الجمهوريـــة العربيـة الســـورية
وزارة التعليم العالي والبحث العلمي
المعهد العالـــي لإدارة الأعمـــال

HIGHER INSTITUTE OF BUSINESS ADMINISTRATION

دراسة جدوى الاستثمار في برنامج أمن معلومات

حالة عملية منظمة إنسانية

Feasibility Study for Information Security Program Investment

Use case NGO

مشروع مقدم لاستكمال متطلبات الحصول على درجة
الماجستير في إدارة الأعمال
"الإدارة التنفيذية"

إعداد
عوني فلوح

إشراف الدكتور
رعد الصرن

الدفعة العاشرة
٢٠٢٠-٢٠٢١

الجمهوريـــة العربيـة الســـورية
وزارة التعليم العالي والبحث العلمي
المعهد العالـــي لإدارة الأعمـــال

HIGHER INSTITUTE OF BUSINESS ADMINISTRATION

دراسة جدوى الاستثمار في برنامج أمن معلومات

حالة عملية منظمة إنسانية

Feasibility Study for Information Security Program Investment

Use case NGO

مشروع مقدم لاستكمال متطلبات الحصول على درجة
الماجستير في إدارة الأعمال
"الإدارة التنفيذية"

إعداد
عوني فلوح

إشراف الدكتور
رعد الصرن

الدفعة العاشرة
٢٠٢٠-٢٠٢١

الإهداء

إلى مَن لا شيء يُضاهي ضوءَهم في عَتمَتي، وبِحُبهِم على اليُبْسِ قُدتُ سَفينتي..

إلى مَن تضيقُ الأبجديَّاتُ أمامَ نُبلِهم وتَعجَزُ الكلماتُ أمامَ عطائِـهم وتضحياتِهم..

إلى كلِّ مَن تركَ لديَّ من ذاتهِ في مشوارِ العُمْرِ طيّبَ الأثـر.. الحاضِرينَ مِنهُم ومن عَبَر..

إلى مَن كانَتْ بِهمُ الحَياةُ أقلَّ وطأةً وأكثرَ جمالاً

إليكم جميعاً أُهدي نِتاجَ عملي هذا

شكر وتقدير

أتقدم بِجَزيل الشُّكر والتقدير إلى الأستاذ الدكتور المُشرف رعد الصرن على كل ما قدمَه لي من توجيهات ومعلومات قيّمة ساهمَت في إثراءِ هذا البحث في جوانبهِ المختلفة.

كما أتقدَم بالشكر الجَزيل للأساتذة أعضاء لجنة المناقشة الموقَّرين، ولكافة أفراد الكادر التدريسي والعِلمي والإداري في المعهد العالي لإدارة الأعمَال على ما قدموه لنا خلال هذه الرحلة الزاخرة بِكل ما هو مفيد وداعم من خبرات ومعَارف ونشاطات أغنَت ما لدينا.

والشكر الموصول لكلِّ من ساعدني وشجعني على إتمام هذا الماجستير وإنجاز هذا البحث.

قائمة المُحتويات

قائمة الأشكال والجداول

كلمات مفتاحيّة ومُصطلحَات

جدول (١): كلمات مفتاحيّة ومُصطلحَات

الكلمة \ المصطلح	الشرح	الصفحات
Acceptable use policy سياسة الاستخدام المقبول	سياسة تؤسس لاتفاقية ما بين الموظف والمنظمة التي يعمل بها تحدد لجميع الأطراف نطاقات العمل المسموحة قبل منح صلاحيات الوصول للشبكة أو الإنترنت	٤٤
Access rights صلاحيات الوصول	هي الصلاحيات التي تمنح للمستخدمين أو البرامج والتي تسمح لهم بإنشاء أو تعديل أو استعراض أو حذف البيانات والملفات من الأنظمة وفق ما تم تحديده من مالك البيانات وسياسة أمن المعلومات المعتمدة.	٧٠-٨٠
Antivirus software برنامج مكافحة الفايروسات	تطبيق برمجي يتم تنصيبه في نقاط مختلفة من بنية تقانة المعلومات، تم تصميمه لاكتشاف وحذف الفايروسات الحاسوبية قبل أن تؤدي إلى حدوث ضرر، كما يقوم بتصحيح أو عزل الملفات المصابة بهذه الفايروسات.	٣٢
Availability الإتاحة	إتاحة الوصول للمعلومات عند الحاجة لذلك من قبل العمليات التشغيلية الآن وفي المستقبل.	٦١
Business case حالة عمل	وثيقة تجمع دراسة بين مزايا وعيوب وتكاليف ومخاطر الوضع الحالي والرؤية المستقبلية بحيث تعتبر وسيلة تساعد الإدارة التنفيذية في أن تقرر ما إذا كان ينبغي المضي قدماً في الاستثمار في المشروع أم لا.	٤٣
Business Continuity Plan خطة استمرارية العمل (BCP)	خطة يتم وضعها واستخدامها من قبل المنظمة للاستجابة للانقطاعات في عمليات تشغيلية حرجة بالنسبة لها، وذلك بالاعتماد على خطة الطوارئ لاستعادة العمل للأنظمة التقنية الحساسة في المنظمة.	٨٠
Business Impact Analysis تحليل الأثر على الأعمال (BIA)	يتم من خلاله تقييم الأصول الحساسة والحرجة بالنسبة للمنظمة ويتنبأ بالنتائج المترتبة على انقطاع الخدمة المقدمة من هذه الأصول على الأعمال التشغيلية بشكل تراكمي ويجمع المعلومات اللازمة لتطوير استراتيجيات الاستعادة والموارد الدنيا اللازمة لذلك كما يرتب أولويات الاستعادة. ويتم من خلاله أيضاً تحديد الخسارة في الدخل، المصاريف غير المتوقعة، القضايا القانونية المترتبة، العمليات المعتمدة على بعضها، بالإضافة إلى التأثير على السمعة وثقة العملاء.	٢٢
Capability Maturity Model نموذج نُضج القدرة (CMM)	منهجية تُستخدم لتحديد العناصر الرئيسية اللازمة لتطوير وتحسين كفاءة العمليات في جانب أو أكثر من المنظمة. ويصف النموذج مساراً تطورياً من خمسة مستويات لعمليات المنظمة بشكل متزايد وأكثر نضجاً للجودة والكفاءة.	٢٨-٣٦
Chief Information Security Officer (CISO) كبير موظفي أمن المعلومات	موقع وظيفي تنفيذي مسؤول عن تطوير وتنفيذ برنامج أمن المعلومات، ويتضمن إدارة إجراءات وسياسات مصممة لحماية اتصالات وأنظمة وأصول المؤسسة من التهديدات الداخلية والخارجية. بالإضافة لإدارة المخاطر المتعلقة بأمن المعلومات والتأكد من وجود درجة كافية من سرية ونزاهة وإتاحة الأصول التكنولوجية في المنظمة.	٢١
السرية Confidentiality	حماية المعلومات الحساسة أو الخاصة من الإفصاح أو الإطلاع غير المسموح به.	٣٨-٣٩
الضابط Control	أحد وسائل التعامل مع الخطر مثل السياسات والإجراءات ودلائل العمل والممارسات ومن الممكن أن يتخذ طبيعة إدارية أو تقنية أو قانونية.	١٠-٣٩
Data/assets classification تصنيف البيانات/الأصول	تقييم درجة حساسية البيانات أو المعلومات أو الأصل والذي ينتج عنه تحديد الضوابط اللازمة لكل مستوى. ويتم تحديد حساسية بيانات كل مستوى وفق فئات مسبقة التعريف لتغطية مراحل إنشاء البيانات ومعالجتها وتخزينها ونقلها. ويعكس مستوى التصنيف قيمة هذه البيانات/الأصول بالنسبة للمنظمة.	٢٣-٤٤-٧٣-٩٤
نزاهة البيانات Data integrity	الخاصية التي تميز أن البيانات تتمتع بدرجة الجودة المطلوبة ويمكن الاعتماد عليها.	٦١
تسريب البيانات Data leakage	يشير إلى المرور غير المصرح به للبيانات أو المعلومات من داخل المنظمة إلى وجهة خارج شبكتها الآمنة.	١٩-٦١-٦٦-٧١-٧٩-٨١-٩٣
Data Leak Protection الحماية من تسريب البيانات	مجموعة من التقنيات والإجراءات المرافقة لها التي تساعد في تحديد ومراقبة وحماية البيانات الحساسة من محاولات الإفشاء غير المصرح به.	٣٣
مالك البيانات Data Owner	هم الأفراد (عادة من المدراء) المسؤولين عن نزاهة ودقة واستخدام البيانات الإلكترونية الخاضعة لنطاق عملهم	٢٣
Disaster Recovery Plan خطة الاستعادة من الكوارث (DRP)	مجموعة من الموارد البشرية والفيزيائية والتقنية والإجرائية المكرسة لاستعادة النشاطات التي تم قطعها نتيجة حالات طوارئ أو كوراث ضمن وقت وكلف محددة.	٧٠-٧١-٩٣
العناية الواجبة Due Care	مستوى العناية المتوقعة من قبل شخص مسؤول يتمتع بالكفاءة والظروف المشابهة	٢٠
التشفير Encryption	عملية تطبيق وظائف رياضية معينة (خوارزمية مع مفتاح تشفير) على رسالة غير مشفرة للحصول على رسالة مشفرة	٣٢-٣٩-٤١
الجدار الناري Firewall	هو نظام أو مجموعة من الأنظمة المتناسقة التي تشكل حاجزاً بين شبكتين حاسوبيتين أو أكثر وعملياً فإنها تشكل فاصل ما بين شبكة آمنة وأخرى مفتوحة كالإنترنت.	٣٢-٧٣-٧٤-٩٤
دليل العمل Guideline	وصف طريقة محددة لأداء شيء ما بأسلوب توجيهي.	٢٤-٣٦
حادثة Incident	أي حدث لا يعتبر جزءاً من العمليات التشغيلية القياسية للخدمة والذي يؤدي أو قد يؤدي إلى انقطاع بالخدمة أو تخفيض جودتها.	٧١-٧٢-٨٠-٨١-٩٣
Incident response الاستجابة للحوادث	استجابة المنظمة للكوارث أو أي حدث خطير من الممكن أن يؤثر بشكل كبير على المنظمة ككل أو العاملين بها أو قدرتها على أداء الوظائف الإنتاجية. وقد يتضمن ذلك: تنفيذ خطة الإخلاء، إطلاق خطة الاستعادة من الكوارث، تنفيذ تقييم للأضرار أو أية نشاطات أخرى ضرورية للعودة بالمنظمة لوضع أكثر استقراراً.	٢١-٤٣-٤٤-٦١-٦٤-٧٨-٨٠
Information security أمن المعلومات	ضمان أن المستخدمين المخولين فقط (السرية) لديهم القدرة على الوصول للبيانات الدقيقة والمكتملة (نزاهة البيانات) عند حاجتهم لذلك (الإتاحة).	٧-١٠-١١-٢١-٢٤-٩٠

Information security program برنامج أمن المعلومات	المزيج الشامل من التدابير التقنية والتشغيلية والإجرائية والهيكلية الإدارية المطبقة للحصول على سرية المعلومات ونزاهتها وإتاحتها وفق متطلبات الأعمال وتحليل المخاطر.	٦-١٣-١٦-٢٨- من ٣٠ حتى٤٩- ٦١-٦٨- من٧٨ حتى٨٦
Intrusion detection system نظام كشف التسلل	نظام مراقبة يكتشف الأنشطة المشبوهة في الشبكة والأجهزة التي قد تشير إلى هجوم أمني محتمل ويصدر تنبيهات عند اكتشافها تساعد في التحقيق في المشكلة واتخاذ الإجراءات المناسبة لمعالجة التهديد.	٣٢
Intrusion prevention system نظام منع التسلل	نظام مراقبة يكتشف الأنشطة المشبوهة في الشبكة والأجهزة التي قد تشير إلى هجوم أمني محتمل ثم يقوم بمنعها من إحداث ضرر بالموارد المعلوماتية.	٣٢
IT steering committee لجنة توجيه تكنولوجيا المعلومات	لجنة على مستوى الإدارة التنفيذية العليا في المنظمة تساعد في تكوين استراتيجيات تكنولوجيا المعلومات وتشرف على النشاطات الإدارية اليومية لتسليم خدمات ومشاريع تكنولوجيا المعلومات وتركز على التطبيق الأمثل لها. ومن المفترض أن تضم ضمن أعضائها مختلف أصحاب المصلحة في المنظمة أو ممثلين عنهم.	٢١-٢٩-٦٩-٩٣
Key goal indicator (KGI) مؤشر الهدف	مقياس يعطي الإدارة فيما إذا حققت عمليات تكنولوجيا المعلومات متطلبات الأعمال المطلوبة منها أم لا.	٣٢
Key performance indicator مؤشر الأداء (KPI)	مقياس يحدد مدى كفاءة العمليات في تحقيق الأهداف المطلوبة، ويعتبر هذا مؤشر أساسي حول مدى احتمالية تحقيق الهدف ومؤشر جيد للقدرة والممارسة والمهارة.	٤٥
فحص الاختراق Penetration test	فحص حي لاختبار مدى فعالية ضوابط الدفاع المطبقة من خلال تقليد نشاطات المهاجمين الحقيقيين.	٣٣-٧٤-٧٥-٩٤
Phishing التصيد الاحتيالي	التصيد هو نوع من هجمات الهندسة الاجتماعية حيث يرسل المهاجم رسالة احتيالية (عبر البريد الإلكتروني غالباً) مصممة لخداع شخص للكشف عن معلومات حساسة للمهاجم أو لنشر برامج ضارة على البنية التحتية للضحية مثل برامج الفدية.	١٧-١٨
السياسة Policy	التوجيهات والنوايا الشاملة للإدارة معبر عنها بطريقة رسمية	٢١-٤٤-٥٥-٦٤
الإجراء Procedure	وثيقة تحوي وصف مفصل حول الخطوات الضرورية لتنفيذ عمليات محددة بما يتلائم مع المعايير المطبقة	٤٥-٧٠-٧٤-٩٣
المفتاح العام Public key	تشفير غير متماثل، وهو نظام تشفير يستخدم أزواج من المفاتيح والمفتاح العام هو الذي يتم نشره بشكل واسع لاتمام ذلك.	٣٢
Redundant array for inexpensive disks (RAID)	تقنية افتراضية لتخزين البيانات تجمع بين العديد من محركات الأقراص الفعلية في وحدة منطقية واحدة أو أكثر لأغراض تكرار البيانات أو تحسين الأداء أو كليهما.	٣٢
الخطر المتبقي Residual risks	مقدار الخطر المتبقي بعد تطبيق نشاطات الاستجابة المناسبة للخطر	٢٣-٢٤
Return on investment (ROI) العائد على الاستثمار	صيغة قياس تمكن المستثمرين من تقييم استثماراتهم والحكم على مدى جودة أداء استثمار معين مقارنة مع استثمارات أخرى مختلفة. يتم استخدام حساب عائد الاستثمار أحياناً مع أساليب أخرى لتطوير دراسة جدوى مقترح معين.	٥١-٨٥-٨٦-٨٩
Security information and event management (SIEM) نظام جمع وتحليل سجلات المراقبة	هي مجموعة من الأدوات والخدمات التي تقدم نظرة شاملة لأمن معلومات المنظمة وتوفر رؤية في الوقت الحقيقي من خلال أنظمة أمن المعلومات المستخدمة، وتقوم بإدارة سجلات الأحداث (log) عبر دمج تلك البيانات التي يتم جمعها من مصادر عديدة.	٣٣-٧٣-٧٥- ٧٦-٧٩-٨٤- ٩٤-٩٧
Service Level Agreement اتفاقية مستوى الخدمة (SLA)	اتفاقية يفضل أن تكون مكتوبة ما بين مزود الخدمة والزبون تحدد المستوى الأدنى من الأداء المطلوب للخدمة، بالإضافة إلى وصف المنتجات أو الخدمات التي سيتم تقديمها، ونقاط الاتصال لحل مشاكل الزبون، والمقاييس التي يتم من خلالها مراقبة فعالية الخدمة والموافقة عليها.	٧٢
Social engineering الهندسة الاجتماعية	هي التلاعب النفسي بالمستخدمين أو مدراء الأنظمة لتسريب أو إفشاء معلومات سرية.	١٨
المعيار Standard	مطلب إجباري لممارسات أو مواصفات معتمدة بواسطة منظمات خارجية متخصصة بالمعايير مثل ISO	٣٢-٩٠
الثغرة Vulnerability	نقطة ضعف في التصميم أو التطبيق أو التشغيل أو في أحد الضوابط الداخلية يمكن أن تؤدي لانتهاك أمن النظام	٣٣-٧٤-٧٥- ٧٩-٨٤-٩٤-٩٧

مُلخص البحث

تُعتبَر الحوادث السيبرانية أحد أكبر التهديدات التي تواجه الأعمال التجارية الحديثة، وتتركز بشكل خاص على المنظمات الصغيرة والمتوسطة ذات الميزانيات والموارد المحدودة التي تعيقُها عن حماية نفسها، مما يؤدي إلى عدم الكفاية في الحماية تجاه الأمن المعلوماتي في هذه المنظمات وإلى وقوع عدد متزايد من الهجمات وحوادث الأمن السيبراني اللاحقة. تحتاج المنظمات الصغيرة والمتوسطة إلى زيادة الاستثمار في هذا المجال، ولكن يجب موازنة ذلك مع أولويّات الأعمال الأخرى.

إن الغرض من هذا البحث هو توفير دراسة جدوى لهذا النوع من الاستثمار تُفيد مُتَّخذي القرار من كِبار المُدراء والمالكين في معظم المنظمات وخاصة منها الصغيرة والمتوسطة في سوريا وتُساعدهم على فَهم العوامل التي تُؤثر على قراراتهم المتعلّقة بالاستثمار الإضافي في الأمن السيبراني. إن فهم تلك العوامل سيُساعد هذه المنظمات بشكل كبير عند صياغة سياسات الحوكمة والمعايير في المستقبل كما أنه سيساهم في تذليل العقبات تجاه التخطيط الاستراتيجي للمنظمة لتحقيق التكامل والاندماج بين الأعمال التجارية من جهة ونشاطات برنامج أمن المعلومات الذي تم تَبَنّيه من جهة أخرى.

تم تطبيق هذه الدراسة على إحدى المنظمات الإنسانية غير الربحية العاملة في الجمهورية العربية السورية وتم اختيار الأبعاد الأربعة التي تُحدد درجة نُضج المنظمة في مجال أمن المعلومات على أنها (١) حوكَمة أمن المعلومات (٢) إدارة مخاطر أمن المعلومات (٣) موارد أمن المعلومات و(٤) الامثال والالتزام. وأظهرَ البحث بشكل حاسم أن المنظمة المُمَثِلة لحالة الدراسة تُقّر بالحاجة إلى الاستثمار في أمن المعلومات وهي مُستعدّة له ولكن هناك حاجة إلى مزيد من التوجيه والمعرفة لضَمَان أن الاستثمار يستهدف المناطق الأكثر تأثيراً على الأعمال. وقد خَلُصت الدراسة إلى مجموعة نتائج كان من أهمها أن لحوادث أمن المعلومات (في حال وقوعها) أثرٌ بالغ الخطورة على مصَالح المنظمة وأعمالها ما قد يطَال جوانب مالية وقانونية (قضائية) بالإضافة لأثرها المباشر على سُمعة المنظمة ومكانتها، بالإضافة إلى وجود درجة نُضج مُنخفضة تجاه حوكمة أمن المعلومات وإدارة المخاطر المتعلقة بذلك. مما يتطلب تخصيص جهود وموارد ملائمة لتطبيق برنامج واضح لنشاطات أمن المعلومات ضمن المنظمة تنتقل بها من الوضع الراهن إلى وضع أكثر أمناً ويتمتع بدرجة أقل من مستويات مخاطر أمن المعلومات المقبولة من قبل المنظمة.

Abstract

Cybercrime is one of the biggest threats to modern businesses. The threat is particularly poignant for small and medium-sized organizations (SMEs) with limited budgets and resources to protect themselves. This leads to insufficient protection towards information security in these organizations and to an increasing number of attacks and subsequent cybersecurity incidents. Small and medium organizations need to invest more in this area but this must be balanced with other business priorities. The purpose of this research is to provide a feasibility study for this type of investment that will benefit decision makers such as senior managers and business owners of most of Syrian organizations, especially small and medium ones, to understand the factors that affect their decisions regarding additional investment in cybersecurity protection. Understanding these factors will greatly help when formulating governance policies and standards in future, as it will contribute to overcoming obstacles towards the organization's strategic planning to achieve integration and combination between business operation and activities of information security program that has been adopted.

Four dimensions that define maturity level of the organization in information security domain were selected as (1) information security governance, (2) information security risk management, (3) resources of information security and (4) commitment and compliance. The research decisively showed that the organization recognizes their needs to invest in information security and they are ready for it. However, more guidance and knowledge are required to ensure that investment targets areas with the most impact on business.

The study concluded that information security incidents (if occured) have very serious impact on the organization interests and business continuity including financial issues, legal aspect and direct impact on reputation and position of the organization. The organization has low level of maturity towards information security governance and related risk management. This requires to allocate appropriate efforts and resources to implement a clear information security program in which it moves from current situation to more secure situation that has lower and accepted level of information security risks for the organization.

الفصل الأول: الإطار العام للبحث

١,١. مقدمة عامة

لقد باتَ مصطلح الأمن المعلوماتي أو السيبراني يتصدَّر عناوين الأخبار والإنترنت ووسائل التواصل الاجتماعي ومنتديات تكنولوجيا المعلومات بشكل يومي وكثيف. ومع ذلك فهو لا يزال ينطوي على الكثير من الغموض بالنسبة للكثيرين، حيث يسعى القائمون على المؤسسات من مديرين تنفيذيين وأعضاء مجلس إدارة ومسؤولي أمن معلومات للحفاظ على أمان بيانات شركاتهم ومواردها المعلوماتية بطرق وأساليب مختلفة ومتعددة، ما يدفعهم بقوة للبحث عن الاستراتيجيات الملائمة لتحقيق الأهداف المنشودة المتعلقة بضمان الأمن في منظماتهم وإعطاء هذه الأهداف كل الدعم والمتابعة الحثيثة وخاصة لدى المنظمات التي تعي خطورة ما يترتب عليه إهمال ذلك.

ومع التزايد المستمر والمتصاعد في اعتماد مختلف المؤسسات على التكنولوجيا في أداء أعمالها بالإضافة للانتشار السريع لمفهوم إنترنت الأشياء والأنظمة الذكيّة التي تُمكّن التجهيزات من الاتصال والتحكم بها عن طريق الإنترنت ومن خلال تقنيات اتصالات الجيل الخامس، فإن الاهتمام بالحفاظ على أمن هذه الأنظمة أصبح أمراً أساسياً ومُلحّاً، وإهماله قد يؤدي لكوارث قد لا تَحتمل أيّة مؤسسة نتائجها مهما كان حجمها. إن الأمن السيبراني هو مجموعة من الأدوات التقنية والعمليات والممارسات المُصمَمة لحماية الأنظمة والشبكات والبرامج والبيانات من المخاطر السيبرانية مثل الهجمات الإلكترونية أو التلف أو الوصول غير المصرح به، ويُشار له أيضاً باسم أمن تكنولوجيا المعلومات أو اختصاراً بأمن المعلومات. ومع تطور وتنوع الهجمات الإلكترونية اليوم وتحولها إلى خطر مباشر على المؤسسات والموظفين والعملاء، فإن الأمن السيبراني باتَ يلعب دوراً مهماً للغاية في الوقاية من هذه التهديدات الأمنية.

