وكذلك أسلوب المقابلات الشخصية لأفراد عينة البحث الميداني ثم اختبار فروض البحث والوصول إلى نتائج وتوصيات البحث.

7/1 حدود البحث

- يقتصر البحث على المخاطر التي تتعرض لها نظم المعلومات فقط دون الدخول في التفسيرات أو الدوافع من وراء ذلك.

بحث أمن المعلومات والبيانات

2- الإطار النظري للبحث

1/2 أمن نظم المعلومات والمخاطر التي تهدد المعلومات وأنظمتها

بدأ علم أمن المعلومات وتطور مع بداية تقنية المعلومات وتطورها، فعندما بدأت الحاسبات الآلية باحتواء معلومات مهمة بدأ القلق على أمن هذه المعلومات والأجهزة التي تعالجها. لذلك بدأ التفكير في تأمين المعلومات والأجهزة التي تحتويها ضد المخاطر المحتملة التي قد تتعرض لها. ومن هذا يجب توضيح الآتي:

1/1/2 مفهوم أمن المعلومات (IS) Information Security

Committee on National Security Systems ووضوح (Withman & Mattord) 2005 أمن المعلومات كما عرفته لجنة أنظمة الأمن القومي الأمريكية

(CNSS) بأنه "حماية المعلومات وعناصرها المهمة بما في ذلك الأنظمة والأجهزة التي تستخدم هذه المعلومات وتخزينها وترسلها."

2/1/2 متطلبات أمن المعلومات

إن حماية أمن المعلومات يتطلب نشر الوعي بين العاملين في المنظمة بالأخطار التي تهدد أمن المعلومات ومن هذه المتطلبات ما يلي:

يرى حامد مخاطر أمن نظم المعلومات بأنها جميع الممارسات البشرية والأحداث السياسية والتأثيرات البيئية المقصودة وغير المقصودة سواء كانت داخل المنظمة أو خارجها وينتج عنها إتلاف أو تدمير أو سرقة أو تزوير لبعض أو كل من نظم المعلومات متبوعة في كثير من الأحيان بتحقيق خسائر في الوقت والجهد والأموال.

وتتعرض نظم المعلومات للكثير من المخاطر والتهديدات ومنها التلاعب في البيانات بقصد تدميرها سواء بالحذف، أو بالدمج غير الصحيح لبعضها، أو بخلطها ببيانات أخرى غير حقيقية أو تبويبها بشكل خاطئ تفقد معه مدلولها ومعناها؛ وقد يحدث التلاعب في البيانات بشكل يجعلها لا تعبر عن الحقائق التي نتجت عنها أصلاً، كما أن هذا التلاعب يحدث في مراحل مختلفة من النظام حيث المدخلات أو التشغيل أو التخزين أو المخرجات. ومن الممكن أن تكون تلك التهديدات في شكل سرقة وقت أجهزة الكمبيوتر واستخدامه في الأغراض الشخصية والدخول غير المصرح به للنظم والشبكات وتخريب وتدمير بعض الملفات، فشل النظام وسقوط شبكة الاتصال، منع الأشخاص المخول لهم بالدخول إلى النظام، الكوارث الطبيعية مثل الحرائق والفيضانات أو انقطاع مصدر الطاقة، الكوارث غير الطبيعية مثل الحرائق المفتعلة وغيرها، إدخال فيروسات للكمبيوتر، الإظهار غير المرخص به للبيانات عن طريق عرضها على شاشات العرض أو طبعتها وتوزيعها بواسطة أشخاص غير مصرح لهم بذلك، وكذلك مقاطعة تحويل البيانات من أماكن بعيدة.

بحث أمن المعلومات والبيانات

إدخال فيروسات للكمبيوتر، الإظهار غير المرخص به للبيانات عن طريق عرضها على شاشات العرض أو طبعها وتوزيعها بواسطة أشخاص غير مصرح لهم بذلك، وكذلك مقاطعة تحويل البيانات من أماكن بعيدة.

2/2 إدارة أمن المعلومات (ISM) Information Security Management

إدارة أمن المعلومات هي نهج أمني مستمر ومنظم لإدارة حماية معلومات المنظمة من التعرض للخطر من قبل الأطراف غير المسؤولة ولضمان بقاء المعلومات آمنة (Zammani & Razali, 2016)، فغالباً ما يواجه أمن المعلومات بالعديد من المشاكل سواء في الأجل الطويل أو الأجل القصير، وقد تركز معظم منظمات الأعمال على منع حدوث مشاكل أمن المعلومات في الأجل القصير دون الاهتمام بمدى خطورة مشاكل الأجل الطويل. لذا يجب على الإدارة وضع خطة طويلة الأجل لمنع حدوث أي تهديد لأمن المعلومات في الأجل الطويل وتخفيض آثارها السلبية على المنظمة إلى أدنى حد ممكن في حالة حدوثها، كما يجب عليها تحديد نوع القضايا الهامة التي تواجه أمن المعلومات وأن تدرسها بعناية وتتفهم طبيعة المشاكل المتعلقة بكل قضية حتى تستطيع تجنب تلك المشاكل في المستقبل وتقديم حلول مناسبة لها .