٢,١. دراسات سابقة

الدراسة الأولى: دراسة رضا ابراهيم صالح وآخرون (٢٠٢٠) بعنوان:

"دراسة أثر إدارة أمن المعلومات على نجاح برنامج أمن نظم المعلومات المحاسبية: مع دراسة ميدانية على الشركات المصرية"

هدَفَ هذا البحث إلى محاولة معرفة أثر إدارة أمن المعلومات على نجاح برنامج أمن المعلومات في بيئة الأعمال المصرية، ولقد قدَّم البحث إطاراً نظرياً لأهم العوامل والمتغيرات التي تؤثر على فعالية إدارة أمن المعلومات وأثرها على نجاح برنامج أمن المعلومات، كما قامَ البحث باختبار عناصر ذلك الإطار ميدانياً على عيّنة من فروع الشركة المصرية للاتصالات WE، وذلك باستخدام قائمة الاستقصاء التي تم تصميمها خصيصاً لهذا الغرض، وقد توصلت نتائج الدراسة إلى أن إدارة أمن

المعلومات لها تأثير جوهري وإيجابي على نجاح برنامج أمن نظم المعلومات المحاسبية فى البيئة المصرية، كما أوصت بضرورة اهتمام منظمات الأعمال بإدارة أمن المعلومات باعتبارها عنصراً هاماً وضرورياً لنجاح برنامج أمن المعلومات فى منظمات الأعمال المصرية.

الدراسة الثانية: Eva Weishäupl and others (University of Regensburg) (٢٠١٨) بعنوان:

"Information Security Investments: An Exploratory Multiple Case Study on Decision-Making، Evaluation and Learning"

استثمارات أمن المعلومات: دراسة حالة استكشافية متعدِدة حول اتخاذ القرار والتقييم والتعلُّم: تناولت هذه الدراسة الحاجة إلى حماية موارد المنظمات من الهجمات الإلكترونية من خلال الاستثمار الضخم في أمن المعلومات في جميع أنحاء العالم، وفي ظل وجود قيود على الميزانيات يتعين على المنظمات أن تُقرر أي التدابير الأمنية لتكنولوجيا المعلومات ينبغي أن تستثمر فيها، وكيفية تقييمها لقرارات الاستثمار، وكيفية التّعلم من القرارات السابقة للتحسين المستقبلي في إجراءات الاستثمار. تضمنت الدراسة جمع بيانات مقابلات أُجريت مع سبع شركات استشارية وخمس شركات غير استشارية تعمل في أوروبا. وكشفَت دراسة الحالة هذه أنَّ: (١) استثمارات الشركات في أمن المعلومات مدفوعة إلى حد كبير بعوامل خارجية تتعلق بالبيئة والصناعة، (٢) ليس لدى الشركات تطبيق معياري لعمليات اتّخاذ القرار، (٣) يُنظر إلى العملية الأمنية على أنها تؤثر على تشغيل الأعمال بطريقة مُزعجة، (٤) نادراً ما يكون تقييم العمليات وتطبيق المقاييس موجوداً، (٥) يتم إجراء أنشطة التعلُّم بشكل عشوائي غير منظّم. وأوصت هذه الدراسة الباحثين بإجراء أبحاث جديدة حول (١) كيفية أخذ العلاقة بين العوامل الخارجية المختلفة في الاعتبار عند اتخاذ قرارات الاستثمار في أمن المعلومات و(٢) كيف يمكن تنفيذ عمليات تقييم واستراتيجيات تعلم مدعومة في المنظمات بحيث تصبح استثمارات أمن المعلومات أكثر فاعلية في الممارسة العملية.

الدراسة الثالثة: دراسة Mohammad Naser Musa Hamdan (٢٠١٧) بعنوان:

"The relationship between network security policies and audit evidence: a culture of security for Accounting Information as mediator"

العلاقة بين سياسات أمن الشبكات وأدلة التدقيق: الثقافة الأمنية للمعلومات المحاسبية كمتغير وسيط. هدَفَت هذه الدارسة لكشف العلاقة بين سياسات أمن الشبكات (سياسة الدائرة، سياسة مدير النظام، سياسة المستخدم، سياسة ضابط أمن المعلومات) من ناحية، وتوثيق أدلّة التدقيق من ناحية أخرى. كما تم إدخال الثقافة الأمنية للمعلومات المحاسبية كمتغير يتوسط تلك العلاقة. أُجري البَحث من

خلال استبيان تم إرساله لكافة الشركات المُدرَجة في بورصة عمَّان في الأردن. ووجَدَت الدراسة أن هناك علاقة مهمة بين سياسات أمن الشبكات وتوثيق أدلة التدقيق. إلى جانب ذلك، بيَّنت أن قيمة مُعامل الارتباط بين سياسات أمان الشبكة وتوثيق التدقيق قد ارتفعَ بعد إدخال متغير الثقافة الأمنية للمحاسبة وأوضحت هذه النتيجة بحسب الدراسة أهمية التوعية بالثقافة الأمنية للشركات. وأوصى الباحث على التّأكيد على أهمية الوعي بالثقافة الأمنية لدى المنظمات.

الدراسة الرابعة: دراسة مايفل نبيل رمسيس (٢٠١٥) بعنوان:

"أثر الاستثمار فى أمن المعلومات على أداء البنوك"

اهتمت هذه الدراسة بتقييم أثَر الاستثمار فى أمن المعلومات على أداء البنوك فى القطاع المصرفي المصري في محاولة لقياس مدى تأثير الاستثمار فى أمن المعلومات على مؤشرات الربحّية وجودة الأصول وقد تناول البحث عينة تتكون من ١٣ مصرفاً. وخَلُصَت الدراسة إلى وجود تأثير معنوي للاستجابة لسرعة معالجة تهديدات أمن المعلومات على معدّل العائد على الأصول، ونظام حماية الخدمات المصرفية الإلكترونية على معدّل العائد على الملكية، والإجراءات الخاصة بتطبيق معيار أمن المعلومات ISO 27001 على معدّل العائد على رأس المال. حيث يوجد تأثير معنوي للإجراءات الخاصة بتطبيق معيار PCI-DSS لحماية بطاقات الائتمان على جودة الأصول من خلال خفض نسبة مخصصات خسائر القروض. وأوصت بالقيام ببحوث مستقبلية فى مجال دراسة أثر الاستثمار فى أمن المعلومات على أداء الشركات، وأثر تهديدات أمن المعلومات على عوائد الأسهم.

الدراسة الخامسة: دراسة Hanna Toivanen (٢٠١٥) بعنوان:

"Case study of why information security investment decision fail?"

دراسة حالة لماذا يفشل قرار الاستثمار في أمن المعلومات؟ (جامعة يوفاسكيلا، فنلندا). رَكّزت هذه الدراسة على عملية اتخاذ قرارات الاستثمار في أمن المعلومات، وكان هدفها هو التحقيق في سبب فشل قرارات الاستثمار في أمن المعلومات. تم استخدام استراتيجية البحث حيث تم البناء من دراسة حالات أربع شركات في فنلندا، وتم جمع المواد البحثية اللازمة من خلال المقابلات، وتم تحليلها من خلال طريقة تحليل المحتوى الاستقرائي. وأشارت نتائج هذه الدراسة إلى أن التّحدي المُتَمثّل في استثمارات أمن المعلومات يكمُن في إدارة استثمار متعدد الأطراف، حيث تتعلق احتمالية رفض اقتراح الاستثمار في أمن المعلومات في مرحلة اتخاذ القرار بأساليب وقدرات المنظمات لتحديد ومناقشة اقتراح الاستثمار، ومستوى المعرفة حول أمن المعلومات لدى الإدارة. ففي مرحلة بدء الاستثمار في أمن المعلومات، يتعلق التَّحدي بقدرات المنظمة على التخطيط المُستمر للعمليات التّجارية ومستوى

معرفة وفهم دور أمن المعلومات والمسؤوليات المتعلقة به. أما في مرحلة اقتراح تحديد استثمار أمن المعلومات فتَلعب قدرات المنظمات على تحديد اقتراح الاستثمار المناسب الدور الأبرز، ويؤثر المستوى الكافي من المعرفة حول أمن المعلومات هنا بقوة. ويبدو أنه ما يزال التحدي الأكبر في مرحلة التعريف يتعلق بتوفير الموارد البشرية الملائمة. حيث اتضح للدارس أنه لا يوجد موارد أمن معلومات خبيرة يمكنها متابعة الاتجاهات الحالية وتحديد المتطلبات والمقترحات وإقناع الإدارة حول ملاءمة مُقترحات الاستثمار في أمن المعلومات خلال مرحلة اتخاذ القرار. كذلك وجدَت الدراسة أن ثقافة المنظمة والتزام ودعم الإدارة تؤثر بشكل كبير على صُنع القرار المتعلق بذلك.

١,٣. ما يُميّز الدراسة الحالية عن الدراسات السابقة

تتميَّز هذه الدراسة عن الدراسات السابقة بعدّة جوانب أهمها:

- تَتعرَّض الدراسة الحالية إلى بحث جدوى الاستثمار في تطبيق برنامج أمن معلومات بشكل متكامل وشامل، وتستعرض آليات إدارته وتطويره على المدى الاستراتيجي للمنظمة، ومع نُدرة وجود دراسات محلية مشابهة فإن معظم الدراسات العربية والعالمية السابقة تناولت أجزاء معينة من مُدخَلات البرنامج أو مُخرجاته فقط.
- في الوقت الذي ركّزت فيه أغلب الدراسات السابقة على الجانب المالي أو المؤسسات ذات طبيعة العمل الماليّة فإن الدراسة الحالية تناولت البحث من جوانب تسويقية وفنّية بالإضافة إلى المالية، وحرِصَت على أن تكون الدراسة موائِمة لِطَيف أوسع من الأعمال وألا تقتصر على المؤسسات ذات طبيعة العمل المالية.
- تختلف البيئة والمنهج المُعتمَد وعيّنة البحث التي تم تنفيذ هذه الدراسة عليها عن غيرها من الدراسات حيث طُبّقت على منظمة إنسانية لم يسبق إجراء مثل هذه الدراسات عليها محلياً.

١,٤. مشكلة البحث

باتت حماية المعلومات في الوقت الراهن أمراً بالغ الأهمية لمختلف المؤسسات وقطاعات الأعمال وذلك بهدف ضمان استمرارية الأعمال بالدرجة الأولى وتَجنُّب الحوادث الأمنية التي من شأنها أن تؤثر على موارد المنظمة أو سُمعتها أو عُملائها. فإدارة أمن المعلومات وبالإضافة لكونها العامل الأساسي في صَون سرّية البيانات ونزاهتها وإتاحتها بالشكل المناسب أصبحت تلعب دوراً فريداً في تأمين وتشغيل الموارد المختلفة اللازمة لتحقيق ذلك من بُنى تحتية وأدوات تقنية وكوادر بشرية.

وعليه فإنه يمكن تلخيص مشكلة البحث في السؤال التالي: **هل هُناك جدوى من الاستثمار في برنامج أمن معلومات؟**

وللحصول على إجابة لهذا السؤال ينبغي الإجابة على الأسئلة الفرعية التالية:

١. هل هنالك جدوى تسويقية من الاستثمار في برنامج أمن معلومات؟
٢. هل هنالك جدوى تقنية من الاستثمار في برنامج أمن معلومات ؟
٣. هل هنالك جدوى مالية من الاستثمار في برنامج أمن معلومات؟

للإجابة على هذه التساؤلات الفرعية قد نحتاج لمعرفة دقيقة حول مدى نُضج بيئة الحَوكَمة في المنظمة وفيما إذا كانت تمتلك إدارة واعيَة وملتزمَة وداعمَة لبرنامج أمن المعلومات أم لا. كما ينبغي معرفة مدى نُضج إدارة مخاطر أمن المعلومات والالتزام بالمعايير ضمن المنظمة. وهل لديها القدرة على تخصيص الموارد اللازمة لتطبيق برنامج أمن المعلومات من خلال امتلاك الكوادر البشرية الخبيرة بالإدارة والإشراف على تطبيق البرنامج بالإضافة لتوفير التكنولوجيا المواكبة لتطبيقه بشكل فعّال.

١,٥. أهمية البحث

الأهمية العلمية: تأتي أهمية البحث العلمية من خلال الحصول على دراسة الجدوى الاقتصادية المتعلقة بالتخطيط والتنفيذ والتشغيل والإدارة لبرنامج أمن معلومات مُتَكامل ضمن المنظمات العاملة في سوريا.

الأهمية العَمَلية: تكمن أهمية البحث التطبيقية في مساعدة الإدارات العليا والمالكين في اتخاذ القرار الاستثماري المناسب المتعلق ببرنامج أمن المعلومات ضمن المنظمات الإنسانية.

١,٦. أهداف البحث

يمكن تلخيص أهداف هذا البحث بما يلي:

١. التعريف ببرنامج أمن المعلومات وما يرتبط به من مشاريع ونشاطات فرعية مكونة وداعِمة له.
٢. إجراء دراسة جدوى اقتصادية لتطبيق ببرنامج أمن المعلومات في المنظمة، ويتفرَّع عن هذا الهدف الأهداف الفرعية التالية:
   - إجراء دراسة تسويقية للاستثمار في برنامج أمن معلومات.
   - إجراء دراسة تقنية للاستثمار في برنامج أمن معلومات.
   - إجراء دراسة مالية للاستثمار في برنامج أمن معلومات.

٧,١. منهج البحث

تم استخدام المنهج الوصفي التحليلي (دراسة حالة)، والمتضمن جَمْع المعلومات والبيانات المتعلقة بمتغيرات الدراسة لتطبيق برنامج أمن معلومات في المنظمة.

وقُسِمَ البحث إلى جزأين: نظري وعملي، في الجزء النظري تم عرض بعض من أهم الدراسات التي تم تقديمها في هذا المجال ضمن الإطار العام للبحث، واحتوى هذا الجزء ثلاثة مَبَاحث: (١) عن برنامج أمن معلومات بشكل عام و(٢) عن دراسات الجدوى الاقتصادية ودورها في عملية اتّخاذ القرار و(٣) عن المنظمة المُمَثِلة لحالة الدراسة وأهمية الدراسة بالنسبة لها. أما بالنسبة للجزء العَمَلي فتم عرض للدراسة التي تم العمل عليها، بالإضافة لمعلومات حول نتائج الدراسات التسويقية والتقنية والمالية المتعلقة بذلك وتحليلها. وأخيراً النتائج والتوصيات المُنبثقة عن هذا البحث.

٨,١. مصادر البيانات والمعلومات

تم الاعتماد على مصادر متَعددة ومتنوعة أثناء إنجاز هذا البحث وهي:

- الكتب والدوريّات والمقالات والتقارير ذات الصلة باللغات العربية والأجنبية.
- المواقع الإلكترونية ذات المحتوى المتعلق بموضوع الدراسة على الإنترنت.
- مقابلات مع المعنيين في المُنظمة.

٩,١. حدود البحث

حدود مكانية: تم تطبيق هذه الدراسة على إحدى المنظمات العاملة في الجمهورية العربية السورية (طلبت المنظمة عدم الإشارة لاسمها في البحث لأسباب خاصة بها).

حدود زمانية: سيتم اعتماد الفترة الزمنية المحددة بالنصف الأول من السنة الميلادية ٢٠٢٢ ابتداءاً من الأول من شهر كانون الثاني ولنهاية شهر حزيران من هذا العام.

الفصل الثاني: الإطار النظري

١,٢. المبحَث الأول: برنامج أمن المعلومات

١,١,٢. مقدمة

٢,١,٢. أهمية أمن المعلومات للمنظمات

٣,١,٢. حَوكَمة أمن المعلومات

٤,١,٢. إدارة المخاطر والالتزام

٥,١,٢. برنامج أمن المعلومات

١,١,٢. مقدمة

تتعامل بعض المؤسسات حتى الآن مع أمان بياناتها باستخفاف، وتقع نتيجة لذلك ضحيّة للهجمات السيبرانية المتنوعة والكثيرة. وفي الواقع لا تزال معظم المنظمات ومنها المنظمات في سوريا غير مُحَصَّنة بالشكل المناسب ضد هذه الهجمات الإلكترونية المتطورة. ولكن بفضل معايير التكنولوجيا سريعة التطور اليوم أصبح الأمن السيبراني أولويّة لكل منظمة في جميع أنحاء العالم.

٢,١,٢. أهمية أمن المعلومات للمنظمات

إن تشكيل وتنفيذ الهجمات الإلكترونية بطرق وأساليب متعددة باتت تعتبر مسألة خطيرة جداً لأنها تحاول أن تحتفظ لنفسها بموقع متقدّم عن التطور التكنولوجي السريع الداعم للحفاظ على أمن المعلومات باستمرار. فعلى سبيل المثال فإن التصيد الاحتيالي (Phishing) وبرامج الفدية (ransomware) والخداع الإلكتروني (cyber scams) هي بعض الهجمات الإلكترونية الشائعة جداً حالياً وهي شديدة الخطورة وتم تصميمها ويتم تطويرها بشكل مستمر بدافع الوصول إلى البيانات الحساسة للمستخدمين واستغلالها وابتزاز الأموال عن طريقها وتعتمد بشكل أساسي على الضعف الموجود لدى العامل البشري للالتفاف على تقنيات حماية أمن المعلومات المتطورة.

فيما يلي بعض من الأسباب التي تساعد في فهم أهمية الأمن السيبراني بالنسبة للمنظمات:

١. انتشار الجرائم الإلكترونية

سواء كانت المنظمة كبيرة أو صغيرة الحجم فلا يستثني مجرمو الإنترنت أحداً. بل على العكس فهم يبحثون عن فرص لاستغلال البيانات وجني الأموال من هذه المؤسسات. فيما يلي بعض المؤشرات العالمية المتعلقة بذلك للعام ٢٠٢١ وفقاً لموقع (Integrity360):

- يبلغ متوسط التكلفة الإجمالية لاختراق البيانات الآن ٤,٢٤ مليون دولار بزيادة قدرها ١٠٪ في متوسط التكلفة الإجمالية لاختراق البيانات من عام ٢٠٢٠ إلى عام ٢٠٢١
- تم اكتشاف أكثر من ٨٠٪ من انتهاكات أمن المعلومات من قبل أطراف خارجية (وليس المؤسسة نفسها).
- ٨٥٪ من الانتهاكات تتعلق بالعنصر البشري.
- ٢٠٪ من الانتهاكات ناتجة في البداية عن حسابات مخترقة لمستخدمين أو مدراء أنظمة معلوماتية.
- متوسط الوقت اللازم لتحديد الخرق واحتوائه هو ٢٨٧ يوم.
- متوسط توفير تكاليف الهجمات عند وجود فرق استجابة لحوادث أمن المعلومات وتنفيذ الاختبارات الدورية لها يبلغ ٢,٤٦ مليون دولار.

- يبلغ التوفير في هجمات خرق البيانات في المؤسسات التي لديها أتمتة أمنية مطبقة بشكل كامل ٣,٨١ مليون دولار.
- تنظر ٨٨٪ من مجالس إدارة المؤسسات الآن إلى الأمن السيبراني باعتباره خطراً تجارياً.
- يستغرق اكتشاف أكثر من ٣٠٪ من الهجمات شهوراً أو سنوات.
- أعلى خمس متوسطات تكلفة إجمالية لأنواع هجمات:
  - اختراق البريد الإلكتروني للأعمال (Business email compromise) (٥,٠١ مليون دولار)
  - التصيد (Phishing) (٤,٦٥ مليون دولار)
  - الهجمات بواسطة عملاء من الداخل (Malicious insiders) (٤,٦١ مليون دولار)
  - الهندسة الاجتماعية (Social engineering) (٤,٤٧ مليون دولار)
  - حسابات الدخول المخترقة (Compromised credentials) (٤,٣٧ مليون دولار)
- ارتفعت التكلفة الإجمالية لإصلاح هجوم برامج الفدية بشكل كبير من حوالي ٧٦١ ألف دولار أمريكي في عام ٢٠٢٠ إلى ١,٨٥ مليون دولار أمريكي في عام ٢٠٢١
- في ٦٢٪ من هجمات سلسلة التوريد كانت البرمجيات الخبيثة هي تقنية الهجوم المستخدمة.
- شهد القطاع العام زيادة كبيرة في تكاليف خرق البيانات حيث ارتفعت بنسبة ٧٨,٧٪ بين ٢٠٢٠-٢٠٢١

٢. <u>التنامي في إنترنت الأشياء</u>

مع الاستمرار في التطوُّر المتعلق بإنشاء المدن الحديثة المزودة بالأجهزة الذكية فقد ازداد الاعتماد على ربط كل شيء بالإنترنت. لم يؤدِ إدخال تقنية إنترنت الأشياء (ربطها بالإنترنت) إلى تبسيط المهام وتسريعها فحسب بل أدّى أيضاً في جانب آخر إلى خلق فجوة من الثغرات الأمنية الجديدة التي يمكن للمخترقين استغلالها بِغَض النظر عن مدى درجة الإجراءات الأمنية التي تُتَّخذ. وإذا لم تتم إدارة هذه الأجهزة المتَّصلة بالإنترنت بشكل صحيح فيمكنها توفير بوابة أعمال مهمة لمجرمي الإنترنت!

إن تزايد الاعتماد على الأنظمة الرقمية على مدى السنوات العشرون الماضية زادَ بشكل جذري عدد المُجتَمعات الفعّالة رقمياً. كما أن التحول الناجم عن وباء COVID-19 أدى إلى تسريع الاعتماد على المنصات والأجهزة التي تسمح بالعمل عن بُعد وتواجُد البيانات الحساسة بشكل مُشتَرَك مع جهات خارجية مثل مزودي الخدمات السحابية ومُجَمِعي البيانات وغيرهم ممن يعتبرون وسطاء مرتبطون بالتكنولوجيا لهذه الأنظمة، في الوقت الذي يتيحون فيه أدوات قوية للتخزين ومعالجة البيانات باتوا يشكلون طبقة اعتماد إضافية كمقدمي خدمات.

٣. فَجوة الأمان في العامل البشري

لطالما كانت الموارد البشرية وموارد تكنولوجيا المعلومات أحد أهم جوانب العمل في أي مؤسسة، وبغض النظر عن درجة اعتمادهم على بعضهم البعض فقد كانت هناك فجوة أمنية دائمة بينهما، حيث كان ولا يزال يُعتبَر العامل البشري هو الحلقة الأضعف في سلسة حماية أمن المعلومات. ومن أجل سد هذه الفجوة فلا بد من تزويد الأفراد العاملين في المؤسسة بالتدريب المناسب لزيادة الوعي والمهارات بالأمن السيبراني وخلق ثقافة عمل مرنة عبر الإنترنت في المؤسسة.

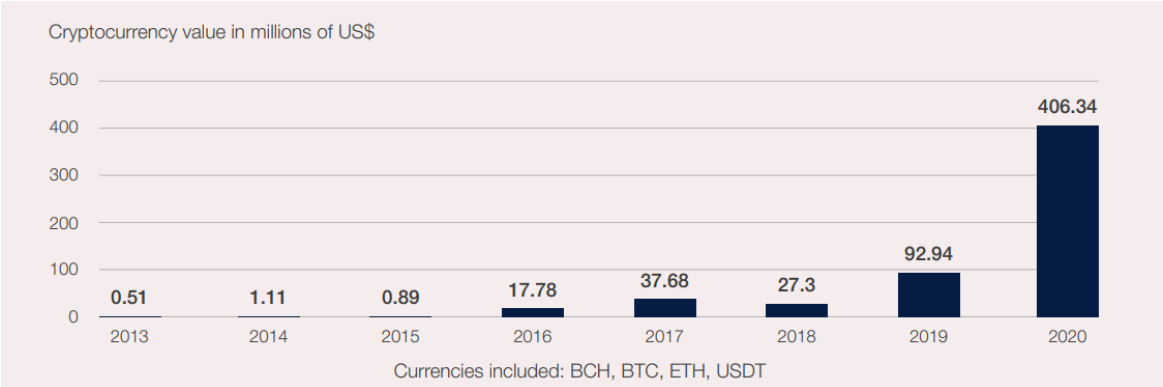
٤. تكاليف المخاطر السيبرانية

لا تتضاعف الهجمات الإلكترونية اليوم في الأعداد فحسب بل تتضاعف أيضاً في تكلفة الضرر الناتج، حيث يمكن أن تكون هذه الهجمات مُكلِفة لدرجة لا تستطيع أي منظمة تحمُّلها إذا لم تتخذ تدابير أمنية مناسبة لتخفيف تأثير المخاطر المرتبطة بها. ومن المتوقع أن تكلّف الجريمة الإلكترونية العالم ١٠,٥ تريليون دولار سنوياً بحلول عام ٢٠٢٥ ولا يقتصر الأمر على الضرر المالي ولكن يتعداه أيضاً للتأثير على سُمعة المؤسسة وفقدان ثقة العملاء في أعمالها التجارية.