ولإدارة أمن المعلومات مجموعة من المتغيرات الداخلية التي تعمل على نجاح برامج أمن نظم المعلومات وهذه المتغيرات هي:

1- سياسة أمن المعلومات IS Policy

سياسة أمن المعلومات هي مزيج من المبادئ والأنظمة والمنهجيات والتقنيات والأدوات التي أنشئت لحماية المنظمة من التهديدات (Tryfonas et al., 2001)، ويرى Alnatheer أنها وثيقة استراتيجية بمعنى أنها تنشأ قبل القيام بأي نشاط من أنشطة أمن المعلومات فهي تتكون من الأهداف والاتجاهات والقواعد التي يجب وضعها واتباعها من قبل الموظفين والأطراف الأخرى التي تتعامل مع المنظمة، لذا يجب أن تكون هذه السياسة واضحة في تحديد الأهداف والأدوار ومسؤوليات الموظفين والأطراف الأخرى ذات المصلحة، كما يجب أن تكون شاملة بمعنى أنها تغطي جميع جوانب متطلبات وضوابط أمن المعلومات وأن تكون متناسقة مع سياسة المنظمة ورؤيتها.

وتمثل سياسة أمن المعلومات حجر الزاوية في إدارة أمن المعلومات الجيدة (Fung et al., 2003)، كما أن هذه السياسة ليست ثابتة أي يجب أن يتم مراجعتها بانتظام على الأقل مرة واحدة في السنة للتأكد من أنها ذات صلة باحتياجات الوقت الحاضر ويتم إرسالها إلى كامل الموظفين والأطراف الأخرى ذات المصلحة مع مراعاة أنه عند قيام المنظمة بإحلال أساليب أمن تكنولوجية حديثة بدلاً من أساليب

بحث أمن المعلومات والبيانات

أمن المعلومات التقليدية يجب المفاضلة من حيث درجة الاستفادة ونجاح برامج أمن المعلومات بين البقاء على الأساليب التقليدية لأمن المعلومات مع تكاملها مع أساليب أمن المعلومات الحديثة أم الإحلال التام أكثر إفادة؟

وينبغي لسياسة أمن المعلومات على المستوى المؤسسي أن تعالج أساسيات هيكل إدارة أمن المعلومات في المنظمة، بما في ذلك: (Alnatheer, 2015)

أدوار ومسؤوليات أمن المعلومات، بيان خط الأساس للضوابط الأمنية وقواعد تجاوز خط الأساس، وقواعد السلوك التي من المتوقع أن يتبعها مستخدمو المنظمة والحد الأدنى من العواقب المترتبة على عدم الامتثال.

وفيما يلي بعض المعايير التي ينبغي على المنظمة اتباعها من أجل تنفيذ سياسة أمن فعالة:

1. يجب أن تكون سياسة أمن المعلومات واضحة ومفهومة من قبل جميع الأطراف المعنية وأن يتم متابعة هذه السياسة بانتظام لمعرفة ما إذا كان يتم انتهاكها (Madigan et al., 2004)، كما يجب وجود مبادئ توجيهية إجرائية محددة بشكل جيد للتعامل مع حوادث انتهاك السياسة (Hone & Eloff, 2002).
2. أن تكون ملائمة للثقافة التنظيمية، وملائمة للنمط الذي يتسق مع أسلوب الاتصال العام في المنظمة (Doherty & Fulford, 2005).
3. استخدام الية بسيطة لضمان سهولة فهمها، وتحديد الغرض من السياسة ونطاق المنظمة وشرح ماهو النشاط المقبول وما هو غير مقبول (Tryfonas et al., 1002).
4. ينبغي وضع سياسة أمن المعلومات على أساس الاحتياجات الأمنية والأهداف التجارية للمنظمة (Mckay, 2003).

بحث أمن المعلومات والبيانات

2- إجراءات أمن المعلومات IS Procedures

يرتبط أمن المعلومات بمجموعة من الإجراءات المصممة لحماية المعلومات (Gordon & Loeb, 2006) فالإجراءات هي المبادئ التوجيهية لتنفيذ العمليات والأنشطة القائمة على أساس الاحتياجات الموضحة في سياسة أمن المعلومات بمعنى أنها إرشادات التشغيل التي تشرح كيفية تنفيذ سياسة أمن المعلومات حيث يتم اشتقاق الإجراءات من سياسة الأمن وذلك لضمان تنفيذ ISM بشكل مناسب وصحيح. كما يجب أن تكون الإجراءات واضحة ومحددة في وصف الخطوات اللازمة لإنجاز العمليات والأنشطة، وينبغي استعراضها بطريقة دورية أو عند تغيرات بيئة الأمن نتيجة التطورات التكنولوجية المستمرة لذلك فإنه من الضروري وجود إدارة مسئولة عن إدارة برنامج التغير وقادرة على رسم إجراءات وخطوات ملائمة لإدارة ذلك التغير حيث إنه قبل إجراء أي تغير لابد من وضع تخطيط جيد يضمن أن اقتناء التكنولوجيا الجديدة لن يؤثر سلباً على سلامة أمن المعلومات ومدى الاستفادة منها

يتضح مما سبق أن إجراءات أمن المعلومات أقرب إلى المستخدمين والأجهزة من السياسة الأمنية حيث إنها توفر الخطوات التفصيلية للتركيب والإعداد والتهيئة، فهي تعمل على تحويل السياسات والتوجيهات إلى أرض الواقع ومن البيئة النظرية إلى بيئة تشغيلية حقيقية.