٥. أمن البيانات الحساسة

عندما يتعلق الأمر بأمن البيانات الحساسة فإن هناك عدد مثير للقلق لانتهاكات البيانات وتسريبات المعلومات التي تتصدَّر عناوين الأخبار كل يوم تقريباً. ويُعَد تنفيذ حلول الأمن السيبراني الصحيحة أمراً ضرورياً للحد من المخاطر الإلكترونية التي تتعلق بتسريب أو سرقة البيانات الحساسة للمؤسسة.

الشكل (١) مبالغ العملات الرقمية المدفوعة لهجمات برامج الفدية المسجلة ما بين ٢٠١٣-٢٠٢٠



المصدر: Based on Chainanalysis. Ransomware 2021: Critical Mid-Tear Update.

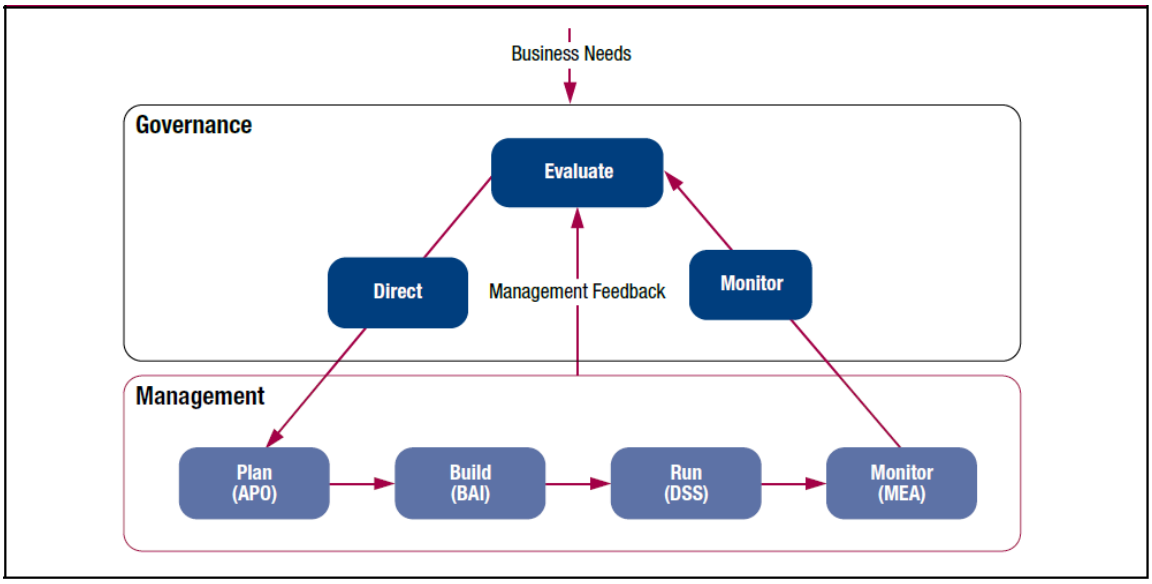
٣,١,٢. حَوكَمة أمن المعلومات

تَضْمَن الحوكَمة أن احتياجات ومتطلبات وخيارات أصحاب المصلحة متوازنة ومتَّسقة وتصُب في اتجاه تحقيق أهداف المنظمة، وأن صياغة التوجيهات تتم عبر الأولويات واتخاذ القرارات المناسبة وتحقيق مراقبة الأداء والالتزام مع الأهداف والتوجيهات المتفق عليها.

لتحقيق مهمّة حماية المعلومات في المنظمة والتي باتت تعتبر من أهم موارد المنظمات يجب أن يتم رفع هذه المسألة إلى مستوى مجلس الإدارة والإدارة التنفيذية كما هو الحال مع مواضيع الحوكمة الحساسة الأخرى، إذ أن تعقيدات وروابط وحساسية أمن المعلومات وتفويضات الحوكمة المتعلقة به يجب أن تُعَالَج ويتم تبنيها على أعلى مستويات إدارة المنظمة.

إن حوكمة أمن المعلومات هي مجموعة من المسؤوليات والممارسات التي يتم وضعها من قبل مجلس الإدارة والإدارة التنفيذية بهدف إعطاء توجُّهات استراتيجية والتأكد من تحقيق الأهداف وضمان وجود إدارة ملائمة للمخاطر واستخدام موارد المنظمة المتاحة بشكل مسؤول. وتُعتبَر إدارة المنظمة العليا مُمَثَّلة بمجلس الإدارة والإدارة التّنفيذية هي المسؤول المباشر عن حوكمة أمن المعلومات ويجب أن تعمل على توفير القيادات الضرورية والهيكل الوظيفي والإجرائي المناسب لتضمن تكامل وشفافية حوكمة أمن المعلومات مع بنية حوكمة المنظمة ككل.

الشكل (٢) علاقة الحوكمة بالإدارة وفق إطار COBIT 5



المصدر: ISACA, COBIT 5, USA, 2012

ويُحقق تطبيق حوكَمة أمن المعلومات العديد من الفوائد من أهمها:

- تحديد المسؤوليات المدنية والقانونية على المنظمة التي قد تنتج عن غياب العناية الواجِبَة أو عدم الدقّة في الامتثال للسياسات.
- توفير تأكيد على الالتزام بالسياسات.
- زيادة القدرة على التنبؤ وتقليل درجة عدم اليقين في الأعمال التشغيلية للمنظمة عن طريق تعريف وتخفيض المخاطر إلى مستويات مقبولة.
- توفير البنية وإطار العمل لتحسين استثمار موارد أمن المعلومات المحدودة بالشكل الأمثل.
- توفير مستوى من الضَمان بأن القرارات الحساسة المُتَخذَة ليست مبنية على معلومات مضلّلة.

- توفير أسس متينة لكفاءة وفعالية إدارة المخاطر وتحسين العمليات والاستجابة للحوادث واستمرارية العمل.
- توفير ثقة أكبر في التفاعل مع الشركاء التجاريين.
- تحسين الثقة في العلاقات مع الزبائن.
- حماية سُمعة المنظمة.
- تمكين طرق جديدة للعمليات الإلكترونية.
- تعزيز مسؤولية تأمين البيانات خلال نشاطات الأعمال الحسَّاسة كالإندماج والإستحواذ والاستجابة للتشريعات.

ويُبيّن الجدول التالي العلاقة بين مُخْرَجات حوكمة أمن المعلومات مع المسؤوليات الإدارية المختلفة:

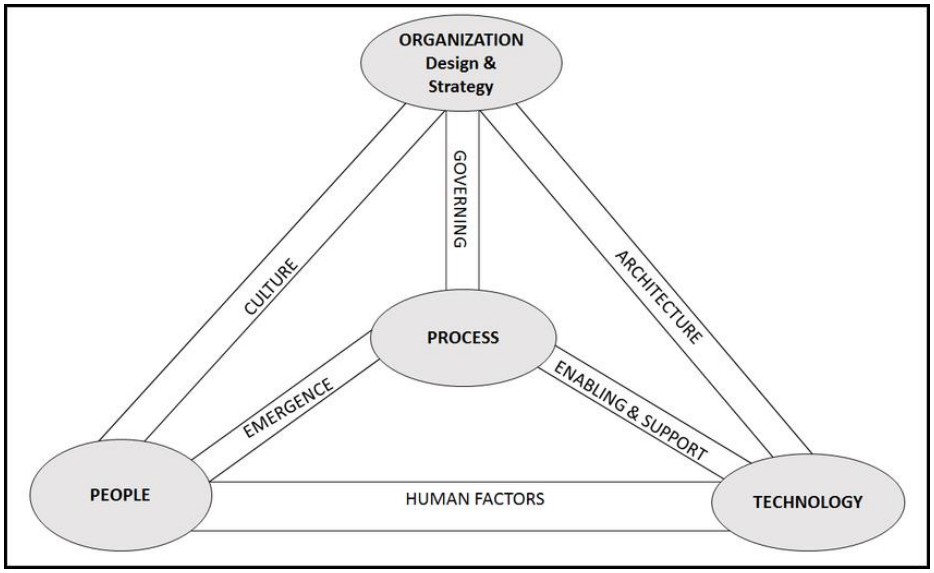
جدول (٢): العلاقة بين مُخرجات حوكمة أمن المعلومات مع المسؤوليات الإدارية

المستوى الإداري	التوافق الاستراتيجي	إدارة المخاطر	القيمة المُكتسَبَة	قياس الأداء	إدارة الموارد	إجراءات الضمان
أعضاء مجلس الإدارة	طلب توافق مثبت بين أهداف الأعمال وأمن المعلومات	– تحديد المخاطر المقبولة والهوامش – الإشراف على سياسة إدارة المخاطر – ضمان الالتزام بالتشريعات	طلب وجود تقارير حول كلف ومنافع نشاطات الأمن	طلب وجود تقارير حول الفعالية الأمنية	الإشراف على سياسة إدارة المعرفة والاستخدام الأمثل للموارد	الإشراف على سياسة تكامل إجراءات الضمان
الإدارة التنفيذية	تحديد العمليات لتكامل أهداف الأعمال وأمن المعلومات	– التأكد من تضمين إدارة المخاطر في كل الوظائف والمسؤوليات – مراقبة الالتزام بالتشريعات	طلب تطوير حالات عمل حول مبادرات الأمن	طلب مراقبة وقياس نشاطات الأمن	التأكد من إجراءات جمع المعارف والقياس الناجح	الإشراف على كافة وظائف وخطط الضمان لتحقيق التكامل
لجنة التوجيه / Steering Committee	المراجعة وتوفير مدخلات استراتيجية الأمن ومتطلبات الدعم الفعّال للأعمال	– تحديد المخاطر المستجدة, اقتراح أفضل الممارسات الأمنية لوحدات الأعمال وتحديد قضايا الالتزام	المراجعة وتقديم النصح حول فعالية كلف نشاطات أمن المعلومات لدعم الأعمال	المراجعة وتقديم النصح فيما إذا كانت مبادرات الأمن توافق أهداف الأعمال	مراجعة إجراءات جمع المعارف والاستخدام الأمثل للموارد	– تحديد عمليات التشغيل الحرجة ومزودي الضمان – بذل جهود مباشرة في التأكد
إدارة أمن المعلومات / CISO	تطوير استراتيجية الأمن بما يتوافق مع أهداف العمل. الإشراف على برنامج أمن المعلومات والتواصل مع أطراف الأعمال للتوافق المستمر	– التأكد من تنفيذ تحليل تأثير المخاطر على الأعمال – تطوير استراتيجيات تخفيف المخاطر – فرض الالتزام بالسياسة والتشريعات	مراقبة وتحسين كفاءة وفعالية موارد أمن المعلومات	تطوير وتطبيق تقارير الرقابة والقياس لدعم اتخاذ القرارات الاستراتجية والإدارية والتشغيلية	– تطوير أساليب لجمع ونشر المعارف – مراقبة وقياس الاستخدام الأمثل للموراد وكفاءة الكلف	– التنسيق مع مزودي الضمان الآخرين – التأكد من أن أية فجوات أو تداخلات تم تحديدها ومعالجتها – عرض التكامل مع نشاطات الضمان الأخرى
إدارة التدقيق	التقييم والإبلاغ عن درجة التوافق	التقييم والإبلاغ عن ممارسات ونتائج إدارة المخاطر للمنظمة	التقييم والإبلاغ عن فعالية كلف برنامج الأمن	التقييم والإبلاغ حول شمولية وفعالية المراقبة والقياس للبرنامج	التقييم والإبلاغ عن الفعالية والاستخدام الأمثل للموارد	التقييم والإبلاغ عن التكامل وكفاءة عمليات الضمان

المصدر: ISACA, Information Security Governance: Guidance for Information Security Managers: 2008

ويمكن تلخيص نموذج الحوكَمة الخاص بأمن المعلومات بأربعة عناصر هي (استراتيجية وتصميم المنظمة، الأفراد، العمليات، التكنولوجيا) مرتبطة ببعضها بستة روابط ديناميكية (الحوكمة، الثقافة، التمكين والدعم، النشوء، العوامل البشرية، البنية) والتي تتفاعل وتؤثر وتتأثر ببعضها البعض. وعند حدوث أي تغيير غير مدروس أو إدارة غير مناسبة لأي جزء من النموذج فإن بقية الأجزاء ستكون حتماً في خطر.

الشكل (٣) نموذج الأعمال الخاص بأمن المعلومات



المصدر: ISACA, CISM Review Manual 14th Edition

٤,١,٢. إدارة المخاطر والالتزام

يُعرَّف الخطر بأنه اتّحاد احتمالية حدوث الحدث (probability) مع نتائجه (consequences) وتتضمن احتمالية الحدوث كلاً من الثغرات أو نقاط الضعف (vulnerabilities) والتهديدات (threats). ومن المفيد معرفة أن احتمالية الحدوث تُحَدَّد عادة من خلال تقييم الخطر (risk assessment) بينما يتم توَقُّع نتائج الخطر في حال حدوثه من خلال تحليل الأثَر على الأعمال (Business Impact Analysis "BIA").

بِغَض النَّظر عن طريقة تعريف الخطر فإن إدارة مخاطر المعلومات هي التطبيق المُنَّظم للسياسات والإجراءات والممارسات المتعلقة بمهام تقييم الخطر التي تتضمن: تحديد وتعريف الخطر بالإضافة إلى تحليله وتقييمه، كما تتضمن أيضاً مُعالجة الخطر (أو الاستجابة له) والإبلاغ عنه ومراقبته.

إن تصميم وتطبيق عمليات إدارة المخاطر في المنظمة سوف يتأثر بما يلي:

- مهمة وأهداف المنظمة
- بُنية المنظمة

- القدرة على استيعاب الخسائر
- المنتجات والخدمات
- عمليات التشغيل والإدارة
- العوامل المتعلقة بالتشريعات والبيئة

١,٤,١,٢. مخرجات إدارة المخاطر

يُعتَبر برنامج إدارة المخاطر الفعَّال أحد مُنتجات تطبيق الحوكمة الجيّدة في المنظمة من خلال تنفيذ المتطلبات اللازمة لتسكين المخاطر وتقليل نتائجها على موارد المعلومات لمستويات مقبولة وإعطاء:

- فهم لنقاط الضَّعف والتهديدات.
- فهم للمخاطر التي تتعرض لها المنظمة والنتائج المحتمَلة لحدوثها.
- معرفة بأولويات إدارة المخاطر وفقاً للعواقب المحتمَلة لكل منها.
- استراتيجات تسكين أو قبول مخاطر ملائمة وفقاً لعواقب المخاطر المتبقية المقبولة بعد تطبيق الاستراتيجات.
- معايير قابلة للقياس بأنَّ الموارد المستخدمة في إدارة المخاطر يتم استغلالها بالطرق الأكثر فعّالية وعائدية.

٢,٤,١,٢. الإدارة الفعّالة للمخاطر

يجب أن يتم دعم الإدارة الفعّالة لمخاطر المعلومات من قبل كافة أعضاء المنظمة، فدعم الإدارة التنفيذية العليا تُضفي المصداقية والزخَم لجهود إدارة المخاطر. وستذهب حتى أفضل ممارسات التصميم والتطبيق في مهب الريح في حال تعامَلَ معها أشخاص غير مهتمين أو غير مدربين.

بالإضافة لذلك ينبغي أن يعلم الموظفون بالمخاطر التي تواجهها المنظمة وأن يفهموا مسؤولياتهم وأن يتم تدريبهم على الإجراءات المُطَبَّقة، كما ينبغي أن تتم مراقبة الالتزام بضوابط أمن المعلومات وفحصها وفرضَها باستمرار على مستوى كامل المنظمة.

ولتطوير برنامج فعّال لإدارة المخاطر يجب مراعاة الخطوات التّالية:

- تحديد محتوى البرنامج والغرض منه
- إنشاء النّطاق والميثاق للبرنامج
- تحديد الصلاحيات والبنية وهرمية الإبلاغات
- تحديد وتصنيف الأصول ومالك كل منها

- تحديد الأهداف
- تحديد المنهجية المستخدمة وفريق التنفيذ

ويتحمل مدير أمن المعلومات مسؤولية تطوير ونشر وتطبيق والإشراف على برنامج إدارة مخاطر المعلومات لتحقيق مستوى مقبول من الخطر. وينبغي عليه مراعاة أفضل فعالية كُلفة ممكنة عند تطبيق ذلك.

٣,٤,١,٢. تحديد إطار عمل إدارة المخاطر

لتطوير برنامج إدارة مخاطر مُنَظَّم يجب الاعتماد على نموذج مرجعي يتوافق مع ظروف المنظمة ويعكس الحالة المستقبلية المرجوّة. ويوجد العديد من المعايير المتاحة عالمياً والتي تؤمن دليل عمل لأساليب إدارة مخاطر تقنيات وأمن المعلومات، منها:

- COBIT 5
- ISO 31000:2018: Risk management- Principles and guidelines
- IEC 31010:2009: Risk management- Risk assessment techniques
- National Institute of Standards and Technology (NIST) Special Publication 800-39: Managing Information Security Risk
- HB 158-2010: Delivering assurance based on ISO 31000:2009
- ISO/IEC 27005:2011: Information Technology-Security techniques-Information security risk management.

ولتحديد إطار عمل فعَّال ومُناسب للمنظمة يجب أن يتم أولاً:

- فهم خلفية المنظمة والمخاطر التي تتعرض لها (مثل جوهر عملها وأصولها القيّمة ومناطق المنافسة).
- تقييم نشاطات إدارة المخاطر الموجودة أصلاً ضمنها.
- تطوير البُنيَة والعمليات لتحسين ضوابط ونشاطات إدارة المخاطر.

وينبغي أن يتكامل برنامج إدارة المخاطر مع نظام المنظمة ككل ويتوافق مع احتياجاتها.

٤,٤,١,٢. تطبيق إدارة المخاطر

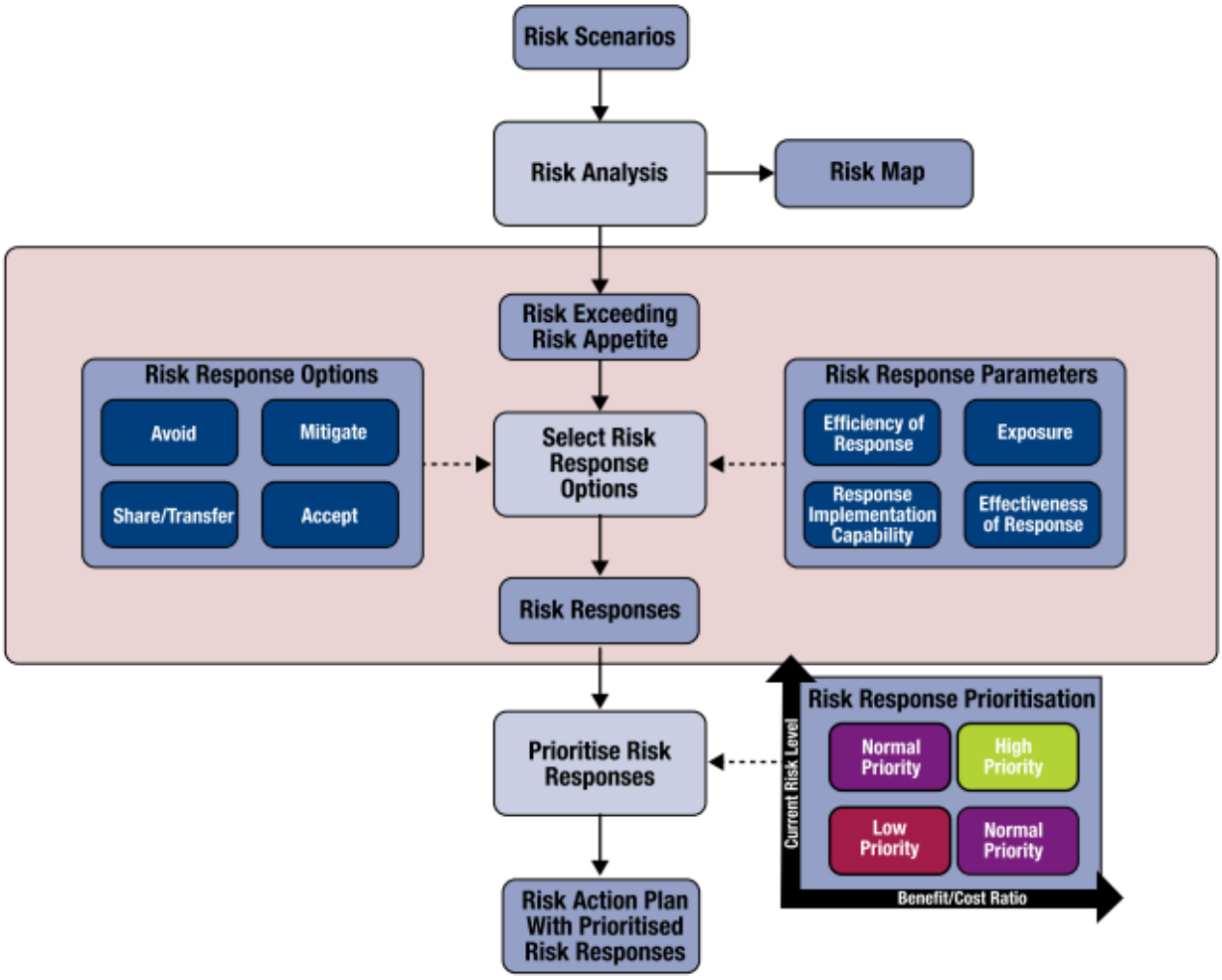
تتألف إدارة المخاطر عادة من العمليات التالية:

- تحديد النطاق والحدود
- تقييم المخاطر

- معالجة المخاطر
- قبول الخطر المتبقي
- مراقبة وتبادل معلومات الخطر

ويُبيّن الشكل (٤) مراحل الاستجابة للخطر حيث يجب التميّز بين أنواع الاستجابة المُتَعدّدة (إلغاء النشاط، تخفيض الخطر، نقل الخطر أو الاحتفاظ بالخطر) باختلاف التَّسميات أو المصطلحات المستخدمة لوصفها وسيتم شرح كل منها بالتفصيل في فقرة لاحقة.

الشكل (٤) مراحل الاستجابة للخطر



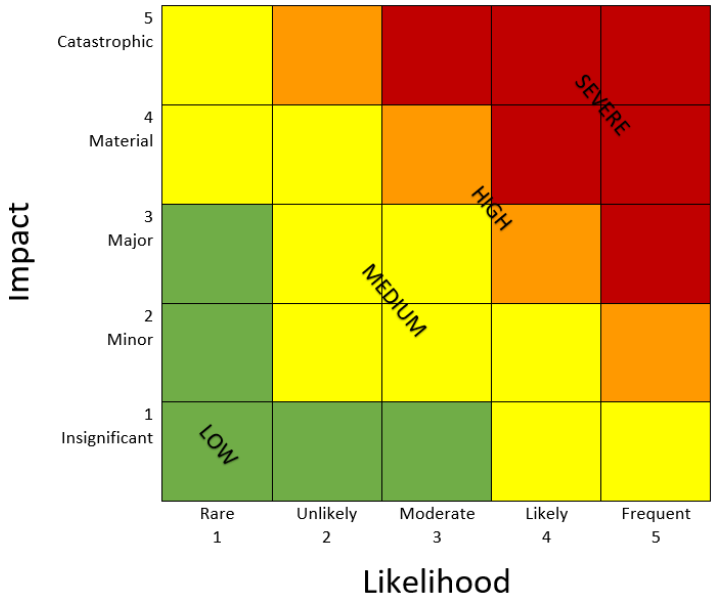
المصدر: ISACA, COBIT 5 for Risk, USA, 2013

٥,٤,١,٢. تحليل المخاطر

في هذه المرحلة يتم تقييم وفهم طبيعة ودرجة الخطر وتعتبر المعلومات الناتجة عنها الدّخل الأساسي لمتخذي القرار لتحديد كيفية التعامل مع الخطر بأكثر الطرق فعالية بالنسبة للكلفة.