3- فريق إدارة أمن المعلومات ISM Team

يتكون فريق إدارة أمن المعلومات من الموظفين المشاركين في معظم أنشطة أمن المعلومات، حيث يجب أن يتمتع هذا الفريق بالمعرفة والمهارات الواسعة والتعاون في تنفيذ عمليات ISM وأن يكون دائم التحديث مع القضايا الأمنية الحالية، كما ينبغي أن يمتلك المهارة التقنية التي تؤهله للقيام بالأعمال والمهام الجديدة (Maarop et al., 2015)

4- فريق تنسيق إدارة أمن المعلومات Coordinator Team

يعمل فريق تنسيق إدارة أمن المعلومات كحلقة وصل بين كل من الإدارة العليا وفريق ISM ومراجعي أمن المعلومات والموظفين، فهو المسئول عن تنظيم التدريب والتوعية بالبرامج وإدارة الموارد المالية والبشرية وتقديم تقرير عن التقدم في ISM إلى الإدارة العليا، كما ينبغي أن يتوافر في أفراد فريق التنسيق مهارات التواصل الجيدة مع الآخرين والمعرفة الكاملة بأنشطة ISM حيث القدرة على التواصل بفعالية مع جميع المستويات في المنظمة (Zammani & Razali, 2016).

بحث أمن المعلومات والبيانات

5- فريق مراجعة أمن المعلومات IS Audit Team

فريق مراجعة أمن المعلومات هو فريق مسئول عن ضمان ضوابط الرقابة، وأنه يتم تنفيذ العمليات والإجراءات والأنشطة بشكل صحيح، فينبغي أن يتمتع هذا الفريق بمهارات الاتصال الجيدة والالتزام بالوقت المحدد لإنهاء عملية مراجعة أمن المعلومات، ولكي يتم نجاح برامج أمن المعلومات يجب أن يكون لدى فريق مراجعة أمن المعلومات فهم جيد لعمليات ISM حيث إن نقص المعرفة قد تؤدي إلى طرح الأسئلة بطريقة خاطئة وبذلك وجود معلومات غير صحيحة .

(ISACA, 2012)

6- تقييم إدارة أمن نظم المعلومات

يتم تقييم إدارة أمن نظم المعلومات من خلال:

الإدارة المستمرة للأعمال - خطة استمرارية الأعمال : الشئ المهم في استمرارية الأعمال هي خطة استمرارية الأعمال، لذلك يجب على المنظمة تحديد متطلبات أمن المعلومات وجعلها جزء لا يتجزأ من خطة استمرارية الأعمال، وأن تقوم المنظمة أيضاً بتحديد خطة العمليات والإجراءات والموارد والمسئوليات للسيطرة على الحوادث والكوارث ولضمان استمرارية الأعمال أثناء الأحداث غير المقصودة وبعدها، ينبغي تطوير هذه الخطة وتوثيقها والموافقة عليها من قبل الإدارة كما يجب اختبارها لمراقبة فعاليتها ISO/IEC 3102:20072 .

3/2 حوكمة أمن المعلومات (ISG) Information Security governance

الحوكمة بوجه عام هي عملية إدارة وتوجيه ومراقبة والتأثير على القرارات والإجراءات والسلوكيات التنظيمية (Greene, 2014)، والهدف الرئيسي لمنظمة أمن المعلومات ISO 27002:2013 هو "إنشاء إطار إداري لبدء ومراقبة تنفيذ وتشغيل أمن المعلومات داخل المنظمة"

1/3/2 مفهوم حوكمة أمن المعلومات

عرف معهد حوكمة تكنولوجيا المعلومات IT Governance Institute 2001- حوكمة أمن المعلومات على أنها "عنصر أساسي لحوكمة الشركات يتكون من القيادة والهيكل التنظيمية والعمليات المشاركة في حماية الأصول المعلوماتية، ومن خلالها يمكن لمنظمات الأعمال معالجة قضايا أمن المعلومات من منظور حوكمة الشركات"

ويرى Abu-Musa أن حوكمة أمن المعلومات هي "مجموعة من المسئوليات والممارسات التي يقوم بها مجلس الإدارة والإدارة التنفيذية بهدف توفير التوجيه الاستراتيجي، وضمان تحقيق الأهداف، والتأكد من إدارة مخاطر أمن المعلومات على نحو مناسب، وكذلك التحقق من أن موارد أمن المعلومات تستخدم بشكل فعال"

بحث أمن المعلومات والبيانات

2/3/2 أهداف حوكمة أمن لمعلومات

- إرساء ودعم أمن تكنولوجيا المعلومات لضمان أن أهداف الأعمال ومتطلبات أصحاب المصلحة لحماية المعلومات يتم الوفاء بها باستمرار.
 - إنشاء بيئة رقابية ملائمة للحفاظ على سرية وتكامل وتوافر المعلومات.
 - دعم العمليات والنظم الخاصة بها، وأيضاً حماية المعلومات من مختلف المخاطر التي يمكن أن تواجهها
- Abu - Musa -
- وتحقق حوكمة أمن المعلومات العديد من المنافع لمنظمات الأعمال التي تقوم بتطبيقها ،
ومن أهم تلك المنافع مايلي: (Whitman and Mattord, 2013)
- ارتفاع قيمة أسهم منظمات الأعمال التي تطبق ممارسات الحوكمة.
 - تعزيز تخصيص الموارد الأمنية المحدودة.
 - إدارة المخاطر بكفاءة وفعالية، وتحسين العمليات وكذلك الاستجابة السريعة للحوادث المتعلقة بأمن المعلومات.
 - وضع سياسة فعالة لأمن المعلومات، والالتزام بتلك السياسة.
 - تخفيض حالة عدم التأكد من خلال تحديد المخاطر المتعلقة بأمن المعلومات والعمل على تخفيضها إلى مستويات مقبولة.
 - توفير مستوى من التأكيد على أن اتخاذ القرارات الحاسمة والهامة لا تستند على معلومات غير صحيحة ومضللة.

4/2 الفرق بين حوكمة أمن المعلومات وإدارة أمن المعلومات

لا ينبغي الخلط بين حوكمة أمن المعلومات وإدارة أمن المعلومات فحوكمة أمن المعلومات (ISO 38500) هي النظام الذي تقوم المنظمة من خلاله بتوجيه ومراقبة أمن المعلومات.

ويصف المعهد الوطني للمعايير والتكنولوجيا National Institute of Standards and Technology (NIST) 2001 إدارة أمن المعلومات بأنها عملية إنشاء وصيانة إطار لتوفير ضمان أن استراتيجيات أمن المعلومات تتماشى مع أهداف الأعمال وتدعمها، وتتماشى مع القوانين واللوائح المعمول

بحث أمن المعلومات والبيانات

بها من خلال الالتزام بالسياسات والضوابط الداخلية، وتوفير إسناد المسؤولية، كل ذلك في محاولة لإدارة المخاطر.

كما أن إدارة أمن المعلومات تهتم باتخاذ قرارات للتخفيف من المخاطر؛ أما الحوكمة فهي تحدد من هو المخول باتخاذ القرارات، وتحدد الحوكمة إطار المساءلة وتوفر الرقابة لكفالة التخفيف من حدة المخاطر على نحو كافٍ، في حين تكفل الإدارة تنفيذ الضوابط للتخفيف من حدة المخاطر، وتوصي الإدارة باستراتيجيات أمنية، أما الحوكمة تضمن مواءمة الاستراتيجيات الأمنية مع أهداف الأعمال واتساقها مع الأنظمة.

ويمكن توضيح الفرق بين حوكمة أمن المعلومات وإدارة أمن المعلومات من خلال الجدول التالي:

جدول 6: الفرق بين حوكمة أمن المعلومات وإدارة أمن المعلومات

إدارة أمن المعلومات	حوكمة أمن المعلومات
القيام بالأمر بشكل صحيح	تعني القيام بالشئ الصحيح
التنفيذ	الرقابه
أذن باتخاذ القرار	يأذن بحقوق القرار
فرض السياسات	سن السياسات
المسئولية	المساءله
تخطيط المشاريع	التخطيط الاستراتيجي
استخدام الموارد	تخصيص الموارد

المصدر (Allen, 2007)

يتضح مما سبق أن الغرض الرئيسي من أي حوكمة داخل المنظمة هو مساءلة الإدارة أمام أصحاب المصلحة؛ ولذلك يجب أن يكون الغرض من حوكمة أمن المعلومات هو مساءلة الإدارة عن حماية أصول المعلومات المتاحة في المنظمة والوصول بالمخاطر والانتهاكات المرتبطة بأمن المعلومات إلى أدنى حد ممكن ، فالحوكمة سواء كانت مالية أو تجارية أو قانونية أو أمن المعلومات تدور حول جعل الناس يفعلون الشيء الصحيح في الوقت المناسب.

بحث أمن المعلومات والبيانات

5/2 برامج أمن المعلومات

يرى البعض أنه لا يكفي أن يكون لدى المنظمة بعض سياسات الأمان والتركيز فقط على تأمين الشبكة الخاصة بها، حيث إنه لدمج الأمان في العمليات التجارية، تحتاج المنظمة إلى برنامج قوي لأمن المعلومات يقوم بتعيين المحركات التجارية ومتطلباتها القانونية والتنظيمية والمخاطر والتهديدات التي تتعرض لها (Vizcayno, 2012)، لذلك من الضروري معرفة ما يلي:

6/5/2 مفهوم ومكونات برنامج أمن المعلومات

معظم المنظمات قد لا يكون لديها فهم واضح فيما يختص ببرنامج أمن المعلومات وأهدافه وكيفية بنائه، لذلك يجب النظر إلى أفضل الممارسات في هذه الصناعة للحصول على بعض التوجيه، فالمبدأ التوجيهي الأكثر استخداماً في جميع أنحاء العالم لبناء برامج الأمن هو ISO 27001:2005، الذي تم اشتقاقه من المعيار البريطاني القياسي BS 7799، وهو معيار معترف به دولياً لإدارة أمن المعلومات يوفر توصيات مفاهيمية رفيعة المستوى بشأن أمن المنظمة؛ ويتألف هذا المعيار من جزأين هما:

- الجزء الأول: هو دليل تنفيذ مع مبادئ توجيهية حول كيفية بناء بنية تحتية شاملة لأمن المعلومات
- الجزء الثاني: هو دليل لمراجعة الحسابات يستند إلى المتطلبات التي يجب تلبيةها لكي تعتبر المنظمة متوافقة مع المعيار ISO 27001:2005

1. سياسة أمن المعلومات للمنظمة Information security policy for the organization: وهي بمثابة خريطة لأهداف العمل ودعم الإدارة والأهداف والمسؤوليات الأمنية.

2. الأمن التنظيمي Organizational security: وهو إنشاء وصيانة هيكل أمني تنظيمي من خلال استخدام منتدى الأمن، وضابط الأمن، وتحديد المسؤوليات الأمنية، وعملية الترخيص، والاستعانة بمصادر خارجية، والمراجعة المستقلة.

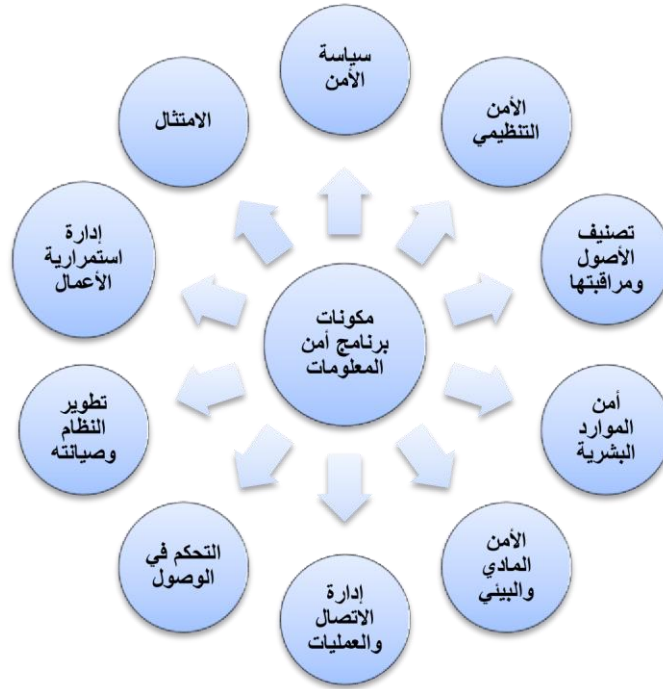
3. تصنيف الأصول ومراقبتها Assets classification and control: حيث تطوير بنية تحتية أمنية لحماية الأصول التنظيمية من خلال إجراءات المساءلة والجرد والتصنيف.

بحث أمن المعلومات والبيانات

4. أمن الموارد البشرية **Human Resources security**: وهو الحد من المخاطر الكامنة في التفاعل البشري من خلال فحص الموظفين، وتحديد الأدوار والمسؤوليات ،وتدريب الموظفين بشكل صحيح وتوثيق تداعيات عدم تلبية التوقعات.

5. الأمن المادي والبيئي **Physical and environmental security**: وهو حماية أصول المنظمة عن طريق اختيار موقع المنظمة بشكل صحيح، وإقامة وصيانة المحيط الأمني، وتنفيذ مراقبة الدخول وحماية المعدات.

1. التحكم في الوصول **Access control**: حيث التحكم في الوصول إلى الأصول استنادًا إلى متطلبات العمل وإدارة الهوية وأساليب المصادقة والمراقبة.



شكل رقم 6 مكونات برنامج أمن المعلومات .

بحث أمن المعلومات والبيانات

إدارة الاتصالات والعمليات Communications and operations Management

وذلك من خلال تنفيذ أمن العمليات حيث الإجراءات التشغيلية ، ومراقبة التغيير السليم، والتعامل مع الحوادث ، والفصل بين الواجبات، وتخطيط القدرات ، وإدارة الشبكات، والتعامل مع وسائل الإعلام.

تطوير النظام وصيانتته System development and maintenance: حيث تنفيذ الأمن في جميع مراحل عمر النظام من خلال التطوير والتنفيذ والصيانة والتخلص.

إدارة استمرارية الأعمال Business continuity management: مكافحة تعطيل العمليات العادية باستخدام تخطيط الاستمرارية والاختبار.

الامتثال Compliance: الامتثال للمتطلبات التنظيمية والتعاقدية والقانونية باستخدام الضوابط التقنية، ومراجعة حسابات النظام والوعي القانوني.

2/5/2 أهداف برامج أمن المعلومات

توجد عدة أهداف رئيسية وفرعية لبرامج أمن المعلومات، ولكن تتمثل الأهداف الرئيسية في جميع برامج الأمن في شكل 2 :

- سرية المعلومات خصوصية المعلومات Confidentially

سرية المعلومات هي إخفاء المعلومات أو الموارد بمعنى حماية المعلومات من عدم اطلاع أي شخص غير مخول له بالاطلاع عليها (White, 2011).