ومن الأساليب الشائعة لتحليل الخطر استخدام مصفوفة من ٥ أسطر و٥ أعمدة والتي تدعى (semiquantitative impact matrix) كما هو موضح في الشكل التالي:

الشكل (٥) مصفوفة درجة تأثير الخطر



المصدر: ISACA: CISM Review Manual 14th Edition

الهدف من طريقة تحليل الخطر هذه هو إسناد قيمة لدرجة الخطر التي تم استنتاجها بالتقييم النوعي (qualitative) وتكون هذه القيمة عادة تقديرية وليست حقيقية وتستخدم كمدخل للتقييم الكّمي (quantitative) ويعطي هذا الأسلوب القدرة على ترتيب المخاطر وتُحسَب القيمة المقابلة لاحتمالية حدوث ونتائج كل خطر (من ١ إلى ٢٥) عن طريق ضرب التأثير باحتمالية الحدوث المقابلة للخطر:

$$Risk = impact \times likelihood$$

ومن الجّدير الملاحظة أن تقييم الخطر أحياناً يقود لاتخاذ قرار بإجراء مزيد من التحليل. وهنا يجب أخذ عدة أمور بعين الاعتبار مثل أهداف المنظمة وآراء أصحاب المصلحة وبالتأكيد نطاق وهدف إدارة الخطر مع الحفاظ على هامش خطأ مقبول. وعادة ما تُؤخذ القرارات المتعلقة بالمخاطر اعتماداً على درجة الخطر ولكن قد يكون هناك عوامل مؤثرة أخرى يجب أخذها بالاعتبار أيضاً منها:

- عواقب الخطر واحتمالية وقوع الحدث
- الأثر المُجَمَّع لعدة أحداث قد تقع بشكل مُتَلاحق
- كلفة التعامل مع الخطر
- قدرة المنظمة على استيعاب الخسائر الناتجة عن وقوع الخطر

٦,٤,١,٢. خيارات معالجة الخطر

تمتلك المنظمات عادة أربع استراتيجيات للتعامل مع المخاطر:

١. إلغاء النشاط

في هذه الحالة يتم تجنب الخطر عن طريق إلغاء النشاط المرتبط به أو إجراء إعادة تصميم أو إعادة هندسة لهذا النشاط، وعادة ما يتم اللجوء لذلك عندما تكون منافع النشاط لا تستحق التعرض للخطر المرتبط بإبقاءه أو تَحمُّل المسؤوليات الناتجة عنه.

٢. نقل الخطر

قد تلجأ المنظمة أحياناً لشراء بوالص تأمين لتغطية بعض المخاطر لديها، وبالتالي يتم نقل الخطر إلى شركة التأمين عن طريق تغطية نتائج الخطر وفق تقديرات شركة التأمين. ولكن يجب الانتباه هنا أن الخطر لم يتم نقله فعلياً لشركة التأمين وإنما يتم تخفيض أثره على المنظمة بقدر ما يغطيه عقد التأمين كلياً أو جزئياً. وعادة ما يتم اللجوء لهذه الاستراتيجية عندما تكون احتمالية حدوث الخطر منخفضة ولكن تأثيرها عالٍ جداً ومن الأمثلة على ذلك الكوارث الطبيعية كالزلازل والفيضانات في الأماكن التي لا تحدث بها عادة.

ومن الأمثلة الأخرى على نقل الخطر تعهيد وظائف تكنولوجيا المعلومات (outsourcing) لموردين خارجيين، ويجب الانتباه هنا للتحديد الدقيق للمسؤوليات عند التعاقد.

أخيراً يجب التأكيد على أن هذه الاستراتيجية قد تُغطّي الآثار المالية الناتجة عن الخطر وتنقلها لطرف آخر ولكن لا يمكن نقل أية تبِعات قانونيّة عادة.

٣. تخفيض الخطر

يمكن تخفيض الخطر أو تسكينه بطرق عديدة، مثلاً يمكن أن يتم التخفيض عن طريق تطبيق أو تحسين ضوابط الأمن والتي يمكن أن تكون ضوابط تمنع حدوث الخطر كلياً أو ضوابط مكملة تُخَفّض من تأثير الخطر حال وقوعه.

٤. قبول الخطر

هناك نطاق واسع من المخاطر التي يتم قبولها من قبل المنظمة. من هذه الحالات عندما تكون كُلفة تخفيض الخطر أعلى بكثير من تأثيره. أو عندما لا يكون من المُجدي تخفيض خطر له درجة تأثير منخفضة أساساً. ويجب الانتباه هنا أن تأثير المخاطر قد لا يكون مالياً في كل الحالات حيث هناك عناصر أخرى يجب أن تؤخذ أيضاً بعين الاعتبار عند التعامل مع المخاطر المختلفة كثقة الزبائن والمسؤولية القانونية والسمعة.

٢,١,٥. برنامج أمن المعلومات

يتضمن برنامج أمن المعلومات مجموعة النشاطات والمبادرات والمشاريع المُرتبة لتحقيق استراتيجية أمن المعلومات ضمن المنظمة وإدارة هذا البرنامج بما يضمن تحقيق ذلك. والاستراتيجية هي الخطة الموضوعة لتحقيق أهداف أمن المعلومات المتواءمة مع أهداف المنظمة. وبذلك فإن برنامج أمن المعلومات يعمل على التوجيه والمراقبة والإشراف على النشاطات المتعلقة بأمن المعلومات لدعم هذه الأهداف. وإدارة هذا البرنامج تعمل على استثمار الموارد البشرية والمادية والمالية المتاحة بالشكل الأمثل لاتخاذ القرارات الأنسب باتجاه دعم عمل المنظمة.

١,٥,١,٢. عناصر برنامج أمن المعلومات الأساسية

يوجد ثلاثة عناصر أساسية تضمن التصميم والتطبيق والإدارة الناجحة لبرنامج أمن المعلومات وهي:

- يجب أن يُبنى البرنامج على استراتيجية أمن معلومات مُعَدَّة بعناية ومتوافقة مع أهداف المنظمة وتدعمها.
- يجب أن يُصمَّم البرنامج بالتعاون والدعم من إدارة المنظمة وكافة الأطراف ذات العلاقة.
- يجب تطوير مقياس فعّال للبرنامج في مختلف مراحلِه يساعد في توفير التّغذية الراجعة ويُقدِّم المؤشرات أثناء تنفيذ البرنامج للحصول على المُخرَجَات المطلوبة.

في الواقع لا تزال العديد من المؤسسات غير جاهزة لتحمُّل التكاليف والجهود اللازمة لتطبيق برامج أمن المعلومات. في مثل هذه الحالة يحتاج مدير أمن المعلومات لتجزئة الأهداف ويمكن أن يتم ذلك من خلال استخدام معايير مُعتَمَدة مثل COBIT أو ISO27001:2013 بالإضافة إلى نموذج نُضْج القُدرة Capability Maturity Model (CMM). هذا الأسلوب سيُمَكّن مدير أمن المعلومات من توصيف الوضع الراهن ووضع الأهداف والاستراتيجية اللازمة لتحقيقها.

٢,٥,١,٢. أهمية برنامج أمن المعلومات

إن تحقيق مستوى مناسب من أمن المعلومات بكلفة معقولة يتطلّب تخطيط جيد واستراتيجية فعّالة وإدارة قادِرة. فبرنامج أمن المعلومات لديه متطلبات متغيرة باستمرار لتوفير حماية الأصول المعلوماتية وتحقيق المتطلبات التشريعية.

لذلك فالتنفيذ الجيد لبرنامج أمن المعلومات سوف يؤدي لتصميم وتطبيق وإدارة ومراقبة نشاطات وفعاليات البرنامج والانتقال بها من الخطط الاستراتيجية إلى الواقع الفعلي.

٣,٥,١,٢. مخرجات برنامج أمن المعلومات

ينبغي أن يتم تحديد وتعريف أهداف البرنامج بدقة كما أنه من الضرورة تحديد مُعَامِلات القياس لتتمكن إدارة البرنامج من تقييمه ومعرفة ما تم تحقيقه من الأهداف وما يجب تحسينه لتلافي أي تقصير.

وبِغض النَّظر عن طبيعة حوكمة أمن المعلومات المطبقة في المنظمة فإن تحقيق مستويات تطبيق مقبولة للمخرجات الستة التالية تُعتبر من أساسيات تطوير أي برنامج أمن معلومات فعّال:

١. التوافق الاستراتيجي

إن الوصول إلى التوافق المنشود ما بين أمن المعلومات ومتطلبات الأعمال التجارية يتطلب تواصل منتظم مع مالك العمل لفهم خططه وأهدافه. وعادة ما يتطلب ذلك الحصول على إجماع حول المعطيات الضرورية لأمن المعلومات بالتعاون مع الوحدات التشغيلية. ويقع الحصول على هذا الإجماع على عاتق مدير أمن المعلومات الذي من واجبه الوصول لفهم مشترك للعديد من القضايا ومنها:

- مخاطر المعلومات في المنظمة
- اختيار أهداف ومعايير الضوابط المناسبة
- التوافق على مستوى وهوامش الخطر المقبولة في المنظمة
- تحديد القيود المالية أو التشغيلية أو غيرها..

ويمكن تحقيق ذلك من خلال عرضه في اجتماعات اللجنة التوجيهية لأمن المعلومات (Security Steering Committee) التي من المفترض أن تضُم ضمن أعضائها مختلف أصحاب المصالح في المنظمة أو ممثلين عنهم. ويجب على إدارة أمن المعلومات عرض الاستراتيجية الخاصة بذلك ضمن تقارير دورية ترسل للإدارة التنفيذية لضمان الشفافية والنجاح والحصول منها على ردود حول التوافق الاستراتجي. وتتنوع هذه البيانات من شرح التقدم في المشاريع وحتى عرض أيّة مخاطر جديدة قد تؤثر على أحد خطوط الإنتاج في المنظمة.

بالإضافة لفوائد هذا التواصل المستمر في بناء تعاون مشترك على مستوى المنظمة فإنه يساعد أيضاً في زيادة الوعي والحس بالمسؤولية تجاه مواضيع أمن المعلومات. وتمتد الجهود المبذولة لتحقيق التوافق مع توجهات الأعمال لتأخذ بعَين الاعتبار موائَمة حلول أمن المعلومات المقترحة مع مبادرات الأعمال الحالية والمخططة ويجب مراعاة العمليات الحالية القائمة ضمن المنظمة، الكلف اللازمة، ثقافة المؤسسة، الحوكمة المتبعة، التقنيات المستخدمة وبنية المنظمة أثناء ذلك.

٢. إدارة المخاطر

تُعد إدارة المخاطر المتعلقة بأمن المعلومات من المسؤوليات الرئيسية لمدير أمن المعلومات. ويُبنى تحليل المخاطر على متطلبات الأعمال ضمن المنظمة وعلى فهم عميق للعمليات والتقنيات والثقافة ضمن المنظمة.

ولتحقيق إدارة مخاطر فعّالة يجب الوصول لفهم متكامل للتهديدات والثغرات التي تواجهها المنظمة بالإضافة إلى سجل المخاطر ومستوى الخطر المقبول بالنسبة لها. وبكل الأحوال فإن المخاطر التي تتعرض لها أية منظمة تكون متغيرة باستمرار لذلك فمن الأهمية بمكان تفعيل عملية إدارة مخاطر مستمرة أثناء كافة مراحل تطوير برنامج أمن المعلومات.

وتُظهِر تقارير المخاطر على الاقتصاد العالمي التي يُصدِرها سنوياً المنتدى الاقتصادي العالمي نمواً متزايداً للمخاطر المتعلقة بالتكنولوجيا وخاصة منها قضايا الأمن المعلوماتي حيث تحتل مرتبة من المخاطر العشرة الأعلى التي تُهدّد الاقتصاد العالمي كما هو موضح في الشكل التالي:

الشكل (٦) موقع المخاطر المتعلقة بالتكنولوجيا على الاقتصاد العالمي

المصدر: The Global Risks Report 2021 16th Edition (published by the World Economic Forum)

٣. القيمة المكتسبة

حيث يجب الحصول على مستوى من أمن معلومات يحقق الفعالية والكفاءة المطلوبة. ويجب إدارة الاستثمارات في أمن المعلومات لتحسين الدعم المقدم نحو تحقيق أهداف الأعمال عن طريق تقديم قيمة مضافة واضحة للمنظمة. ولا يمكن لإدارة أمن المعلومات البقاء في وضع ساكن بل ينبغي التحرك باستمرار لتطوير ثقافة أمن المعلومات باتجاه التحسين المستمر.

٤. إدارة الموارد

تتضمن الموارد المستخدمة في تطوير وإدارة برنامج الأمن كلاً من الأشخاص والتقنيات والعمليات.

وأحد المبادئ المُهمَة في إدارة الموارد يتم تحقيقه عن طريق جمع المعارف وجعلها متاحة لهؤلاء الذين بحاجة لها.

٥. قياس الأداء

ينبغي أن تحدد استراتيجية أمن المعلومات المُطَوَرة طيف واسع من متطلبات المُراقبة والقياس بهدف المتابعة المستمرة للتقدم في تحقيق الأهداف وإجراء التغييرات المطلوبة لتلافي أية أخطاء أو ثغرات ويسمح ذلك للمدققين المستقلين بالتأكد من أن برنامج أمن المعلومات في وضعه الصحيح ويخضع لإدارة فعّالة.

٦. التكامل مع إجراءات الضمان الأخرى

من المهم لمدير أمن المعلومات أن يكون لديه معرفة وتَفهُّم لوظائف الضمان الأخرى في المؤسسة لأنها بدون شك ستؤثر على برنامج أمن المعلومات بشكل أو بآخر. قد تتضمن هذه الوظائف: الأمن المادي (الفيزيائي)، إدارة المخاطر، ضمان الجودة، التدقيق، إدارة التغيير، التأمين، الموارد البشرية، استمرارية العمل، الاستعادة من الكوارث وغيرها..

لذلك يجب تطوير صيغة علاقات رسمية مع مزودي الضمان الآخرين في المنظمة لخلق نوع من التكامل في النشاطات مع نشاطات أمن المعلومات ولتفادي التكرار في النشاطات ذات الأهداف المتقاربة أو المتشابهة.

٤,٥,١,٢. أهداف برنامج أمن المعلومات

يَهدُف برنامج أمن المعلومات إلى تطبيق الاستراتيجية بأفضل طريقة فعّالة من حيث التكلفة مع تعظيم الدَّعم المُقدَم لوظائف الأعمال وتقليل الانقطاعات للحد الأدنى.

عندما يتم تطوير الاستراتيجية بالشكل الأمثل فإن تحويلها لواقع يصبح مجرد تنفيذ سلسلة من المهام والمشاريع. ومع ذلك هناك عناصر يجب أن تُعدَّل طوال مراحل البرنامج وذلك لأسباب عديدة مثل حدوث تغيُّر في متطلبات الأعمال، تعديلات في البنية التحتية أو في التقنيات أو في مستوى الخطر. وقد يكون نتيجة توافر حل أفضل من الحل المقترح سابقاً ولم يكن متاحاً من قبل في وقت ما من مراحل تطوُّر البرنامج. وربما يكون للممانعة غير المتوقعة من قبل هؤلاء المتأثرين بالتغيير أثراً في إجراء التعديلات أحياناً.

ومن الأساسي أن يتم تحديد القوى التي تقود احتياجات الأعمال لأمن المعلومات ضمن المنظمة حيث من الممكن أن يكون الدَّافع لذلك:

- الحاجة المتزايدة لمتطلبات الالتزام بالتشريعات
- تواتُر متزايد وخسائر جرَّاء حصول حوادث أمن معلومات
- هواجس حول تضرر سمعة المنظمة

- نمو في المتطلبات التجارية مثل استخدام بطاقات الدفع (Payment Card Industry)
- تزايد في الأخطار المتعلقة بالعمليات الإنتاجية

إن تحديد الدافع سوف يوضّح أهداف برنامج أمن المعلومات ويعطي أسس تطويره ومراقبته. عند تحديد أهداف البرنامج بوضوح يصبح الغرض من نشاطات البرنامج هو أن يتم إنشاء العمليات والمشاريع التي تَردُم الفجوة بين الوضع الراهن والوضع المأمول. وحتى لو كان هناك برنامج مطبَّق مسبقاً أو لم يكن فهناك مجموعة من الأسُس يجب أن تُبنَى لدعم نشاطات البرنامج والتأكد من فعاليتها وتكون الخطوة الأولى لذلك دوماً هي تحديد أهداف الإدارة لأمن المعلومات وإنشاء مؤشرات واضحة تعكس هذه الأهداف (Key Goal Indicators) ثم تطوير آليات القياس للتَحَقُّق فيما إذا كان البرنامج يمضي بالاتجاه الصحيح لتحقيق هذه الأهداف أو لا.

٥,٥,١,٢. الموارد التقنية لبرنامج أمن المعلومات

يتضمن برنامج أمن المعلومات في معظم الحالات طيف واسع من التقنيات (بالإضافة إلى السياسات/الإجراءات والموارد البشرية). ويجب أن يتم اتخاذ القرارات بشأن اختيار المناسب من هذه التقنيات والقابل للاستخدام منها بما يتوافق مع أهداف البرنامج واحتياجات المنظمة. فيما يلي عيّنة من التقنيات الحالية المرتبطة مباشرة بأمن المعلومات:

- الجُدران النارية (Firewalls)
- تقنيات النسخ الاحتياطي والأرشفة (مثل Redundant array for inexpensive disks (RAID)
- أنظمة مكافحة الفايروسات الحاسوبية (Antivirus software)
- وظائف أمن المعلومات المضافة للأجهزة الشبكية (مثل switches،routers)
- أنظمة كشف التسلّل (Intrusion detection systems)
- أنظمة منع التسلّل (Intrusion preventing systems)
- تقنيات التشفير (مثل public key infrastructure PKI، advanced encryption standard AEC)
- التوقيع الرقمي
- البطاقات الذكيّة
- آليات المصادَقَة (authentication) والتخويل (authorization) مثل:
  multi factor authentication، biometrics، One Time Password OTP
- طرق حماية البث اللاسلكي (wireless)
- الحوسبة والأجهزة المتنقلة (mobile computing and devices)

- طرق حماية التطبيقات (application)
- طرق الوصول عن بعد (مثل virtual private network VPN)
- أساليب الحماية عبر الإنترنت
- أدوات جمع وتحليل سجلات المراقبة (مثل security information and event management SIEM)
- أدوات المسح عن الثغرات وفحص الاختراق (vulnerability scanning and penetration testing)
- تقنيات وأساليب منع تسريب المعلومات (data leak prevention DLP)
- أنظمة إدارة الدخول وتحديد الهوية (identity and access management systems)

تُعتبَر معظم التقنيات أعلاه مرتبطة بشكل مباشر بأمن المعلومات إلا أنه يجب الاعتراف –على الأقل نظرياً– بأن كل التقنيات المطبَّقة في المنظمة بمختلف أشكالها لها علاقة ما بأمن المعلومات ضمنياً.

٦,٥,١,٢. نطاق برنامج أمن المعلومات

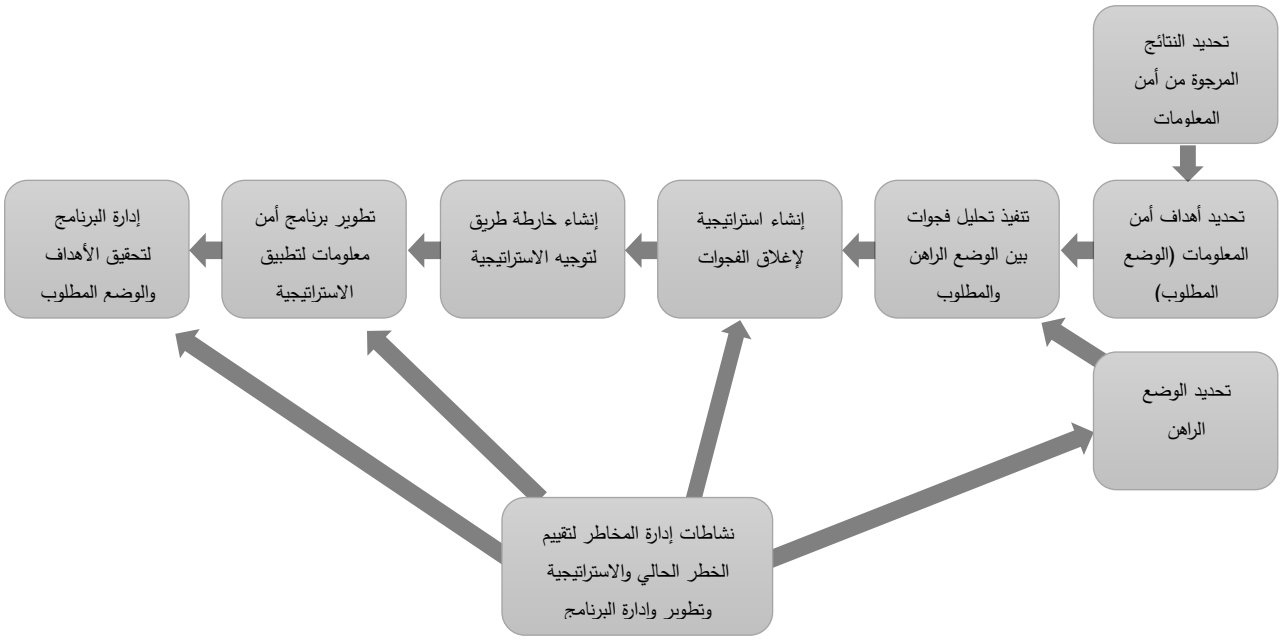
سواء كانت نقطة الانطلاق تتطلب تشكيل برنامج أمن معلومات جديد أو أن هناك برنامج مسبق مطلوب استكماله فيجب أخذ عدة قضايا مهمة بعين الاعتبار. من أهم هذه النقاط هو تحديد نطاق عمل ومسؤولية وميثاق برنامج أمن المعلومات. للأسف فإنه من النّادر أن نجد هذه العناصر مُعرَّفة ومُوثَّقة بشكل واضح مما يؤدي إلى صعوبة في تحديد من يُدير ماذا أو مدى ملائمة وظائف أمن المعلومات لأهداف المنظمة.

لذلك فعلى مدير أمن المعلومات أن يبدأ عمله الجديد ببذل جهود استقصائية للحصول على فهم جيّد من المعنيين حول التوقعات، المسؤوليات، نطاق العمل، الصلاحيات، الميزانيات، متطلبات البلاغات،.. وسيكون من المفيد جداً توثيق هذه المعطيات والحصول على تفاهم مع الإدارة حولها.

وفيما يتعلق بالسلسلة الإدارية ينبغي فهم هيكلية المنظمة وأين تقع وظائف أمن المعلومات ضمن هذه الهيكلية. في العديد من الحالات يُمكن أن يكون هناك هيكلية إدارية متوارثَة ومتعارِضة قد تؤدي لظهور تضارب في المصالح، وهنا ينبغي مناقشة ذلك مع الإدارة والاتّفاق حول آليات التعامل مع هذا الوضع. عادة ما يُعتبر قسم أمن المعلومات على أنه من الوظائف التنظيمية وقدرته على العمل بشكل فعّال يتعارض مع كونه تابعاً لوظائف من المفترض أن يكون رقيباً عليها. ومع وجود بعض الاستثناءات، فإن مدير أمن المعلومات التابع لإدارة التكنولوجيا أو أي إدارة تشغيلية أخرى ستكون قدراته على توفير وظيفة أمن معلومات فعّالة على مستوى المنظمة محدودة جداً.