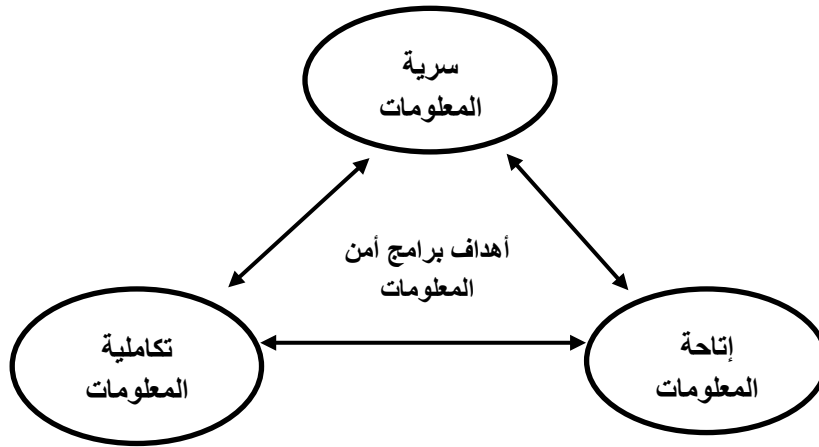
- تكاملية المعلومات سلامة المحتوى Integrity of Information

تكاملية المعلومات تعني ضمان سلامة محتوى المعلومات وضمان عدم تغييرها أو تدميرها من قبل جهات غير مخولة.

- إتاحة المعلومات القدرة على الوصول Availability of Information

إتاحة المعلومات تعني التأكد من استمرار عمل نظام المعلومات، واستمرار القدرة على التفاعل مع المعلومات وتقديم الخدمة لمستخدم المعلومات وتوافرها عند الحاجة إليها، والتأكد من أن مستخدمي تلك المعلومات لن يتعرضوا إلى منع استخدامهم لها بطريقة تير مشروعة.

بحث أمن المعلومات والبيانات



شكل رقم (٢) أهداف برامج أمن المعلومات

3- الدراسات السابقة

1/3 استقراء الدراسات السابقة

١. دراسة (Solms 2005)

قامت هذه الدراسة باختبار التوافق بين الاستخدام المتكامل لكل من الـ COBIT, ISO 17799 كآليات لإدارة أمن المعلومات.

ومن أهم النتائج التي توصلت إليها هذه الدراسة ما يلي:

١. أن كلا من COBIT, ISO 17799 يوفر محتوى أكثر فائدة لتطبيق بيئة شاملة وموحدة لحوكمة أمن المعلومات.

٢. يوفر COBIT إرشادات جيدة لماهية حوكمة أمن المعلومات.

٣. يوفر ISO 17799 المزيد من التفاصيل اللازمة لكيفية تطبيق حوكمة أمن المعلومات.

٢. دراسة (ISACA 2008)

قامت جمعية ضبط وتدقيق المعلومات Information Systems Audit and Control Association (ISACA) بوضع نموذج كمنهج رئيسي لإدارة أمن المعلومات وأظهر النموذج عد مجالات

بحث أمن المعلومات والبيانات

رئيسية إذا اتبعتها المنظمة سوف تصل إلى عدة عوامل تؤدي إلى نجاح برامج أمن المعلومات وهذه المجالات تتمثل في:

- ☐ حوكمة برامج المعلومات.
- ☐ إدارة خطر المعلومات.
- ☐ تطوير برامج أمن المعلومات.
- ☐ إدارة والاستجابة لحوادث أمن المعلومات.

ومن أهم النتائج التي توصلت إليها هذه الدراسة ضرورة قيام منظمات الأعمال بتطبيق تلك المجالات حتى تصل إلى عدة عوامل تساعد في تفعيل ونجاح برامج أمن المعلومات.

٣. دراسة حامد والحمود (٢٠٠٩)

تناولت هذه الدراسة أشكال نظم المعلومات المستخدمة في القطاع الصناعي ودرجة حوسبتها، كما تناولت أهم المخاطر التي تهدد أمن نظم المعلومات في شركات القطاع الصناعي ؛ وأثر العلاقة بين العوامل الديموغرافية للقائمين على نظم المعلومات ودرجة إدراكهم لأهمية مخاطر أمن نظم المعلومات ، وقامت هذه الدراسة أيضاً بدراسة العلاقة بين الأنشطة التي تزاولها منظمات الأعمال الصناعية والمخاطر التي تهدد أمن نظم المعلومات وأيضاً أثر العلاقة بين العوامل الديموغرافية للقائمين على نظم المعلومات ودرجة إدراكهم لعدد مرات تكرار مخاطر أمن نظم المعلومات.

ومن أهم النتائج التي توصلت إليها هذه الدراسة ما يلي:

أ- إهدار وسرقة وقت الحاسب الآلي من قبل الموظفين.

ب- تعرض أجهزة الحاسب الآلي للإصابة بالفيروسات والبرامج الخبيثة.

ج- الإدخال الخاطئ غير المتعمد من قبل الموظفين.

د- اشتراك الموظفين بكلمة مرور واحدة.

هـ- التأخير غير المتعمد لإدخال بعض البيانات والمستندات.

بحث أمن المعلومات والبيانات

٤. دراسة (Abu-Musa (2010

هدفت هذه الدراسة إلى البحث في خصائص وأهمية تطبيق حوكمة أمن نظم المعلومات، وأيضاً تقييم الوضع الحالي والملاحم الرئيسية لحوكمة أمن نظم المعلومات في منظمات الأعمال السعودية.

ومن أهم النتائج التي توصلت إليها هذه الدراسة ما يلي:

١. معظم منظمات الأعمال السعودية تدرك أهمية حوكمة أمن المعلومات لنجاح إدارة المنشأة إلا أن معظمها ليس له سياسة أو استراتيجيات أمن واضحة ومحددة.
 ٢. معظم منظمات الأعمال السعودية تعاني من حوادث أمن المعلومات والتي يصعب قياسها وتحديدتها.
 ٣. عدم امتلاك منظمات الأعمال السعودية خطط التعافي من الكوارث للتعامل مع حوادث أمن المعلومات وحالات الطوارئ، ولا يتم تنفيذ إجراءات تقييم المخاطر بشكل كافٍ وفعال.
- وأوصت الدراسة مجالس الإدارة في منظمات الأعمال السعودية بضرورة الاهتمام بحوكمة أمن نظم المعلومات واعتبارها عنصراً إلزامياً في أجندتها.

٥. دراسة (Muhrtala and Ogundeji (2013

تناولت الدراسة معرفة التهديدات المحتملة لنظم المعلومات والمستخدمة في مجال الأعمال التجارية وأيضاً كيفية التغلب على هذه التحديات في اقتصاديات الدول النامية.

ومن أهم النتائج التي توصلت إليها هذه الدراسة ما يلي:

١. أن الموظفين تشكل التهديدات الرئيسية لأصول المعلومات المستخدمة في المحاسبة الإلكترونية عندما لا يتم التحكم فيها على نحو فعال، وهذا يشير إلى أن الإدارة ينبغي أن تضع في إجراءات الترخيص على أساس الحاجة إلى معرفة فقط.
٢. يجب أن يكون هناك تسجيل منتظم ورصد الوصول المنطقي إلى الأنظمة والبيانات والسياسات والإجراءات مع الفصل بين الواجبات وحقوق الوصول للسجلات والمعاملات.
٣. يجب على المستخدمين المصرح لهم الوصول إلى التطبيقات والبيانات المطلوبة فقط لأداء مهام محددة فقط.

بحث أمن المعلومات والبيانات

٦. دراسة خليل وإبراهيم (٢٠١٦)

تهدف هذه الدراسة إلى توضيح الدور الذي تقوم به حوكمة أمن المعلومات في الحد من المخاطر التي تتعرض لها نظم المعلومات من خلال المعايير الدولية لحوكمة أمن المعلومات حيث التعرف على نوعية المخاطر التي تتعرض لها هذه النظم، وأسباب تعرضها للمخاطر، وأيضاً التعرف على ماهية حوكمة أمن المعلومات والتحقق من مدى استخدامها في بيئة الأعمال، وتحديد المعايير المستخدمة عند تطبيق حوكمة أمن المعلومات.

ومن أهم النتائج التي توصلت إليها هذه الدراسة ما يلي:

١. يوجد العديد من المخاطر التي تتعرض لها نظم المعلومات المحاسبية الإلكترونية يتمثل أهمها في المخاطر الخارجية.

٢. من أهم أسباب حدوث تلك المخاطر هي عدم وجود سياسات وبرامج لأمن المعلومات داخل منظمات الأعمال، وأيضاً عدم تطبيق الأهداف والمبادئ الخاصة بحوكمة أمن المعلومات وعدم تضمينها داخل استراتيجيتها المستقبلية.

وأوصت هذه الدراسة بضرورة وجود نشرات إرشادية لتوعية منظمات الأعمال عن دور وأهمية حوكمة أمن المعلومات من خلال قيام وزارة الاستثمار بإصدار دليل لقواعد ومبادئ ومعايير حوكمة أمن المعلومات بحيث يكون من مرفقات دليل قواعد ومبادئ حوكمة الشركات، وقيام الهيئة العامة للرقابة المالية بإلزام منظمات الأعمال بتطبيق ما ورد به من قواعد ومعايير.

٧. دراسة (Zammani and Razali (2016)

تهدف هذه الدراسة إلى تخفيف التهديدات الأمنية ونقاط الضعف التي تعصف بالعديد من المنظمات من خلال وضع مجموعة من العوامل الرئيسية لإدارة أمن المعلومات من المؤلفات الموجودة أولاً ومن ثم تأكيد العوامل واكتشاف عوامل أخرى ذات صلة من منظور الممارسين والمختصين، ومن هذه العوامل: (الموظفين، الأطراف الخارجية ذات المصلحة، تخطيط الموارد، السياسات والإجراءات، فريق تنسيق ومراجعة أمن المعلومات، إدارة المخاطر، تطوير الكفاءات والتوعية).