وتتوقف فعالية إدارة أمن المعلومات في بعض المنظمات على ثقافة المنظمة ومدى فهم مدير أمن المعلومات لهذه الثقافة. وغالباً ما تتعلق وظيفة الأمن بالقوى المُتَفاعلة داخل المنظمة لذلك فنجاحها يعتمد بشكل كبير على بناء علاقات صحيحة مع مختلف الأطراف، فغالباً ما يرتبط نجاح العمل في المنظمات بقوة تأثير العلاقات أكثر من ارتباطه بمواثيق العمل المكتوبة. يبين الشكل التالي الخطوات اللازمة لتطوير برنامج أمن معلومات باختصار:

الشكل (٧) خطوات تطوير برنامج أمن المعلومات



المصدر: ISACA: CISM Review Manual 14th Edition

يُبنى نطاق برنامج أمن المعلومات عن طريق تطوير استراتيجية المنظمة المتعلقة به وربطها بمسؤوليات إدارة المخاطر ويحدِد ميثاق البرنامج مدى دعم كل إدارة ضمن المنظمة نشاطات تطبيق هذا البرنامج.

إن تطبيق برنامج أمن المعلومات لا بد أن يغيّر في طريقة المنظمة في عملها الأشياء. ويجب أن يسعى مدير أمن المعلومات ضمن بُنية الموظفين والإجراءات والتقنيات الموجودة على دمج التغييرات ضمن الاجراءات والسياسات المعمول بها مسبقاً، ولا شك أن هذا سيوَلد درجة ما من المُمانعة للتغيير وهذا ما يجب توقعه والتخطيط له.

فيما يلي مثال على وصف برنامج أمن معلومات ناضج يمكن الاعتماد عليه كأساس للاستراتيجية ويساعد في تحديد النطاق والميثاق لبرنامج أمن المعلومات:

" أمن المعلومات هي مسؤولية مشتركة من قبل إدارات الأعمال والتكنولوجيا وأمن المعلومات، وهو يتكامل مع أهداف المنظمة التشغيلية. إن متطلبات أمن المعلومات قد تم تحديدها بوضوح وتحسينها

وجمعها ضمن خطة أمن مُعتمَدة. تتكامل وظائف أمن المعلومات مع التطبيقات في مراحل التصميم، ويجب التركيز على إعطاء المستخدمين النهائيين دوراً متزايداً في إدارة الأمن. تُعطي تقارير وإبلاغات أمن المعلومات إنذاراً مبكراً حول التغييرات أو أية مستجدات بالمخاطر باستخدام أساليب مراقبة آلية فعّالة للأنظمة الحساسة. يتم التعامل مع الحوادث وفق إجراء الاستجابة المُعتمَد لها مدعوماً بمجموعة أدوات آلية. يتم تنفيذ تقييم أمني دوري لتحديد فعّالية تطبيق الخطة الأمنية. يتم جمع معلومات عن التهديدات والثغرات الأمنية الجديدة بشكل آلي ويتم التواصل بشأن الضوابط المناسبة اللازم تطبيقها. يُعتبر فحص الاختراق وتحليل السبب الجذري للحوادث وتحديد المخاطر بشكل مُسبق هي أساسيات التحسين المستمر. تتكامل عمليات وتقنيات أمن المعلومات على مستوى المنظمة ككل ".

(المصدر: ISACA, CISM Review Manual 14th Edition)

٧,٥,١,٢. إطار عمل برنامج أمن المعلومات

مع التطور الكبير في قطاع الأعمال أصبح العالم الآن يتجه نحو توفير بيئة عمل فيها العديد من التقنيات الحديثة، مثل: منصَّات التواصل الاجتماعي والحوسبَة السَحابية وتقنيات تحليل البيانات، ومع زيادة هذا التطور الذي يؤدي من جانب إلى زيادة معدّل نجاح الأعمال، لكنه من جانب آخر يُشير إلى مخاوف ومخاطر أُخرى تتعلق بكيفية الإدارة والحوكمة لتقنية المعلومات، مما دفع إلى ظهور حاجة لحلول جذرية لسيناريوهات مخاطر تقنية المعلومات. لهذا السبب تم إنشاء مجموعة من أُطر العمل المعياريّة كحل فعّال يُساعد على تسهيل عملية حوكمة تقنية المعلومات في الشركات والمُنشآت. ويوجد اليوم أكثر من إطار عمل يمكن أن يتم استخدامه لتطوير برنامج أمن المعلومات ومن أكثرها شيوعاً واستخداماً على مستوى العالم COBIT 5 و ISO/IEC 27001 وفيما يلي شرح مختصر عن كل منها:

١,٧,٥,١,٢. إطار عمل COBIT 5

هو إطار عمل تم إنشاؤه بواسطة منظمة التدقيق والرقابة على نُظم المعلومات (ISACA) يُستخدم لإدارة وحوكمة تقنية المعلومات داخل المؤسسات، حيث تُعتبر الحوكمة الفعّالة لِتقنية المعلومات أمر بالغ الأهمية وأساس نجاح الأعمال.

يُعرّف إطار العمل COBIT (Control Objectives for Information and Related Technology) بأنه إطار حوكمة تقنية المعلومات المُعترَف به دولياً، ويُسمّى أيضاً الإطار/ النموذج المرجعي للأمن ولضمان استغلال تقنية المعلومات بالشكل الأمثل، يُستخدم لتحسين أداء الأعمال بإطار متوازن ولخلق قيمة لتقنية المعلومات وخفض المخاطر المحتملة منها.

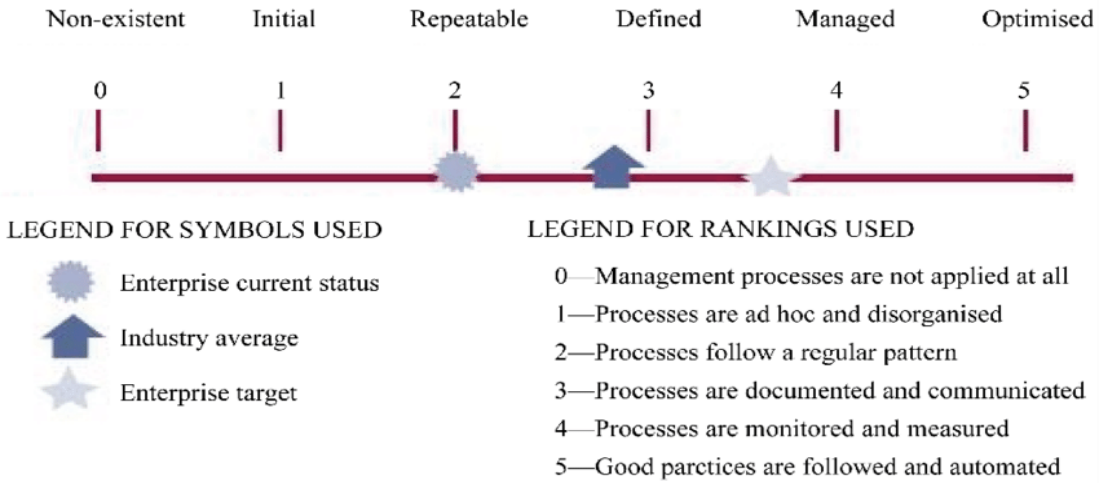
يتكون هذا الإطار من مجموعة من الممارسات والعمليات الراسخة والمقبولة (مع كل عملية يتم تحديد المُدخَلات والمُخرجات للعملية، وأنشطة العملية الرئيسية، وأهداف العملية، ومقاييس الأداء، ونموذج

نضج القدرة) لتضمن أن تقنية المعلومات المستخدمة داخل المُنشآت تُغطّي أهداف العمل، وأنَّ الموارد تُستخدم بشكل جيد، وأنَّ المخاطر يتم رصدها بشكل كافٍ.

مكونات إطار العمل COBIT :

١. الإطار :(Framework) يعمل على تنظيم عملية حوكمة تكنولوجيا المعلومات وتقديم أفضل الممارسات الجيدة حسب مجالات تكنولوجيا المعلومات المختلفة وربطها باحتياجات الأعمال.
٢. التعريفات وأوصاف العمليات :(Process objectives) يُقدِم نموذج مرجعي ولغة مشتركة لكل فرد في المنشأة، وتتضمن أوصاف العمليات ومجالات المسؤولية (من تخطيط، وبناء، وتشغيل، ومراقبة) لجميع عمليات تقنية المعلومات.
٣. أهداف التحكم :(Control objectives) تُوفّر مجموعة كاملة من المتطلبات عالية المستوى التي يجب أن تنظر فيها الإدارة للتحكّم الفعّال في كل عملية.
٤. إرشادات الإدارة :(Management guidelines) تُساعد في تحديد المسؤوليات بشكل أفضل، والاتفاق على الأهداف المشتركة، وقياس الأداء، وتوضيح العلاقة المتبادلة مع العمليات الأخرى.
٥. نماذج النضج (Maturity models): تعمل على تقييم نُضج القدرة لكل عملية وتساعد على معالجة الفجوات بينها. يتألف هذا النموذج من مستويات ما بين الصفر والخمسة تُحدَّد اعتماداً على درجة نضوج عمليات أمن المعلومات في المنظمة كما في الشكل التالي:

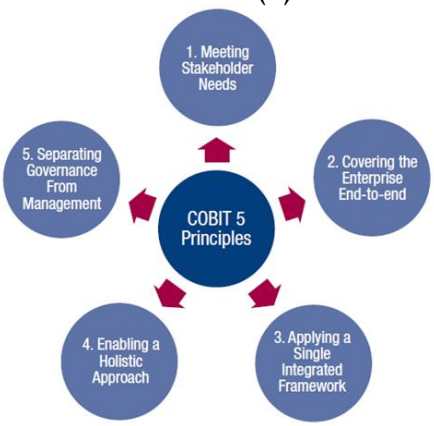
الشكل (٨) نموذج نضج القدرة



المصدر: ISACA, COBIT 5, USA, 2012

مبادئ إطار العمل COBIT 5 :

الشكل (٩) مبادئ COBIT 5



المصدر: ISACA, COBIT 5, USA, 2012

لبناء نظام إدارة وحوكمة تقنية المعلومات فعّال داخل المُنشآت، يجب مراعاة الأسلوب الذي يتَّبِعه إطار كوبت (COBIT 5) لإدارة تقنية المعلومات، ويعتَمِد على خمسة مبادئ أساسية وهي:

١. يعمل إطار COBIT على تلبية احتياجات أصحاب المصلحة: المبدأ الأول هو الأهم، فهو يساعد على تحديد أصحاب المصلحة الرئيسيين وتلبية احتياجاتهم ومتطلباتهم عن طريق إجراء تحليل مناسب لاحتياجات أصحاب المصلحة وتقديم الفوائد المناسبة لهم في الوقت المناسب. يعمل إطار COBIT على ترجمة احتياجات أصحاب العمل إلى أهداف محددة قابلة للتنفيذ ومخصصة في سياق الأهداف المتعلقة باستغلال تقنية المعلومات والأهداف التمكينية وأهداف المؤسسة. إذ أنَّ تلبية احتياجات أصحاب العمل يتطلّب إنشاء نظام إدارة وحوكمة لأصول تقنية المعلومات داخل المُنشأة، حيث يتم طرح الأسئلة التالية قبل اتّخاذ كل قرار:

- لِمَن المنافع أو من هم المستفيدون؟
- من يتحمل المخاطر أو من يتحمل المسؤولية عن المخاطر التي تنطوي عليها؟
- ما هي الموارد المطلوبة لضمان تلبية المتطلبات بسلاسة؟

٢. تغطية المنشآت من البداية إلى النهاية: ينص إطار عمل COBIT على أنه يجب على الإطار تغطية المنشأة بأكملها من البداية إلى النهاية حتى تتمكن من إدارة وتشغيل كل قسم بنفس المستوى، وتتم معالجة جميع خدمات تقنية المعلومات الداخلية والخارجية ذات الصلة، ومعالجة العمليات التجارية الداخلية والخارجية.

٣. تطبيق إطار واحد متكامل: يُعتبر إطار العمل COBIT بأنه إطار عمل متكامل للأسباب التالية:

- القدرة على التوافق أو الاندماج مع أحدث الأُطر والمعايير ذات الصلة، مثل:

CMMI, Prince 2, TOGAF ،ISO 27001, ISO 38500, ITIL، ISO 31000, ISO 9001…

- يعتبر وسيلة شاملة لتغطية المنشأة بشكل متكامل مع إطار الإدارة والحوكمة.
- يوفر أساس قوي لدمج الأُطر والمعايير والممارسات الأُخرى بشكل فعّال لجعل عمل المُنشأة يحقق آفاق جديدة.
- يدمج المعرفة عبر الأُطر الإدارية المختلفة لتقنية المعلومات.
- يوفّر بنية بسيطة لهيكلية عناصر التوجيه وإنتاج مجموعة منتجات متّسقة.

٤. تمكين نهج شمولي: يهتم هذا المبدأ بتمكين نهج شامل في العمل التنظيمي، بمعنى أن تعمل المنشأة بأكملها كوحدة واحدة. ويعمل الإطار على دمج حوكمة تقنية المعلومات في المنشاة مع حوكمة المنشآت، لأن جميع أجزاء أي مشروع تكون مرتبطة ببعضها، وهذا يعني أن أي نوع من المشكلات في أي قسم قد يؤدي إلى حدوث مشاكل في القسم الآخر.

٥. فصل التحكم عن الإدارة: يعمل إطار COBIT على التمييز الواضح بين الحوكمة والإدارة، حيث يُطلب من كل قِسْم أنواع مختلفة من الأنشطة، وتتطلب أيضاً هياكل تنظيمية مختلفة تخدم أغراض مختلفة. يهتم COBIT بتحديد اتجاه المنشأة من خلال تحديد الأولويات، وآلية اتخاذ القرار، بالإضافة إلى مراقبة الامتثال ومدى التقدُّم مقابل الأهداف والاتجاهات الثابتة، والتخطيط للأنشطة المختلفة ومراقبتها وإدارتها بما يتناسب ويتماشى مع الاتجاه الذي حددته هيئة الحوكمة لتحقيق أهداف المنشأة.

عوامل تمكين إطار (COBIT):

يعتمد COBIT بشكل كامل على مجموعة شاملة تتكون من سبعة عوامل تمكين تعمَل على تحسين الاستثمار في تقنية المعلومات واستخدامها لصالح جميع أصحاب العمل، وهي:

- الأشخاص والسياسات والأُطر.
- العمليات.
- الهياكل التنظيمية.
- الثقافة والأخلاق والسلوك.
- المعلومات.
- الخدمات والبُنية التحتية والتطبيقات.
- المهارات والكفاءات.

٢,٧,٥,١,٢. إطار عمل إدارة أمن المعلومات ISO 27001

يُعتبر معيار الآيزو (ISO/IEC 27001:2013) المعيار الدّولي الذي يوضح كيفية وضع نظام إدارة أمن المعلومات بشكل مُعتَمد وتطبيقه والحفاظ عليه وتحسينه باستمرار ضمن أُطر عمليَّة مما يسمح بالحفاظ على البيانات الحساسة والسرية بشكل آمن والتقليل من احتمال الوصول إليها بشكل غير قانوني أو بدون إذن كما يسمح بإدارة المخاطر الأمنية واسترداد المعلومات وتقليل الخروقات الأمنية والتأكد من وجود نظام أمن معلومات يؤدي المهام بكفاءة ويُتابِع مستويات الحماية الخاصة بالمنظمة من خلال:

- إدارة الأعطال الأمنية.
- حماية أصول المنظمة.

- السماح بتبادل آمن للمعلومات.
- الحفاظ على سلامة المعلومات السّرية.
- تقديم الخدمات بشكل ثابت ومستقر.
- تزويد المؤسسة بخاصية تنافسية.

إن اعتماد نظام الآيزو سواء للحصول على الشهادة أو تطبيقه في المنظمة كأفضل مُمارسة سيعود على المنظمة بفوائد عديدة أهمُّها:

- إدارة وتقليل تأثير المخاطر المتعلقة بالأصول المعلوماتية من خلال تصميم أفضل الضوابط الأمنية الداخلية وأكثرها ملاءَمة لبيئة الأعمال.
- حماية المنظمة وحماية أصول المستفيدين والموردين والمحافظة على أمن المعلومات السرية.
- ضمان استمرارية الأعمال بشكل آمن في حالات الأزمات.
- تزويد العملاء وأصحاب المصلحة بالثقة في كيفية إدارة المخاطر المرتبطة بالأصول المعلوماتية.

يوجد في الإصدار الأخير من هذا المعيار ١١٤ ضابط تحكم موزعة ضمن ١٤ فقرة (يبدأ ترقيمها من A.5 وحتى A.18 لتكون متوافقة مع الترقيم في المعيار ISO/IEC 27002:2013 الذي يُعطي إرشادات لمعايير أمن المعلومات التنظيمية وممارسات إدارة أمن المعلومات) كما يلي:

١. A.5 سياسات أمن المعلومات (٢ ضابط)
٢. A.6 تنظيم أمن المعلومات (٧ ضابط)
٣. A.7 أمن الموارد البشرية (٦ ضابط)
٤. A.8 إدارة الأصول (١٠ ضابط)
٥. A.9 التحكم في الوصول (١٤ ضابط)
٦. A.10 التشفير (٢ ضابط)
٧. A.11 الأمن المادي والبيئي المحيطة (١٥ ضابط)
٨. A.12 أمن العمليَّات (١٤ ضابط)
٩. A.13 أمن الاتصالات (٧ ضابط)
١٠. A.14 الاستحواذ على النظام وتطويره وصيانته (١٣ ضابط)
١١. A.15 العلاقة مع الموردين (٥ ضابط)
١٢. A.16 إدارة حوادث أمن المعلومات (٧ ضابط)
١٣. A.17 جوانب أمن المعلومات لإدارة استمراريَّة الأعمال (٤ ضابط)
١٤. A.18 الامتثال مع المتطلبات الداخلية، السياسات والمتطلبات الخارجية، القوانين (٨ ضابط)

سلسلة معايير ISO27k

نظراً لأن ISO 27001 يُحدِّد متطلبات نظام إدارة أمن المعلومات (ISMS)، فإنه يُعتبَر المعيار الرئيسي في مجموعة معايير ISO 27000 وهو يُعرِّف بشكل أساسي ما هو مطلوب لتطبيق النظام، وليس كيفية القيام بتطبيق النظام وتفعيله داخل المنظمة، ولذلك فقد تم تطوير العديد من معايير أمان المعلومات الأخرى لتوفير إرشادات إضافية. ويوجد حالياً أكثر من ٤٠ معياراً في سلسلة ISO27k من أكثرها شيوعاً:

- ISO/IEC 27000 يوفّر المصطَلَحات والتعريفات المستخدَمة في سلسلة معايير ISO27k
- معيار ISO/IEC 27002 يوفّر إرشادات وتفاصيل مهمّة لتنفيذ الضوابط المُدرَجة في "الملحق A" لمعيار ISO 27001
- معيار ISO/IEC 27004 يوفّر إرشادات لقياس أمن المعلومات في المنظّمة، بالإضافة إلى كونه يشرح كيفية تحديد ما إذا كان نظام إدارة أمن المعلومات يُحقّق الأهداف المرجوَّة منه.
- معيار ISO/IEC 27005 يوفّر إرشادات لإدارة مخاطر أمن المعلومات، ويُعتبر مكمّل جيد لمعيار ISO 27001 لأنه يقدم تفاصيل حول كيفية إجراء تقييم المخاطر ومعالجة المخاطر، والتي ربما تكون أصعب مرحلة في التنفيذ.
- معيار ISO/IEC 27017 يوفّر إرشادات لأمن المعلومات في البيئات السحابية.
- معيار ISO/IEC 27018 يوفّر إرشادات لحماية الخصوصية في البيئات السحابية.
- ISO/IEC 27031 هذا المعيار هو رابط كبير بين أمن المعلومات وممارسات استمرارية الأعمال.

يُعَد إطار إدارة أمن المعلومات التمثيل المبدئي لبنية إدارة أمن المعلومات في المنظمة ويجب أن يُحدِد العناصر التقنية والتشغيلية والإشرافية والإدارية للبرنامج. كما يُركّز الإطار الفعّال على بعض الاحتياجات قصيرة المدى كحاجة مُتَّخذي القرار في المنظمة لشرح حول المخاطر وطرق تخفيفها والتي من الممكن أن تكون متعلقة ببعض نشاطاتها مثل الاستضافة الخارجية (السَحَابيّة) لنظام معلوماتي ما.

٨,٥,١,٢. نشاطات إدارة وتنظيم برنامج أمن المعلومات

تتضمَّن إدارة برنامج أمن المعلومات نشاطات التوجيه والإشراف والمراقبة المتعلقة بأمن المعلومات لدعم أهداف المنظمة. والإدارة هي عملية تحقيق أهداف المنظمة عن طريق دمج الموارد البشرية والمادية والمالية بالشكل الأمثل مع العمليات والتقنيات واتّخاذ أفضل القرارات لصالح المنظمة آخذين بالاعتبار بيئتها التشغيلية. تتضمن الإدارة المُستمرة للبرنامج نشاطات متعددة مثل:

- متابعة أداء الموظفين وتنظيم الوقت والاحتفاظ بالسجلات
- الاستخدام الأمثل للموارد
- الشراء / الاستحواذ
- إدارة المخزون
- تتبع ومراقبة وإدارة المشاريع
- تطوّر برنامج التوعية
- الإدارة المالية والميزانية وضبط الأصول
- إدارة الأشخاص والعلاقة مع الموارد البشرية
- إدارة العمليات التشغيلية وتسليم الخدمات
- تطبيق ومراقبة مؤشرات القياس والتقارير
- إدارة دورة حياة عناصر تقانة المعلومات

كما يوجد العديد من المتطلبات التقنيّة والتشغيلية أيضاً مثل:

- إدارة مفاتيح التشفير
- مراقبة ومراجعة سجلات التشغيل
- الإشراف على طلبات التغيير ومراقبتها
- الإشراف على الإعدادات والتحديثات ومراجعتها
- مسح الثغرات
- مراقبة التهديدات
- مراقبة الالتزام
- فحص الاختراق

حيث يتم باستخدام الأسلوب المناسب مناقشة مخاطر أمن المعلومات مع مختلف الأقسام ضمن المنظمة واقتراح الحلول التي تُراعي كلاً من المتطلبات الأمنية والتأثير الأقل على النشاطات التشغيلية للمنظمة.

فيما يلي الأبعاد المُهمّة التي يجب مراعاتَها في إدارة برنامج أمن المعلومات:

١,٨,٥,١,٢. شؤون الموظفين، الأدوار، المهارات والثقافة

يُمكن أن يتضمّن فريق العمل في برنامج أمن المعلومات مهندسي أمن معلومات، مختصين بضمَان الجودة والاختبار، مدراء الوصول، مدراء مشاريع، منسقي التزام، مختصين بِبُنى أمن المعلومات، منسقي توعية، ومختصين بالسياسات. ويجب أن تكون المسؤوليات موضحة لكل دور من الوظائف التي يتم إسنادها لضمان التطبيق الفعّال.

ومن المهم فهم مهارات الأشخاص المتاحين في الفريق للمساعدة في وضعهم ضمن المهام الصحيحة المناسبة لقدراتهم ضمن البرنامج. ويمكن الحصول على بعض المهارات غير المتوفرة عن طريق تدريب الفريق الحالي أو الاستعانة بموارد خارجية (والتي قد تكون أكثر جدوى في حالات الحصول على استشارات تخصصية لفترة محدودة أو لمشاريع صغيرة). ويجب أن يتم تجهيز اتفاقيات توظيف رسمية وفق المسؤوليات المسندة لكل موظف خلال بداية عملية التوظيف.

تعكس الثقافة سلوك المنظمة وتوجهاتها ومستويات التأثير الرسمية وغير الرسمية في بنية أداء الأعمال، السلوك، الأعراف، درجة نُضج العمل الجماعي، ووجود أو عدم وجود روح المنافسة. وتتأثر الثقافة بخلفيات الأفراد، أخلاقيات العمل، القيم، الخبرات السابقة، ومعتقداتهم في الحياة التي يُحضِرونَها معهم لمكان العمل. ولكل منظمة ثقافة معينة بغض النظر فيما إذا كان قد تم تصميمها وبناؤها بشكل متعمَّد أو بُنيَت ببساطة نتيجة التراكمات الإدارية عبر الزمن.

وبما أن دور أمن المعلومات متشعّب ضمن كل المنظمة ويحتاج لبناء علاقات مع مختلف الأقسام لذلك يجب التأسيس لثقافة أمن معلومات تحترم أدوار كل الموظفين الذين يؤدُّون مهامهم مع مراعاة حماية الأصول التي يعملون بها. وعلى كل موظف مهما كان موقعه أن يَعِي كيف ترتبط مهام أمن المعلومات بدورِه في المنظمة. للوصول لذلك ينبغي التركيز على تحسين التواصل والمشاركة ضمن اللّجان والمشاريع بفعالية وإعطاء الاهتمام الضروري للمستخدمين النهائيين.

٢,٨,٥,١,٢. التثقيف والتوعية والتدريب بأمن المعلومات

لا يمكن التعامل مع المخاطر المتوارَثَة الناتجة عن استخدام أنظمة المعلومات المختلفة عن طريق الآليات التقنية البحتة. يُساهم برنامج التوعيّة الفعّال في الحد الكبير من المخاطر عن طريق استهداف عنصر السُلوك الأمني لدى الأشخاص. يجب أن يركّز برنامج التوعية على المخاوف الأمنية الشائعة للمستخدمين مثل اختيار كلمات المرور، الاستخدام المناسب للموارد التقنية، أمان البريد الإلكتروني وتصفح الإنترنت، وأساليب الهندسة الاجتماعية ويجب تخصيص كل برنامج توعية لمجموعة معينة مع الأخذ بالاعتبار أن المستخدم النهائي هو خط الاكتشاف الأول للتهديدات التي قد لا تكون قابلة للاكتشاف عن طريق الأنظمة الأمنية التقنية مثل أساليب الاحتيال والهندسة الاجتماعية.

٣,٨,٥,١,٢. التوثيق

يُعتبر التوثيق من المهام الإشرافية الضرورية المرافقة لبرنامج أمن المعلومات. ويجب أن تسند كل وثيقة لمالك معين يكون مسؤولاً عن تعديلاتها. ومن المهم اعتماد إصدارات متعددة لكل وثيقة للتأكد

من أن الجميع يستخدم الإصدار الصحيح مع وجود آلية للنشر وإبلاغ أصحاب العلاقة بأية إصدارات جديدة. وينبغي تطبيق إجراء واضح للإضافة أو التعديل أو حتى إتلاف الوثائق المرتبطة بالبرنامج.

٤,٨,٥,١,٢. تقدم البرنامج وإدارة المشاريع

إن تحقيق أهداف البرنامج للانتقال من الوضع الراهن للوضع المُستَهدف لزيادة درجة الأمن والحصول على مستوى مقبول من المخاطر يتطلَّب تنفيذ العديد من المشاريع التي تساعد في التقدم ضمن البرنامج. يجب أن تتم مراجعة المشاريع الضرورية لردم هذه الفجوة بشكل دقيق، حيث أن العديد من هذه المشاريع سيكون لتطبيق تقنيات جديدة أو لمراجعة وتعديل إعدادات الأنظمة المستخدمة. وينبغي التأكيد على أن يكون لكل من هذه المشاريع وقت مُحدَد وميزانية ونتائج قابلة للقياس لتحقيق زيادة في المستوى الأمني مع مراعاة عدم تأثيرها على المستوى الأمني سلبياً لجوانب أخرى ضمن المنظمة.

كما ينبغي التعامل مع هذه المشاريع ضمن محفظة مشاريع متكاملة بحيث يتم ترتيبها وفق الأهمية مع مراعاة عدم التأخر في المشاريع المتداخلة وتخصيص الموارد اللازمة لكل منها بالشكل الأمثل ودمج نتائجها بشكل سلس ضمن العمليات التشغيلية.

٥,٨,٥,١,٢. إدارة المخاطر

تسعى كل نشاطات البرنامج نظرياً لإدارة المخاطر ضمن الحدود المقبولة، ولكن مع التغيُّر المستمر في أبعاد المخاطر فإنه من الأساسي أن تُلاحِق نشاطات أمن المعلومات هذه التغييرات وتُكيّف نفسها بالشكل المطلوب للتعامل بشكل فعّال مع الظروف الحالية. وفي الوقت الذي تُهمِل فيه بعض المنظمات الاهتمام بتأثيرات حوادث أمن المعلومات فإنه من الأساسي للبرنامج التأكد من قدرة المنظمة على الاستجابة للحوادث الأمنية التي قد تسبب انقطاعات في الأعمال التشغيلية.

٦,٨,٥,١,٢. تطوير حالات عمل (Business Case)

إن الغاية من حالات العمل هي إيجاد تبرير وأسباب للمشاريع والمهام ويجب أن تتضمن تلك الحالات العوامل التي يمكن أن تؤدي لنجاح أو فشل المشروع. ويتم عرض هذه الحالات وفق الأسلوب المتبع في كل منظمة كما يمكن أن يتم ذلك إلكترونياً عبر مستند جيد التحضير أو عرض تقديمي مناسب. وينبغي أن يتم تحديد المنافع والكلف والمخاطر ضمن كل حالة، حيث عادة ما تكون المنافع قابلة للقياس وداعمة ومتماشية مع المنظمة، ويجب الاهتمام بشكل خاص بالجانب المالي للعرض كما يجب أن يتم الإشارة للمخاطر الواقعية المرافقة لفترة حياة المشروع. ومن الأفضل تجنب الثقة الزائدة والتفاؤل المفرط والعمل على تقديم حالات واقعية تعطي نتائج ملموسة.

٧,٨,٥,١,٢. تمويل البرنامج

التمويل هو جزء أساسي من برنامج أمن المعلومات ويمكن أن يكون له تأثير كبير على نجاح البرنامج. وكما هو الحال مع نشاطات الأعمال الأخرى فإن المعرفة والتحضير العميق تعتبر من العوامل الرئيسية بالنجاح في إدارة مجريات هذا التحدي. ومن العوامل الأساسية الأخرى هو وجود استراتيجية أمن معلومات بشكل مسبق للحديث عن التمويل وكل المصاريف والنفقات يجب أن تكون مدعومة ضمن الاستراتيجية لأنها تحدد خارطة طريق واضحة للتقدم في تطبيق برنامج أمن المعلومات المتفق عليه. فوجود استراتيجية متفق عليها ومعتمدة يجب أن يَسبق الدخول في إجراءات التمويل.

وتجدر الإشارة إلى وجود بعض العناصر في برنامج أمن المعلومات التي لا يمكن التنبؤ بها والتي قد تتطلب نفقات مفاجِئة وغير مخططة خاصة أثناء الاستجابة للحوادث مثل ضرورة الاستعانة بمختصين من خارج المنظمة لتقديم استشارات خارج مهارات فريق المنظمة. في مثل هذه الحالات يمكن تخصيص ميزانية بالاعتماد على البيانات التاريخية لحالات مشابهة.

٨,٨,٥,١,٢. قواعد عامة لسياسة الاستخدام المقبول

بينما تزوِّد الإجراءات المحددة خطوات تفصيلية للعديد من الوظائف على المستوى التشغيلي فإنه لا يزال هناك مجموعة كبيرة من المستخدمين الذين قد تكون الفائدة الأكبر لهم نابِعة من الخلاصات سهلة التناول حولَ ما يجب وما لا يجب فعله للالتزام بالسياسة. ومن الطرق الفعالة لتحقيق ذلك إنشاء سياسة للاستخدام المقبول (Acceptable Use Policy) والتي يُمكن أن تُوَزَّع لكل المستخدمين ليتم بعدها التأكد من قراءتها وفهمها من قبل الجميع. وينبغي أن تُوزَّع سياسة الاستخدام المقبول لكافة الموظفين الجُدد الذين سيستخدمون موارد تكنولوجيا المعلومات.

تكون عادة القواعد التي يتم تضمينها في سياسة الاستخدام المقبول حول ضوابط الدخول، التصنيف، طرق معالجة وثائق البيانات، متطلبات الإبلاغ وقيود التصريح، وقد تتضمن قواعد حول استخدام البريد الإلكتروني والإنترنت حيث تضع الحد الأدنى من الضوابط اللازمة لتحقيق مستوى أمن المعلومات على صعيد المنظمة.

٩,٨,٥,١,٢. ممارسات إدارة مشكلات أمن المعلومات

تتطلب إدارة المشكلات أسلوب مُنظَّم لفهم أبعاد القضيّة المختلفة وتحديد المشكلة وتصميم برنامج عمل بالتوازي مع إسناد المسؤوليات وتوراي الإنجاز للحل. كما ينبغي تطبيق آلية تبليغ تضمن متابعة النتائج والتأكد من أن المشكلة قد تم حلها.

وبما أن بيئة تكنولوجيا المعلومات تتغير باستمرار في أي منظمة فإنه من الضروري متابعة ضوابط أمن المعلومات المستخدمة بشكل دائم للتأكد من أنها لا تتعرض لأيّة مشكلات نتيجة التغييرات، وهنا

يمكن استخدام بعض الضوابط البديلة ريثما يتم التأكد من حل المشكلة. على سبيل المثال عند تعرُّض أحد جدران الحماية النارية لمشكلة أدت لتوقفه عن العمل يمكن اللجوء لعزل الأنظمة المرتبطة به من الوصول للخارج حتى يتم إصلاح المشكلة لحماية المنظمة من المخاطر المحتملة. في الوقت الذي تمَّت فيه حماية المنظمة في هذا المثال فإن الإجراء المُتَّخذ أثَّر بنفس الوقت على تنفيذ المنظمة لأعمالها لذلك فمن الضروري منح الصلاحيات الملائمة لمثل هذه الحالات من قبل الإدارة.

١٠,٨,٥,١,٢. إدارة الموردين

تُعتبر الإدارة والمراقبة المستمرة للموردين الخارجيين للبرمجيات والتجهيزات والخدمات الأخرى من المسؤوليات الرئيسية لأمن المعلومات. ومن الشائع جداً حالياً أن يتم الاستعانة بموردين خارجيين أيضاً لتنفيذ أو تشغيل وظائف مرتبطة بأمن المعلومات، ويخلق استخدام جهات خارجية لتزويد خدمات متعلقة بأمن المعلومات مخاطر يجب أن يتم إدراتها بالشكل المناسب. كما يجب مراعاة جوانب أخرى مرتبطة بذلك مثل قدرة المورّد المالية على الاستمرار، جودة الخدمة، الكادر المؤهل، الالتزام بسياسة أمن معلومات المنظمة وحق التدقيق لدى المورد.

١١,٨,٥,١,٢. تقييم إدارة البرنامج

من المهم أن يتم إعادة تقييم برنامج أمن المعلومات بشكل دوري وكلما دعت الحاجة بالإضافة لمراجعة كفاءة البرنامج بالمواضيع المتعلقة بالتغييرات ضمن توجهات المنظمة، أو البيئة أو القيود. وينبغي مشاركة نتائج هذا التحليل مع لجنة توجيه أمن المعلومات وأصحاب المصلحة الآخرين للمراجعة وتطوير الاستراتيجات اللازمة لتعديل البرنامج. ومن المُستحسن أن يشمل التحليل أهداف البرنامج، متطلبات الالتزام، إدارة البرنامج، إدارة عمليات أمن المعلومات، إدارة المعايير التقنية ومستوى الموارد المالية والبشرية والتقنية المكرَّسة للبرنامج.

١٢,٨,٥,١,٢. خَطط–نَفذ–افحص–تصرّف

يقوم برنامج أمن المعلومات على كفاءة وفعالية إدارة الضوابط المصممة والمطبقة للتعامل مع التهديدات والمخاطر ونقاط الضعف وتخفيفها. وهنا ينبغي تحقيق تناغم مستمر بين استراتيجية البرنامج وأهداف المنظمة. ويُعتبر تطبيق عناصر الحوكمة التالية أمراً أساسياً للحفاظ على كفاءة وفعالية عالية للبرنامج: الرؤية والأهداف الاستراتيجية، مؤشرات تحقيق الأهداف (KGIs)، مؤشرات الأداء (KPIs)، والخطط التكتيكية والسنوية الضرورية لتحقيق الأهداف الاستراتيجية.

١٣,٨,٥,١,٢. المتطلبات القانونية والتشريعية

تُركّز الأقسام القانونية عادة في المنظمات على العقود والأمور ذات العلاقة بالمستندات القانونية والمالية، وفي كثير من الحالات لا يكون لديها إطلاع على المتطلبات القانونية المتعلقة بأمن

المعلومات وعليه يجب ألا يعتمد مدير أمن المعلومات على القسم القانوني في ذلك وينبغي عليه القيام بمراجعة قانونية لتوضيح موقع المنظمة تجاه الالتزام بالمتطلبات القانونية. بالإضافة لذلك قد يتم الطلب من مدير أمن المعلومات دعم المعايير القانونية المتعلقة بخصوصية البيانات والعمليات، استخراج ومعالجة سجلات التدقيق، سياسات الاحتفاظ بالبيانات، إجراءات التحقيق في الحوادث، والتعاون مع السلطات القانونية المعنية. وينبغي الانتباه والتعامل مع القضايا القانونية بحذر شديد كحالة استجواب أو مراقبة أحد موظفي المنظمة أو اتخاذ اجراءات تأديبية بحق أحدهم نتيجة سلوك غير مناسب.

١٤,٨,٥,١,٢. العوامل الفيزيائية والبيئية

يمكن أن يتعرَّض أمن المعلومات للخطر أو التخريب من خلال الوصول الفيزيائي أو تخريب عناصر فيزيائية، يتم تحديد مستوى الحماية الضروري المحيط بالموارد المختلفة وفقاً لدرجة أهميتها وحساسيتها وكلفتها بالنسبة للمنظمة. حيث يوجد طيف واسع من ضوابط الحماية الفيزيائية التي تساعد مدير أمن المعلومات في تحقيق الأمن المادي مثل أنظمة إدارة الدخول، الأقفال الإلكترونية، مُستشعِرات الحركة، الكاميرات، الأقفاص الفولاذية وأجهزة التتبع الراديوية وغيرها. كما يجب مراعاة العوامل الجغرافية وتوزع الموارد عبرها خاصة فيما يتعلق بمواقع الاستعادة من الكوارث التي تؤمن استمرارية نشاطات المنظمة في حالات الكوارث الكبرى كالزلازل والفيضانات. كل ذلك ينبغي أن يكون ضمن سياسات وإجراءات واضحة ومعتمَدة على مستوى المنظمة.

١٥,٨,٥,١,٢. الأخلاقيات

تُنفِذ العديد من المنظمات تدريب أخلاقي للعاملين ضمنها لتوضيح السلوك الذي تعتبره المنظمة قانوني ومناسب، وعادة ما يتم ذلك للأفراد الذين يتطلَّب عملهم الانخراط في نشاطات ومهام ذات طبيعة خاصة وحساسة مثل مراقبة نشاطات المستخدمين، فحص الاختراق، والاطلاع على بيانات شخصية أو حساسة. يجب على فريق أمن المعلومات أن يكونوا حسَّاسين لإمكانية حصول تضارب في المصالح أو النشاطات التي قد تضر بالمنظمة. كما ينبغي أن يتم إنشاء مدونة لقواعد السلوك الخاصة بالمنظمة يوقّعها كل موظف وتحفظ مع سجلاته الوظيفية.

١٦,٨,٥,١,٢. الاختلافات الثقافية والمناطقية

على مدير أمن المعلومات أن يُدرك الاختلافات في العادات والتقاليد والسلوك الملائم بين المناطق والثقافات المختلفة فما هو مقبول في ثقافة ما يمكن أن يكون مرفوضاً في أخرى. لذلك يجب مراعاة ومعرفة المتأثرين بنشاطات أمن المعلومات وفق الثقافات المتنوعة في المنظمة. كما أن التشريعات في بعض البلدان تحد من إمكانية مشاركة المعلومات الشخصية، وهنا يجب مراعاة أن يكون برنامج

أمن المعلومات ملائم للمنظمة ككل. كما يجب أن يتم تطوير وتطبيق السياسات والإجراءات والضوابط مع احترام هذه الاختلافات وتحاشي تناول العناصر التي قد تؤذي المنتمين لثقافات مختلفة والاستعانة ببدائل ملائمة لتحقيق المستوى المطلوب من أمن المعلومات. وفي مثل هذه الحالات يمكن التعاون مع القسم القانوني وقسم الموارد البشرية للوصول لأفضل الحلول على مستوى المنظمة.

١٧,٨,٥,١,٢. الخدمات اللوجستية

يجب أن يراعي مدير أمن المعلومات تأثير القضايا اللوجستية وخاصة الحجم الكبير من التقاطعات مع الوحدات التشغيلية الأخرى أو الأفراد الذين يتطلَّب البرنامج مساهمتهم بنشاطاته. من هذه القضايا:

- التخطيط والتنفيذ الاستراتيجي عبر المنظمة
- تنسيق موارد ونشاطات أمن المعلومات مع النشاطات والمشاريع الأكبر
- تنسيق اجتماعات اللجان ونشاطاتها
- جدولة الإجراءات التي تتطلب تنفيذ دوري
- ترتيب الموارد وإدارة عبء العمل

٩,٥,١,٢. تحديات برنامج أمن المعلومات

عادةً ما يواجه إنشاء برنامج أمن معلومات جديد أو حتى تطبيق تعديلات على برنامج موجود مسبقاً العديد من العقبات غير المتوقعة والتي يمكن أن تتضمن:

- مُمَانعة المنظمة للتغيير الناتج عن البرنامج
- الاعتقاد السائد بأن تعزيز الأمن سيُقلّل إمكانيات الوصول للموارد اللازمة للعمل
- الإفراط في الاعتماد على المقاييس الذاتية
- فشل الاستراتيجية
- تأخر مبادرات أمن المعلومات نتيجة عدم فعالية إدارة المشاريع

ومن أبرز التحديات التي تواجه مدير أمن المعلومات أثناء تطبيق البرنامج:

١,٩,٥,١,٢. دعم الإدارة

إن ضعف دعم الإدارة شائع عادة في المنظمات الصغيرة أو تلك التي ليس لديها صناعات تتأثر بشكل مباشر بمخاطر أمن المعلومات. حيث تُعتَبر وظيفة أمن المعلومات في مثل تلك المنظمات من الوظائف الهامشية التي تتطلب كلف بدون قيمة مستفادة منها.

في مثل هذه الظروف يجب أن يقوم مدير أمن المعلومات بضبط استخدام الموارد بالشكل الأمثل ومراجعة التهديدات الشائعة لأنظمة معالجة البيانات الخاصة بالمنظمة. بالإضافة لذلك ينبغي تقديم الإرشاد اللازم للإدارة لتوضيح ما هو متوقع منها وكيف يتم التعامل مع أمن المعلومات لدى المنظمات المشابهة. إن التدريب وزيادة الوعي المستمرَين بأمن المعلومات في مثل هذه الحالات سوف يؤدي لظهور نتائج حتى ولو تأخر ذلك.

٢,٩,٥,١,٢. التمويل

ربما يعتبر التمويل غير الملائم لاحتياجات أمن المعلومات من أكثر القضايا ازعاجاً وتحدياً أمام مدير أمن المعلومات. وفي الوقت الذي قد يكون فيه ذلك امتداداً لضَعف دعم الإدارة فإن هناك بعض العوامل التي يجب الانتباه لها لأنها قد تؤثر على التمويل:

- عدم إدراك الإدارة لقيمة الاستثمار بأمن المعلومات
- يتم النظر للأمن بأنه مركز كلفة غير قيّم
- عدم فهم الإدارة لأماكن صرف الأموال
- عدم الفهم باحتياجات المنظمة المتعلقة بأمن المعلومات
- الحاجة لمزيد من التوعية بتوجهات الاستثمار في أمن المعلومات لدى الصناعات المشابهة.

ويوجد بعض الاستراتيجيات التي تساعد في الالتفاف على نقص التمويل مثل:

- تحويل ميزانيات عناصر أخرى (مثل تطوير منتج، تدقيق داخلي،..) لتطبيق العناصر الضرورية في برنامج أمن المعلومات.
- تحسين كفاءة عناصر برنامج أمن المعلومات الموجودة أصلاً.
- العمل مع لجنة توجيه أمن المعلومات لإعادة ترتيب أولويات موارد أمن المعلومات وتوضيح المخاطر المحتملة لإهمال ذلك للإدارة.

ويجب الانتباه لمصاعب تبرير تمويل برنامج أمن المعلومات للإدارة، ففي حال نجاحه فإن الإدارة قد لا ترى أين تم صرف الأموال ولماذا يتم صرف كل ذلك. وفي حال فشل تطبيق البرنامج فإن الإدارة ستكون متعجبة من صرف الأموال على أنظمة لا تعمل. لذلك فمن الضروري أن يتم باستمرار إيجاد الطرق الملائمة لاستعراض أهمية أمن المعلومات وعمله وارتباطه الوثيق بأعمال المنظمة.

٣,٩,٥,١,٢. التوظيف

ربما تمتد تأثيرات ضعف التمويل لتبرز كتحدي في تأمين الموظفين بالمهارات اللازمة لمتطلبات البرنامج. من العقبات التي تواجه الحصول على فريق عمل فعّال:

- ضعف الفهم بالنشاطات التي سينفذها هؤلاء الموظفين.
- الشك بالحاجة إلى موظفين جدد أو فوائدهم.
- عدم معرفة درجة الانتفاع من الفريق الموجود أصلاً والاعتقاد أنهم يعملون بأقل من طاقتهم الممكنة.
- الرغبة بالاستعانة بمصادر خارجية عوضاً عن التوظيف.

ومن الاستراتيجيات الممكن اتباعها في حال تعذَّر الحصول على كوادر جديدة لتمكين برنامج أمن المعلومات:

- التعاون مع وحدات العمل الأخرى لتحديد فيما إذا كان بإمكانها تحمُّل مسؤوليات إضافية خاصة بأمن المعلومات وإسناد المهام الملائمة مع الحفاظ على الإشراف عليها.
- دراسة إمكانية الاستعانة بمصادر خارجية خاصة بالنشاطات ذات الكثافة التشغيلية العالية.
- العمل مع لجنة توجيه أمن المعلومات لإعادة ترتيب مهام موظفي أمن المعلومات وتزويد الإدارة بالأعمال التي لن يتم تغطيتها مع الفريق الحالي المتاح وشرح المخاطر المترتبة على ذلك.

٢,٢. المبحَث الثاني: الجدوى الاقتصادية لمشروع

١,٢,٢. مقدمة

٢,٢,٢. تعريف دراسة الجدوى الاقتصادية لمشروع

٣,٢,٢. خصائص دراسة الجدوى

٤,٢,٢. أهمية دراسة جدوى المشاريع

٥,٢,٢. متطلبات دراسة جدوى المشاريع

٦,٢,٢. مجالات التطبيق لدراسات الجدوى الاقتصادية

٧,٢,٢. دراسة الجدوى التسويقية

٨,٢,٢. دراسة الجدوى التقنية (الفنية)

٩,٢,٢. دراسة الجدوى المالية

١٠,٢,٢. صعوبات ومشاكل إجراء دراسات الجدوى

١,٢,٢. مقدمة

الجدوى الاقتصادية هي عملية جمع المعلومات عن المشروع المُقترح ومن ثم ترتيبها وتحليلها لمعرفة إمكانية تنفيذه وتقليل المخاطر المرتبطة به وزيادة ربحيّته. وبالتالي يجب معرفة مدى نجاح هذا المشروع وربحيته أو خسارته مقارنة بمعطيات السوق المحلية واحتياجاتها خلال فترة محددة من الزمن. ويعتبر الإعداد الجيد للجدوى الاقتصادية من أهم خطوات نجاح المشاريع، فنجاح وفعالية أي مشروع تعتمد بالمقام الأول على التخطيط السليم، كما يُمثّل التخطيط الدقيق الركيزة الأساسية التي يعتمد عليها العائد المادي المتوقع من المشروع. ومن هنا برزت الحاجة إلى ما يُعرَف بدراسة الجدوى الاقتصادية للمشروع.