ومن أهم النتائج التي توصلت إليها هذه الدراسة ما يلي:

أثبتت الدراسة صحة العديد من العوامل التي تعمل على نجاح إدارة أمن المعلومات، وأوضحت أيضاً وجود فهم عالٍ لدى الممارسين لهذه العوامل. وأوصت الممارسين بتنفيذ هذه العوامل في إدارة أمن المعلومات من خلال التركيز على العمليات التي تحتاج إلى تنفيذ والوثائق الاستراتيجية والتقنية للمنظمة.

بحث أمن المعلومات والبيانات

المراجع :

- Abu-Musa, Ahmed A, (2010), "Information Security Governance in Saudi Organizations: An Empirical Study", ***Information Management and Computer Security***, Vol. 18, No. 4, pp. 20-276.
- Allen, Julia, (2007), "Characteristics of Effective Security Governance".
- Alnatheer, M, (2015), "Information Security Culture Critical Success Factors", ***International Conference on Information Technology- New Generation***.

- Doherty, N.F & Fulford, H., (2005), "Do Information Security Policies Reduce the Incidence of Security Breaches: An Exploratory Analysis", ***Information Resources Management Journal***, Vol. 18, No. 2.
- Fung, P., Kwok, L. & Longley, D., (2003), "Electronic Information Security Documentation", Australian Computer Society, Vol. 21.
- Gordon, L.A & Loep, M.P, (2006), "Budgeting Process for Information Security Expenditures", Communications of the ACM, Vol. 49, No.1.
- Greene, Sari, (2014), "Security Program and Policies: Governance and Risk Management", ***Pearson IT Certification***, Available at:
<http://www.pearsonitcertification.com/articles/article.aspx?p=2192704>
 (23/11/2019).
- Hone, K & Eloff, J.H.P., (2002), "What makes an Effective Information Security Policy", Network Security, Vol. 20, No. 6.

بحث أمن المعلومات والبيانات

- ISACA (2008), "Model Curriculum for Information Security Management", ***Information Systems Audit and Control Association***.
- ISACA, (2012), "COBIT 5 for Information Security".
- ISO/IEC 27002:2013, "Information Technology_ Security Techniques_ Code of Practice for Information Security Management", Geneva: ISO, 2013.
- Maarop, N; Mustapha, N; Yusoff, R; Ibrahim, R and Zainuddin, N, (2015), "Understanding Success Factors of an Information Security Management System Plan Phase Self-Implementation", ***International Journal of Computer and Information Engineering***, Vol. 9, No. 3.

adigan,

E.M., Petulich, C. and Motuk, K., (2004), "The Cost of Non-Compliance When Policies Fail", Proceeding of the 32nd annual ACM SIGUCCS Conference on User services, USA.

- Muhrtala, T. and Ogundeji, M., (2013), "Computerized Accounting Information Systems and Perceived Security Threats in Developing Economies: The Nigerian Case", ***Universal Journal of Accounting and Finance***, Vol. 1, issue. 1, pp. 9-18.
- NIST Special Publication 800-100, (2006), "Information Security Handbook: A Guide for Managers".
- Rotvold, Glenda, (2008), "How to Create a Security Culture in Organization", ***Information Management Journal***, pp. 32-38.

بحث أمن المعلومات والبيانات

- Singh, A and Gupta, M, (2014), "Identifying Factors of organizational information security management", ***Journal of Enterprise Information Management***, Vol. 27, No. 5.
 - Solms, B.V., (2005), "Information Security Governance: COBIT or ISO 17799 or both?" ***Computer & Security***, Vol.24, pp. 99-104.
 - Tryfonas, T., Kiountouzis, E. & Poulymenakou, A., (2001), "Embedding Security Practices in Contemporary Information Systems Development Approaches", ***Information Management & Computer Security***, Vol. 9, No. 4.
 - Vizcayno, Danieliyo, (2012), "What is Information Security Governance?", Available a White, R, (2011), "Computers at Risk: Safe Computing in the information Age", Available at: <http://www.books.google.co.zw/books?isbn=0309043883> . (20/11/2019)
 - White, R, (2011), "Computers at Risk: Safe Computing in the information Age", Available at: <http://www.books.google.co.zw/books?isbn=0309043883> . (20/11/2019)
- Whitman, M.E & Mattord, H.J; (2005), "Principles of Information Security"
- Zammani, M and Razali, R, (2016), "An Empirical Study of Information Security Management Success Factors", ***International Journal on Advanced Science Engineering information Technology***, Vol. 6, No. 6.

بحث أمن المعلومات والبيانات

خاتمة بحث أمن المعلومات والبيانات:

هكذا نكون قد قدمنا لكم بحث كامل وتفصيلي عن أمن المعلومات والبيانات وقد عرضنا في البحث طرق حماية البيانات والمعلومات وأنواع التهديدات التي تواجه أمن المعلومات وكيفية المحافظة على البيانات الشخصية، فإن كان العالم إنفتح على بعضه البعض لابد من الحفاظ على خصوصية البيانات.

خاصةً وأنها أصبحت بيانات بها الكثير من الأهمية كأرقام الحسابات البنكية وما إلى ذلك، وكم من جرائم تم عملها نتيجة إختراق البيانات وسرقتها واستغلالها في أعمال غير مشروعة.

والله ولي التوفيق