٢,٢,٢. تعريف دراسة الجدوى الاقتصادية لمشروع

تعددت التعريفات الخاصة بدراسات الجدوى الاقتصادية وتقييم المشاريع وخاصة عند الكتابات الأولى منها سواء في كتابات جون ماينزكينز عندما تناول في الثلاثينات والأربعينيات معدل العائد على الاستثمار وفكرة تكلفة رأس المال، أودن جول عام ١٩٥١ م عندما أصدر أول كتاب لمعالجة مشكلة المشاريع الاستثمارية وقد دارَت كل التعريفات التي وردت منذ ذلك التاريخ حول أن عِلم دراسات الجدوى الاقتصادية هو من أهم فروع الاقتصاد التطبيقي الذي يستمد منهجيته من النظرية الاقتصادية بشقّيها الجزئي والكلي متأثراً إلى جانب ذلك بالعلوم الأخرى كالمحاسبة والإدارة وبحوث العمليات بهدف ترشيد القرار الاستثماري من عدة وجوه أو دراسة جدوى المشروع من عدة جوانب، على ضوء هذا يمكن إعطاء مجموعة من التعاريف لدراسات الجدوى:

"هي منهجية لاتخاذ القرارات الاستثمارية تعتمد على مجموعة من الأساليب والأدوات والاختبارات والأسس العلمية التي تعمل على المعرفة الدقيقة لاحتمالات نجاح أو فشل مشروع استثماري معين واختبار مدى قدرة هذا المشروع على تحقيق أهداف محددة تتمحور حول الوصول إلى أعلى عائد ومنفعة للمستثمر خاصة أو الاقتصاد القومي أو كليهما على مدى عمر افتراضي." (دراسات الجدوى الاقتصادية لاتخاذ القرارات الاستثمارية، د.عبد المطلب عبد الحميد)

كما يمكن تعريف دراسات الجدوى على أنها: "تلك المجموعة من الدراسات التي تسعى إلى تحديد مدى صلاحية مشروع استثماري ما، أو مجموعة من المشاريع الاستثمارية من عدة جوانب تسويقية، فنيّة، ماليّة، تمويلية، اقتصادية، اجتماعية، تمهيداً لاختيار المشاريع التي تحقق أعلى منفعة صافية ممكنة". (دراسات الجدوى التجارية والاقتصادية والاجتماعية مع مشروعات Bot، عبد القادر محمد عبد القادر عطية)

يمكننا القول أن دراسة جدوى للمشاريع هي تلك السلسلة المترابطة والمتكاملة من الأساليب العلمية التي تطبق على الفُرَص الاستثمارية منذ بحثها كفكرة إلى حين الوصول إلى القرار النهائي بقبول أو رفض أو إعادة تشكيل تلك الفرصة.

٣,٢,٢. خصائص دراسة الجدوى

إن من أهم خصائص دراسة الجدوى الاقتصادية لمشروع ما يلي (إعداد دراسات الجدوى وتقييم المشروعات، د. نبيل شاكر):

- التعامُل مع المستقبل

حيث نُحدّد بدراسات الجدوى مدى إمكانية تنفيذ فكرة استثمارية وإقرارها الآن ليمتد عمرها الافتراضي لتغطية فترة طويلة مُقبلة، الأمر الذي يُؤكد بالضرورة أن كل نتائج مراحلها تُمثّل تقديرات محتملة تحمل في طيَّاتها احتمالات مطابقة للواقع أو انحراف عنه، مما يُلزمنا مراعاة الدِّقة في هذه التقديرات خاصة في ظل درجة من درجات ظروف عدم التأكد.

- ارتفاع التكلُفة

حيث تتزايد التكلفة المالية التي يتحملها المستثمرون مقابل إعداد الدراسة وخاصة بالنسبة للمشاريع الكبيرة التي تحتاج إلى دراسات أكثر تفصيلاً من طرف مجموعة من الخبراء والمختصين وعليه غالباً ما تكون هناك دراسات استكشافية أو تمهيدية الغرض منها الحكم المبدئي على قبول أو رفض المشروع محل الدراسة وبالتالي التقليل من التكاليف.

- الأهمية القصوى لعنصر الزمن

والذي نقصد به الفاصل الزمني بين نهاية إعداد الجدوى وموافقة الجهات المسؤولة عنها وبين فترة بداية التنفيذ الفعلي للمشروع حيث أن طول هذه الفترة قد يعود بالسلب على المشروع نظراً للتغيُّرات السريعة التي قد تقع في الواقع العملي في هذه الفترة.

- ترابط المراحِل

أي أنَّ قرار استكمال أي مرحلة لاحقة من عدمه يُبنى على نتائج المرحلة التي سبقتها، فنتائج كل مرحلة هي مُدخلات مباشرة للمرحلة التالية لها مما يجعلنا نؤكد على أهمية تتابع مراحلها.

- المرونة

والتي نقصد بها عدم الالتزام المطلق في إعطاء نفس الأهمية لمختلف مراحل دراسة الجدوى، هذا يعني أنه قد نولي اهتماماً متزايداً لدراسة معينة على أخرى.

٤,٢,٢. أهمية دراسة جدوى المشاريع

تتعلق أهميّة دراسة الجدوى بشكل رئيسي بما يلي (اقتصاديات المشروعات، د.محمد الصاريف):

- تحديد مدى ربحيّة المشروع من خلال تقدير العوائد المتوقعَة منه ومقارنتها بالتكاليف المتوقعة ومن ثم حساب الربح الصافي في كل سنة من سنوات التشغيل وطيلة مدة التشغيل.
- المساعدة في اتخاذ القرارات حول أفضل الاستثمارات باستخدام الموارد المتاحة للمستثمر مما يؤدي إلى ترشيد القرار الاستثماري خاصة عندما تكون ميزانية الاستثمار محدودة بسبب ضيق مصادر التمويل وارتفاع تكاليفه.
- تحتاج بعض المشاريع إلى تكاليف ضخمة يكون جزء منها مُغرِقاً أي يصعب استردادها، كتكاليف الآلات والمعدات والأجهزة المتخصصة، لذا فإن فشل المشروع نتيجة عدم القيام بدراسة الجدوى أو لانخفاض مستواها يُعَرِّض مالك المشروع لخسائر ضخمة ويكلف المجتمع موارد اقتصادية ضائعة.
- تُفيد دراسات الجدوى، وخاصة الجانب المتعلق بالدراسات السّوقية في التَّعرف على فرصة المشروع في بيع سلعة في الأسواق سواء المحليّة أو الأجنبية.
- تسهيل الحصول على تمويل للمشروع والمساهمة في تخفيض تكاليف التمويل.
- المساهمة في تحديد الهيكل الأمثل لتمويل المشروع ما بين اقتراض وإصدار أسهم أو أرباح محتجزة أو غيرها من مصادر التمويل بناء على الوزن النسبي لكل منها في التكلفة الإجمالية لتمويل المشروع.
- المساعدة في تحديد الهيكل الأمثل لتكاليف المشروع ما بين تكاليف ثابتة وتكاليف مُتغيّرة بناءً على المساهمة النسبية لكل منهما في التكلفة الكليّة وانعكاس ذلك على ربحية المشروع.
- تسهيل عملية تقييم أداء المشروع وذلك من خلال مقارنة مدى ما تحقق من أهداف المشروع (أرباح، مبيعات، معدل نمو،....) بعد بدء التشغيل مع ما خُطّط له من هذه الأهداف في دراسات الجدوى.
- التقليل من مخاطر عدم التأكد من خلال تقييم التأثيرات المختلفة على أداء المشروع مثل تغيُّرات أسعار السلعة المُنتَجة وأسعار مستلزمات الإنتاج وتكاليف التمويل وتغيُّرات الطلب والتطورات التقنية والتغيرات في ظروف الإنتاج.

٥,٢,٢. متطلبات دراسة جدوى المشاريع

تتوقف سلامة ودقة النتائج التي تقدمها دراسة الجدوى على نوعية البيانات والمعلومات ومصداقيتها، ولذلك فإن توفُّر بيانات ومعلومات تفصيلية عن المشروع تُعَد مطلباً أساسياً لضمان اختيار البديل

من البدائل المتاحة أي اتخاذ القرار الاستثماري السليم، وحتى يمكن إخضاع المشروع للدراسة والتقييم فإن الشروط الآتية يُفتَرض أن تتوفر فيه (الجدوى الاقتصادية للمشروعات، د. طلال محمود كداوي):

- **المعرفة التفصيلية بمتطلبات المشروع:** تنفيذاً أو تشغيلاً سواء كانت تلك المُتطلبات متوفرة في الأسواق المحلية أو الخارجية، وهذا يستلزم تحديد مقدار النقد الأجنبي اللازم لتوفير تلك المتطلبات في مرحلتي التنفيذ والتشغيل خلال عُمر المشروع المتوقع بالإضافة إلى تكاليف المشروع بالعملة المحلية.
- **تحديد طبيعة وحجم السلع والخدمات التي سيقوم المشروع بإنتاجها:** وكذلك تحديد مستويات الطاقة الإنتاجية للمشروع لغرض معرفة مدى قدرة المشروع على تلبية الطَّلب المحلي والخارجي معاً، وعلى ضوء هذه المعلومات يصبح بالإمكان تقدير العوائد المتوقعة للمشروع عبر الفترات الزمنية من عمره المتوقع.
- **المعرفة الدقيقة والتفصيلية لمراحل تنفيذ المشروع وعمره الإنتاجي:** وتثبيت ذلك بوحدات زمنية متعارف عليها كالسنة.
- **قابلية مستلزمات المشروع (تكاليفه) للقياس والتقييم:** لأن الدراسة ستكون مستحيلة في حالة عدم القدرة على التعبير رقمياً عن المتغيرات.
- **القدرة على قياس وتقييم مخرجات المشروع بوحدات نقدية:** وتعد المتطلبات آنفة الذكر شرطاً أساسياً يجب توفرها في أية فكرة حتى يمكن وضع تلك الفكرة موضع دراسة وتحليل.

٦,٢,٢. مجالات التطبيق لدراسات الجدوى الاقتصادية

تتعدد المجالات التطبيقية لدراسات الجدوى الاقتصادية ويمكن الإشارة إلى أربعة مجالات رئيسية (دراسات الجدوى الاقتصادية لاتخاذ القرارات الاستثمارية، د.عبد المطلب عبد الحميد):

١. دراسات الجدوى للمشاريع الجديدة:

يُعَد هذا إجمالاً من أكثر المجالات التطبيقية انتشاراً وأهمية لما يحتاجه المشروع الاستثماري الجديد من دراسات وتقديرات وتوقعات تقوم على منهجية وأساليب دقيقة في ظل ظروف عدم التأكد المُصاحِبة لأي مشروع جديد، في هذه الحالة تختلف دراسات الجدوى من حيث الحجم والعمق والتكلفة والمختصون والخبراء وهذا حسب نوعية المشروع (صغير، متوسط، كبير)

٢. دراسات الجدوى للمشاريع التوسعية:

تكون دراسة الجدوى هنا أمام مشروع قائم بالفعل ولكن لأسباب عديدة يتم التوسع الاستثماري فيه، من خلال إقامة مصنع تابع له مثلاً أو إضافة خط إنتاجي جديد مما يؤدي إلى إنتاج جديد إضافي

للمنتجات القائمة أو قد يكون التوسع من خلال زيادة الطاقة الإنتاجية باقتناء آلات إنتاج جديدة وفي كل الحالات يحتاج قرار التوسع إلى دراسة الجدوى لاتخاذ القرار الاستثماري السليم.

٣. دراسات الجدوى الاقتصادية للإحلال والتجديد:

وتتم تلك الدراسة عندما يتعلق القرار الاستثماري بإحلال أو استبدال آلة جديدة محل آلة قديمة بعد انتهاء العمر الافتراضي للآلة القديمة، وتحتاج هذه المسألة إلى أداة للاختيار بين الأنواع من الآلات وتقدير التدفقات النقدية الداخلة والخارجة المتوقعة، والعائد من كل بديل واختيار البديل الأفضل، وهذا القرار من القرارات الاستراتيجية التي يجب دراسة جدواها بعناية ودقة.

٤. دراسات الجدوى للتطوير التكنولوجي:

نظراً للتقدم التكنولوجي الذي يشهده العالم في مختلف المجالات فقد ازدادت رغبة المستثمر في إدارة المشاريع بأساليب جديدة من أساليب التكنولوجيا الحديثة المُستخدَمة في العمليات الإنتاجية، مع الأخذ في الاعتبار أن هناك دائما مفاضلة بين نوعين من التكنولوجيا إما تكنولوجيا كثيفة العمل أو تكنولوجيا كثيفة رأس المال، في كل الأحوال يحتاج القرار الاستثماري هنا إلى دراسة جدوى لاختيار البديل الأفضل.

٧,٢,٢. دراسة الجدوى التسويقية

إن دراسة الجدوى التسويقية هي الدراسة التي تهدف إلى التعرُّف على الجوانب المختلفة لسوق السلعة أو الخدمة التي ينتجها المشروع بهدف تقدير المبيعات الحالية والمتوقعة ورسم السياسة التسويقية المناسبة. ويمكن تحديد عدد من الأهداف التي يرجى تحقيقها من خلال القيام بتلك الدراسات أهمها (دراسات الجدوى الاقتصادية وتقييم المشروعات الاستثمارية، شقيري نوري موسى):

- تقدير حجم الطلب المتوقع على منتجات المشروع ومعدل نموه وتحديد الحجم الكلي للسوق المرتقب والشريحة التسويقية بما يتضمنه ذلك من دراسة العوامل المحددة للطلب على منتجات المشروع.
- تحديد هيكل ونوع السوق ودرجات المنافسة التي يمكن أن يتعرض لها المشروع وتحديد التقسيم الجغرافي والقطاعي للسوق حسب نوعيات المستهلكين ودخولهم وأعمارهم.
- تحديد نمط الأسعار واتجاهاتها في الماضي، والحاضر والمستقبل وتخطيط الإستراتيجية السعرية.
- تحديد الحملات الاعلانية والترويجية الخاصة بالسُلع أو الخدمة محل الدراسة.
- التوصية بحجم الإنتاج الملائم طوال عمر المشروع.

لمعرفة أهمية بحوث التسويق بالنسبة لدراسات الجدوى للمشاريع المقترحة ودورها في تنميتها فإنه يتحتم علينا معرفة ثلاثة أشياء مهمة (دور وأهمية الكفاءة التسويقية في تحسين أداء المؤسسة الصناعية، أباي ولد الداي):

١- **إمكانيات المشروع:** بفضل الدراسة التسويقية يستطيع أصحاب المشروع تحديد مجال نشاطهم وفقاً للإمكانيات التي يتوفر عليها المشروع وتجنُّب ما لا تستطيع الإمكانيات أن تصل إليه حتى لو كان نشاطاً مربحاً، أي أن الدراسة التسويقية تُعطي فكرة ولو مبدئية عن كيفية استغلال الموارد المتاحة للمشروع استغلالاً أمثلاً.

٢- **البيئة التسويقية:** إن عملية الربط بين المستهلك وإمكانيات المشروع إنما تحدث في الوسط الذي يعمل فيه المشروع أي ما يسمى بالبيئة التسويقية تلك التي تضمن إلى جانب المنافسين، السياسات الحكومية، وكذا التشريعات المتعلقة بالتميُّز والتعبئة والتغليف والإعلان والمحافظة على البيئة وغيرها، كل هذه العناصر يتم معالجتها والاستفادة منها بفضل بحوث الدراسة التسويقية، ولا ننسى هنا التقدم التقني الذي يُعتبر عنصراً حساساً وهاماً يؤثر على البيئة التسويقية، بالإضافة إلى هذه المتغيرات تكتسي الدراسة التسويقية أهمية كبيرة فيما يخص البيئة التسويقية عندما يتعلق الأمر بالتحديد بدور المتابعة المستمرة لعناصر المزيج التسويقي (المنتج، السعر، الترويج، التوزيع) وهي عناصر تضعُنا على الدوام في مواجهة عنصر المنافسة الخاصة.

٣- **رغبات واحتياجات المستهلك:** يعكس هذا العنصر الأهمية البالغة لبحوث التسويق، والتي تسعى إلى دراسة رغبات واحتياجات المستهلكين حيث يتم طرح المنتج بحسب هذه الرغبات، ما يؤكد أهمية الدراسة هو فشل العديد من المؤسسات الصناعية والتجارية في طرح منتجاتها الجديدة في الأسواق وعدم قبولها من طرف المستهلكين، نتيجة لعدم وجود بحوث تعكس هذه الرغبات.

٨,٢,٢. دراسة الجدوى التقنية (الفنيّة)

تُعتبر دراسة الجدوى الفنيّة المرحلة التي تلي دراسة الجدوى التسويقية، في إطار دراسة الجدوى الاقتصادية، ولكي نتمكن من الانتقال إلى هذه المرحلة يجب الاستعانة بما أفرزته دراسة السوق من نتائج وفيما إذا كان حجم الطلب يُبرر الاستمرار أو التوقف عن دراسة الجدوى ككل. ويُقصد بالجدوى الفنية لمقترح استثماري دراسة الجوانب الهندسية المتعلقة بإقامة المشروع ومدى تحقيقها بهدف اتخاذ قرار تبنّي الاستثمار أو رفضه على أساس جدواه. مما سبق يمكننا التأكيد على ارتباط هذه الدراسة بالصفات التالية (دراسات الجدوى الاقتصادية، د.بهاء الدين أمين):

- تتم على مراحل تفصل بينها مسافات زمنية، الأمر الذي يُحَتّم على مَن يتصدّى لإعدادها مراعاة عنصر الزمن وتأثيره على نتائجها.
- تُعطي هذه الدراسة وزن كبير لعنصر التكنولوجيا الحالي والمتوقع مستقبلاً.
- تُعطي هذه الدراسة أهمية متزايدة للعنصر البشري القائم بإعدادها من حيث الإلمام العلمي والخبرة العملية من الخبرات السابقة.

- تسمح هذه الدراسة بإمكانية الاقتصار على إعداد بعض مراحلها الكلية في تلك الحالات التي لا تتطلب إعداد الدراسة الفنية بكامل جوانبها.
- تُحدِد هذه الدراسة طبيعة الدراسات البيئية والتسويقية التي تسبقها في الإعداد.
- الأهمية المطلقة لمراعاة عنصر الموضوعية عند إعدادها تفادياً لانعكاسات مؤثرة وخطيرة مثل عدم كفاية الطاقة الإنتاجية أو وجود طاقات إنتاجية غير مُستغَلَّة، بالإضافة إلى تضخم التكاليف الاستثمارية والتشغيلية وزيادة نسبة الإنتاج التالف والمعيب والمرتجع من العملاء.

٩,٢,٢. دراسة الجدوى المالية

تعتمد دراسة الجدوى المالية والتمويلية للمشروع على نتائج الدراسة الفنية وبالضبط بعد تحديد تكاليف المشروع الاستثمارية من خلال التعرُّف على مصادر الأموال المتاحة ليتم اختيار الهيكل المالي المناسب للمشروع، ثم يليه تقدير تكلفة أموال هذا الهيكل والذي يُعتبر الأساس لقبول أو رفض المشروع الاستثماري، وإذا اتُّخِذ قرار بقبول المشروع تنتهي هذه الدراسة بإعداد القوائم المالية وإلا فالمشروع يُلغى.

١,٩,٢,٢. تحليل الهيكل التمويلي للمشروع

يُقصد بتحليل الهيكل التمويلي تحديد مصادر واستخدامات الموارد المالية المتاحة لتمويل المشروع سواء كانت بالعملة المحلية أو الأجنبية، مع التأكيد على التلاؤم بين أوقات تدفق هذه الموارد وأوقات استخدامها بما يضمن تشغيل المشروع وفقاً للهدف المرسوم له.

وهناك أربعة مصادر للتمويل هي: أموال المُلكية (التي يتضمنها الأسهم العادية والأسهم الممتازة والأرباح المحتجزة)، والقروض (السندات، الائتمان المصرفي، القروض القصيرة والمتوسطة والطويلة الأجل)، والائتمان التجاري (لشراء الخامات والبضائع والأصول الثابتة)، وأخيراً التمويل بالاستئجار والذي ينقسم إلى الاستئجار التمويلي والاستئجار التشغيلي (دراسات الجدوى الاقتصادية وتدقيق المشروعات، سمير محمد عبد العزيز).

١٠,٢,٢. صعوبات ومشاكل إجراء دراسات الجدوى

هناك العديد من الصعوبات والمشاكل التي يمكن مواجهتها عند السَّعي لإجراء دراسات الجدوى في المجالات التطبيقية المُشار إليها، لعل من أهمها (دراسات الجدوى الاقتصادية لاتخاذ القرارات الاستثمارية، د.عبد المطلب عبد الحميد):

- في ظل العولمة والتحّول لآليات السوق، تزداد مشاكل التعامل مع المُتغيرات الداخلية في الاقتصاد القومي والمتغيرات العالمية في الاقتصاد العالمي، مما يزيد من مخاطر عدم التأكد في تقدير عدد من المتغيرات في دراسات الجدوى خلال العمر الافتراضي للمشروع، مثل الأسعار والطلب وأسلوب الإنتاج وغيرها، وهو ما يتطلَّب المزيد من التعمق في البحث عن الأدوات والأساليب التي تتغلب على تلك المشكلات وهنا تكسب تحليلات الحساسية دوراً كبيراً في هذا المجال.
- مع ازدياد حجم المشاريع تزداد صعوبات تقدير بنود التدفقات النقدية الداخلة والخارجة وبالتحديد الأخيرة أي التكاليف، بالإضافة إلى أن بعض المتغيرات قد تكون غير قابلة للقياس الكمّي وتأثيرها غير مباشر وهو ما يتطلَّب السعي دائماً إلى إخضاع مثل تلك المتغيرات للقياس الكمّي كلَّما أمكن من خلال الاستعانة بعلوم الإحصاء والاقتصاد القياسي، وبحوث العمليات وغيرها.
- عدم التوازن بين تكاليف دراسات الجدوى وتقييم المشاريع وحجم المشروع ورأس المال المخصص للاستثمار في المشروع وهو ما يتطلَّب البحث دائماً في إحداث هذا التوازن وتفضيل دراسات الجدوى على المشروع كحالة منفصلة دائماً فكل مشروع هو حالة لابد أن تتلاءم دراسات الجدوى مع أوضاعه وحجمه.
- هناك أيضاً بعض الصعوبات الفنية خاصة عندما تكون الخبرات الفنية التي تقوم بالمشروع ضعيفة وهو ما يتطلب دائماً الاستعانة بالخبرات الفنية ذات المهارة العالية والمتخصصة في النشاط الخاص بالمشروع والدراسات الفنية له.
- أخيراً هناك صعوبات ومشاكل نقص البيانات والمعلومات أو تضاربها أو عدم وضوحها مما قد يؤثر على دقة تقدير بعض المتغيرات الداخلية في دراسات الجدوى وهو ما يمكن علاجه من خلال العديد من الأساليب التي تُطبق في كل حالة على حدة.

٣,٢. المبحَث الثالث: المُنظمة موضوع البحث

١,٣,٢. مقدمة

٢,٣,٢. مبادئ الحركات الإنسانية

٣,٣,٢. أهمية الاستثمار في برنامج أمن المعلومات بالنسبة للمنظمة

٤,٣,٢. حاجة قطاع المنظمات الإنسانية لجعل الأمن السيبراني أولوية

٥,٣,٢. أسباب فشل الاستثمار في أمن المعلومات في المنظمات

١,٣,٢. مقدمة

هي منظمة إنسانية تتمتع بالاستقلال المالي والإداري ذات شخصية اعتبارية مُعترَف بها من قِبل اللجنة الدولية للصليب الأحمر بجنيف، لها مركز رئيسي والعديد من الفروع الموزعة في المحافظات السُّورية.

تَعمل هذه المنظمة في القطّاع الطّبي لتقديم المساعدات الطبية الأولية أو المتقدمة من خدمات تغذية أو أطراف صناعية، وفي المجالات الخدمية والإغاثة، وضمن المجال المُجتَمعي والإنساني لدعم سُبل العيش وتقديم الخدمات المالية للمستفيدين ليتم صرفها في المواضع التي يحتاجونها، هذا بالإضافة لتقديم المساعدات المتعلقة بمشاريع المياه وإعادة الإعمار.

تسعى المنظمة لتقديم خدمات للفئات الأشد احتياجاً في كافة أرجاء الجمهورية العربية السورية. حيث يتم أثناء عملية تقديم المساعدات والخدمات تسجيل بيانات تفصيلية عن المستفيدين وأخذ بياناتهم الشخصية لتحليل مدى الحاجة والمجالات الأهم التي يحتاج المستفيد الدَّعم ضمنها. بالإضافة لذلك تهتم المنظمة بالعاملين والمتطوعين لديها وتحتفظ لهم لديها بالسجلات والبيانات المطلوبة من الجوانب القانونية وإدارة الموارد البشرية.

إن حماية البيانات المتعلقة بالمستفيدين والعاملين والمتطوعين هي من أهم النقاط التي تعمل كوادر المنظمة المختصة في الحفاظ عليها كونها تُعتبر من البيانات المهمة والحساسة لأنها تتضمن طيف واسع من المعلومات الشخصية والطبية والمالية والقانونية وغيرها، ومن الواجب تأمين الحماية الفيزيائية والمنطقية لها لضمان سرية التعامل بها ونزاهتها وإتاحتها بالشكل الأمثل عند الحاجة من خلال قاعدة البيانات الضخمة الموجودة لدى المنظمة والتي يتم تخزين هذه البيانات ضمنها.

٢,٣,٢. مبادئ الحركات الإنسانية

تمثل المبادئ الأساسية السبعة، التي أُعلِنت في فيينا سنة ١٩٦٥، الرابط بين مختلف المنظمات العاملة في المجال الإنساني والإغاثي وهي الضّامن لاستمرارية عملها:

- **الإنسانية:** تواصل جهودها على الصعيدين الدولي والوطني للوقاية والتخفيف من آلام الإنسان أينما كانت وحماية الحياة والصحة وضمان الكرامة الإنسانية وتعزيز التفاهم والصداقة والتعاون والسلام الدائم بين جميع شعوب العالم.
- **عدم التحيُّز:** لا تُميّز بين القوميات أو الأجناس أو الطبقات أو الأديان أو العقائد السياسية فهي لا تهدُف إلا إلى إزالة معاناة الإنسان وتُعطي الأولوية للحالات التي تتطلب عملاً عاجلاً.

- **الحياد:** للاحتفاظ بثقة الجميع، تمتنع عن الاشتراك في أيّة أعمال عدائية أو في مجادلات متعلقة بالمسائل السياسية والدينية والعرقية والإيديولوجية.
- **الاستقلال:** رغم أن الجمعيات الوطنية تعمل كأجهزة مُساعدة للسلطات العامة فيما تضطلع به من نشاطات إنسانية وتخضع للقوانين السارية في بلادها، فإنه يجب عليها أن تحافظ دائماً على استقلالها حتى تستطيع أن تتصرف بموجب هذه المبادئ في جميع الحالات.
- **الخدمة التطوعية:** تعمل للإغاثة التطوعية ولا تسعى لتحقيق أي ربح.
- **الوحدة:** يجب أن تكون خدماتها مُتاحة للجميع وشاملة لكافة أنحاء القطر.
- **العالمية:** حركات عالمية تتمتع كل الجمعيات بنفس الحقوق في ظلّها وتلتزم بالتعاون فيما بينها.

٣,٣,٢. أهمية الاستثمار في برنامج أمن المعلومات بالنسبة للمنظمة

تستخدِم المُنظمة أصول تكنولوجيّة متنوعة وواسعة تُتيح لها ممارسة أعمالها بسهولة ويُسر وتنظيم بياناتها واستخراج التقارير اللازمة للتطوير وبناء برامج ومشاريع العمل الجديدة. وبما أن لديها قواعد بيانات ضخمة تحتفظ فيها بالسجلات المتعلقة بالبيانات الشخصية والصحية والمالية والقانونية وغيرها الخاصة بالزبائن (المستفيدين) والموظفين والمتطوعين وغيرهم من أصحاب المصلحة كالمانحين والموردين والمتعاقدين، لذلك فإنه من مسؤولية وواجب المنظمة تأمين الحماية اللازمة لهذه البيانات الحساسة لضَمان تخفيف المخاطر المتعلقة بتسريبها أو فقدانها أو التلاعب بها بالإضافة إلى تأمين استمرارية الأعمَال التي قد تتعرض للفشل وخروجها عن الخدمة نتيجة حوادث أمن معلومات معينة.

وعليه فإن أهمية الاستثمار في برنامج أمن المعلومات بالنسبة للمنظمة تتلخص بما يلي:

- تعزيز قدرة المنظمة على حماية أصولها المعلوماتيّة من حوادث أمن المعلومات بما في ذلك سرية ونزاهة وإتاحة هذه الأصول.
- تعزيز قدرة المنظمة في الاستجابة لحوادث أمن المعلومات واحتوائها.
- تعزيز قدرة المنظمة على الاستعادة من الكوارث لتأمين استمرارية تنفيذ أعمالها.

٤,٣,٢. حاجة قطاع المنظمات الإنسانية لجعل الأمن السيبراني أولوية

في الماضي غير البعيد ، كانت المنظمات الدولية والمنظمات غير الحكومية التي تعمل في المبادرات الإنسانية تعتمد إلى حد كبير على الخطوط الأرضية وأجهزة الفاكس للتواصل ونقل البيانات إلى مراكزها الإقليمية أو مقارها الرئيسية.

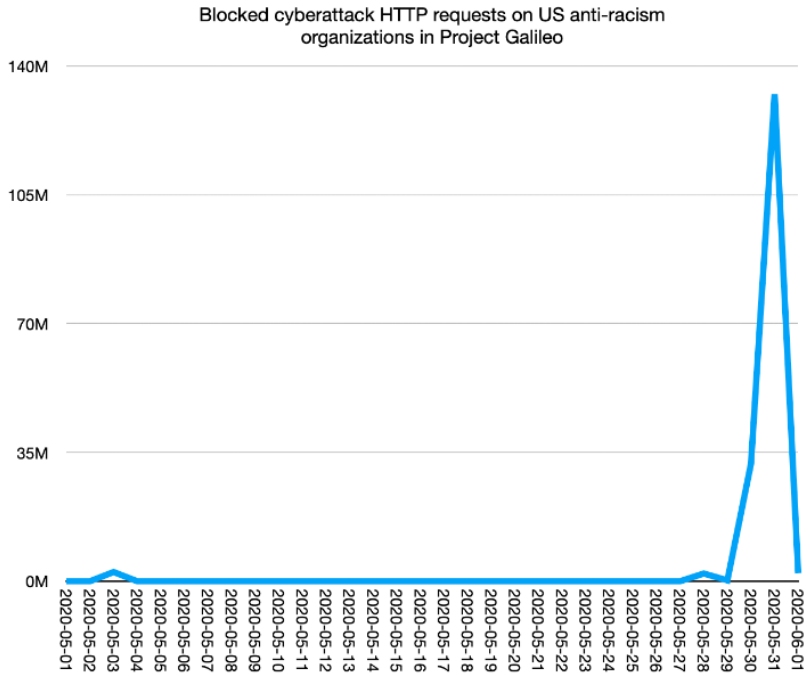
أما الآن، فمثل معظم الشركات، استثمرت المنظمات غير الحكومية والمنظمات الدولية أموالاً كبيرة في تقنيات المعلومات والاتصالات لتعزيز قدراتها في إدارة الأزمات. على سبيل المثال، يتم تحقيق عملية صنع القرار بشكل أفضل وأسرع من خلال التقاط وتحليل البيانات الديموغرافية لتحديد الفئات الضعيفة، وقد أثبتت الدراسات الاستقصائية عبر الإنترنت أنها حاسمة لفِرَق المياه والصرف الصحي والنظافة في تقديم خدمات الصحة للسكان، كما أن القسائم أو البطاقات الرقمية (الإلكترونية) التي تدعم القياسات الحيوية كان لها دور فعّال في الحد من الأخطاء والاحتيال في الدفع للمستفيدين.

هذه التغييرات تجعل المساعدات الإنسانية أسرع وأكثر كفاءة، يُساعد اختيار هذه الأدوات الرقمية في إنقاذ الأرواح، ومع ذلك ، فقد جعل التحول الرقمي أيضاً المنظمات الدولية والمنظمات غير الحكومية أهدافاً مغرية للهجمات الإلكترونية من قبل المجرمين والإرهابيين. وتتراوح أسباب ذلك من الأسباب المالية البحتة (فالأشخاص الذين يمرُّون بأزمات يصبحون أهدافاً سهلة للخداع والسرقة) إلى السياسية وغيرها من الأسباب.

على سبيل المثال، ازدادت الهجمات الإلكترونية ضد حقوق الإنسان وجماعات المناصرة بنسبة ٢٦٪ خلال الاحتجاجات المُطالِبة بالعدالة العِرقيَّة التي وقعت في أعقاب مقتل جورج فلويد في الولايات المتحدة الأمريكية، وخلال شهري أيار وحزيران ٢٠٢٠ حظرت شركة أمن مواقع الويب Cloudflare عدداً هائلاً من الطلبات عبر الإنترنت لتنفيذ هجمات رفض الخدمة الموزعة (DDoS) أو اقتحام مواقع الويب والتطبيقات، كانت المنظمات الأكثر استهدافاً هي مجموعات المُناصَرة، والتي شهدت زيادة بمقدار ١١٠٠ ضعف، وينتقل العديد من الهجمات من صفر إلى ٢٠٠٠٠ طلب في الثانية على موقع واحد مما يجعل من المستحيل الكشف عن هوية المُهاجم في الفضاء الإلكتروني بالتأكيد، وامتدَّ تأثير ذلك على هذه المنظمات ليشمل تراجُع أداء مواقع الويب، ومشكلات في البنية التحتية، وزيادة التعرُّض للهجمات الإلكترونية الأخرى.

واجهَت المنظمات الأكبر حجماً أيضاً تهديدات مماثِلة، حيثُ تم اختراق الأمم المتحدة من قبل متسللين في أوائل عام ٢٠٢١، ولا تزال التهديدات القائمة على هذا الخرق مستمرة حتى الآن. وقيل حينها أن خرق البيانات كان قد نشأ من بيانات اعتماد أحد الموظفين التي تم بيعها على شبكة الإنترنت المُظلِمة، واستخدم المهاجمون نقطة الدخول هذه للتوغل أكثر في شبكات الأمم المتحدة، وإجراء الاستطلاع والبدء في مزيد من الهجمات.

الشكل (١٠) ازدياد الهجمات الإلكترونية ضد جماعات حقوق الإنسان في أعقاب مقتل جورج فلويد



المصدر: www.cloudflare.com

وحتى الاتصالات مع بعض أكثر الحكومات تمويلاً وحرصاً في العالم لا يمكنها توفير الحماية من مجرمي الإنترنت. في أيار ٢٠٢١، تسللت مجموعة قراصنة تدعى Nobelium إلى أنظمة البريد الإلكتروني لوكالة التنمية الدولية التابعة لوزارة الخارجية الأمريكية (USAID) وشرعت في إرسال رسالة مصابة إلى ٣٠٠٠ حساب تستهدِف ١٥٠ منظمة مختلفة في ٢٤ دولة أكثر من ربعِها تشارك في التنمية الدولية والعمل الإنساني وحقوق الإنسان حول العالم.

تُعاني المنظمات الدولية والمنظمات غير الحكومية من نقص كبير في التمويل عندما يتعلق الأمر بمعالجة التهديدات السيبرانية المتصاعدة، وذلك على الرغم من استهدافها بشكل متزايد. من المؤكد أن بعض هذه الهجمات مدفوعة بطبيعة عمل هذه المنظمات، لكن العديد من المهاجمين الآخرين عبر الإنترنت يرون أنها مجرد ثمار سهلة الوصول في محاولتهم للحصول على فدية أو الوصول إلى الأموال عن طريق الاحتيال. ونقص التمويل جعل من الصعب على العديد من تلك المنظمات توظيف خبراء ممارسين وتنفيذ برامج لخرائط طريق للأمن السيبراني التي تشتد الحاجة إليها يوماً بعد يوم وكل ذلك في ضوء تأثير وباء COVID على الاقتصاد العالمي الذي جعل جمع الأموال أكثر صعوبة بكثير من السابق.

كل ذلك جعل من التفكير في مخاطر أمن المعلومات أمر حيوي للمنظمات الدولية والمنظمات غير الحكومية، حتى ولو لم يكن الحصول على التمويل كافياً لتحقيق الدفاع اللازم عن الأمن السيبراني،

فيمكن للقادة في هذه المنظمات أن يأخذوا بعض الدروس الإستراتيجية التي تعلَّمَها القطاع الخاص عن طريق تنفيذ الأنظمة المرنة عبر الإنترنت والحفاظ عليها، ويجب مراعاة النقاط التالية، مع مراعاة أن معظم هذه الأفكار لا تتطلب زيادة إلى تكاليف المنظمة بل تتطلب فقط التخطيط والفهم لقضايا المخاطر الإلكترونية على مستوى القيادة:

- **تقييم المخاطر:** يُعد فهم التهديدات المختلفة للمخاطر أمراً أساسياً لتأمين أنظمة تكنولوجيا المعلومات. عند تطوير أنظمة أو تطبيقات جديدة، يجب إجراء تقييم للمخاطر لتحديد جميع التهديدات والتأثيرات ومطابقتها مع الإجراءات المضادة والمالكين وتواريخ الاستحقاق.
- **بناء القدرات:** كحد أدنى، يجب أن يكون هناك فريق محوري مُخصَّص لأمن المعلومات داخل المنظمة، يكون مسؤول عن مراقبة التهديدات والاستجابة لها، ويمكن إشراك خبراء متخصصين خارجيين بسرعة حسب الحاجة.
- **استمرارية الأعمال والاستجابة للحوادث:** يجب أن يكون لدى المنظمة خطة لاستمرارية الأعمال يمكن استخدامها في حالة وقوع حادث أمني معطِّل. يجب أن يعرف الموظفون أيضاً ما يجب فعله ومع من يتَّصلون عند وقوع حادث أمني، يجب أن يكون لدى نقطة اتصال أمن المعلومات أو فريق الاستجابة للحوادث خطة موثقة للرد على كل خرق، وهذا يشمل الأطراف الخارجية التي يتعيَّن عليها الاشتراك لتقديم مساعدة موثوقة.
- **عمليات تدقيق أمنية مستقلة:** يجب إجراء عمليات التدقيق الأمني سنوياً على الأقل ويجب أن يتم إجراؤها من قبل طرف خارجي ليس له أي علاقات أو مصالح راسخة في المنظمة.
- **إدارة البيانات:** تضمن سياسة حوكمة البيانات أن تكون بيانات المنظمة موثوقة ودقيقة ومتاحة في الوقت المناسب لمن لديهم حاجة مشروعة إليها وسلطة الوصول إليها، تضمن مثل هذه السياسة أيضاً أن البيانات آمنة ومحمية بناءً على حساسيتها.
- **موازنات أفضل:** وذلك يتطلب تحولاً في العقلية من جانب المانحين والقيادة التنظيمية. يجب على المانحين أن ينظروا إلى الأمن السيبراني على أنه أمر بالغ الأهمية لعمليات المساعدة الإنسانية، ويجب تقديم عروض تقديمية مفصَّلة للممولين الذين يقدِّمون التمويل اللازم للمنظمات الإنسانية للاستعداد بسرعة، وبناء فرق الأمن، وتطوير قدرات الاستجابة للأمن السيبراني.

أخيراً، مثل العديد من قضايا الأمن السيبراني، يعد التعاون بين المدافعين أمراً أساسياً حيث يمكن للمنظمات الإنسانية الاستفادة من علاقات عمل أوثق مع بعضها ومع القطاع الخاص.

ويجب أن تضمن هذه المنظمات أن لدى مجالس إدارتها بعض الخبرة في مجال الأمن السيبراني، واعتماداً على سجل تعريف مخاطر المنظمة قد يتطلب ذلك جلب خبير في التكنولوجيا أو الأمن السيبراني ووضع المخاطر الإلكترونية كموضوع متكرر على جدول أعمال مجلس الإدارة مما يسمح للمنظمات بوضع الأمن السيبراني من ضمن المخاطر واسعة الانتشار، وفهم الآثار القانونية لها، وتعزيز حماية الأصول القيّمة ضد الهجمات الإلكترونية، والتركيز على مخاطر سلسلة التوريد من الأمور التي يجب مراعاتها في هذا السياق.

٥,٣,٢. أسباب فشل الاستثمار في أمن المعلومات في المنظمات

عادةً ما يقود الجهد المبذول في غير محله إلى فشل الاستثمار، يتم التعامل مع أمن المعلومات بشكل عام على هيئة مشاريع امتداداً لنشاطات تقنية المعلومات ويتم على هذا الأساس توفير الدعم التمويلي لمشاريع أمن المعلومات التي يجب وفق هذه الرؤية أن تبدأ بتاريخ وتنتهي بتاريخ والتي تُعتَبر طريقة خاطئة في إدارة أمن المعلومات لحماية أصول المنظمة.

يُعتبر أمن المعلومات عملية مستمرة يجب دمجها ضمن مختلف القطاعات لتأمين ديمومة الحماية خلال مراحل العمل المتعددة، ويُعتبر أول أساس قويم لحماية الأصول ضمن المنظمة هو دعم الإدارة العليا وتبنيها لنشاطات أمن المعلومات، وتكون الجهود بدون هذا الأساس غير مكتملة وبلا دعم تنفيذي يؤدي لتشكيل وعي جَمعي مؤسَّسي حول أهمية أمن المعلومات.

إن تعزيز ثقافة أمن المعلومات داخل نطاق العمل تقتضي أن يتم تأهيل الكوادر اللازمة لإدارة أمن المعلومات بشكل فعّال، ومن مهام هذه الإدارة إنجاح الاستثمار في أمن المعلومات، وأول الخطوات لإنجاح تلك الاستثمارات هو تحويل أمن المعلومات إلى جزء من العمل اليومي على مستوى المنظمة ككل، وأن يتحول إلى جزء من إجراءات وعمليات المنظمة لا أن ينفصل عنها بنشاطات مستقلة. إن تحويل أمن المعلومات الى إجراء على مستوى المنظمة بدلاً من أن يكون إجراء يتم قبل أو بعد إتمام العملية التشغيلية نفسها يُحَوّل الحماية من أمر مرحلي إلى أمر مُستدام ويؤمن الحماية الفعالة للعمليات المختلفة في كل قطاعات العمل. وبذلك يتحول أمن المعلومات من مكوّن جانبي في العمليات إلى مكون أساسي يتطلَّب تدخل أفراد أمن المعلومات وتنفيذ إجراءات، تحاليل، حوكمة، اختبارات وتقييم لمستوى وحالة أمن المعلومات في هذه العمليات بشكل مستمر.

وبهذا الشكل يمكِن تأمين عمليات القطاعات المختلفة بإشراف أمن المعلومات ومن خلال استثمارات ناجحة حسب متطلبات القطاعات المختلفة بدلاً من أن تكون استثمارات خارجة عن نطاق العمل ولا

تهتم فعلياً بتأمين العمل ومتطلباته وإنما مشاريع تتطلب مجرد مُخرجَات ينبغي تحقيقها بِغض النظر عن تأمين عمليات المنظمة.

ومن الملاحَظ مؤخراً ازدياد الاعتماد على متعهدين خارجيين (outsourceing) في مختلف القطاعات الحكومية أو الخاصة في مجالات أمن المعلومات وتُعامَل تلك المشاريع وكأنها مشاريع لا تختلف عن بقية المشاريع ضمن المنظمة ما قد يؤدي لفشل الاستثمار المتعلق بها في كثير من الحالات وهذا مرتبط بعدة أسباب من أهمها أن أمن المعلومات يُعنَى بتأمين قطاعات العمل كلها وليس مجرد بعض العمليات التشغيلية كما تمت الإشارة إليه أعلاه وأن متطلبات أمن المعلومات تفرض الاطلاع على أكثر القطاعات أو المعلومات حساسية في مختلف أرجاء المنظمة وبالتالي قد يكون هناك تضارب في المصالح في مراحل المشروع أثناء العمل مع متعهدي خدمات لا يمكن ومع كل الضمانات إسناد مهام العمل الأمنية لهم. كما أن الاستثمار في مشاريع أنظمة حماية بمبالغ طائلة وعدم تأهيل كفاءات المنظمة نفسها لتشغيلها يعني هدر الأموال ودفعها إلى تقنيات وأجهزة قد يتوقف العمل عليها مجرد قطع العلاقة مع المتعهّد.

عدة عوامل تجعل الاستثمار في مشاريع أمن المعلومات أمراً ناجحاً مع ضرورة فهم أن نجاح أمن المعلومات لا يُحقّق نفس الرضى في نجاح المشاريع الأخرى، فالمقارنة هنا غير عادلة، فلا يمكن المقارنة بين مشروع انتهى ونجح بتحقيق أهدافه وبين عملية مُستمرة نتائجُها غير ملموسة.

يجب قياس مدى نجاح الاستثمار في أمن المعلومات بمدى دعم أمن المعلومات للأهداف الرئيسية المُعلَنة للمنظمة، فمثلاً إذا كان أحد أهدافها خدمة الزبائن بطريقة ما والاحتفاظ بمعلوماتِهم لتوفير هذه الخدمة، فمُهمّة أمن المعلومات تأمين هذه المعلومات من التسريب، الكشف، الضياع أو التلاعب حسب حساسيتها وعند الفشل في تأمين تلك المعلومات فإن الاستثمار المرتبط بذلك قد يواجه الفشل.

ويُمكن القول أخيراً إن أي خرق في أمن معلومات منظمة قد لا يكون فَشَلاً في الاستثمار بحد ذاته ولكنه في الغالب يكون نتيجة لعدم وجود فَهم كافي من قبل الإدارة العليا وتقصير في إدارة أمن المعلومات ككل.

الفصل الثالث: الإطار العمَلي

١,٣. مقدمة

تمَّ في الجزء النظري من هذا البحث عرضُ البعض من الدراسات التي تم تقديمها في نطاق مشابه، حيث تم تغطية المَبَاحث الثلاثة التالية:

- برنامج أمن معلومات
- دراسات الجدوى الاقتصادية ودورها في عملية اتّخاذ القرار
- المنظمة المُمَثِلة لحالة الدراسة وأهمية الدراسة بالنسبة لها

أما بالنسبة للجزء العَملي هذا فسوف يتم عرض للدراسة الميدانية التي تم العمل عليها في المنظمة متضمنةً معلومات حول الدراسات التسويقية والتقنية والمالية المتعلقة بذلك بالإضافة للخطة الزمنية المقترحة للتطبيق، وأخيراً النتائج والتوصيات المُنبثقة عن هذا البحث.

٢,٣. المُنظمة الإنسانية

تم تنفيذ هذا البحث من خلال دراسة حالة منظمة إنسانية تتمتَّع بالاستقلال المالي والإداري ذات شخصية اعتبارية وتعمل في الجمهورية العربية السورية. تَنشُط هذه المنظمة في القطّاع الطّبي حيث تُقدم المساعدات الطبية الأولية أو المتقدمة، وفي المجالات الخدمية والإغاثة، وضمن المجال المجتمعي والإنساني، بالإضافة لتقديم المساعدات المتعلقة بمشاريع المياه وإعادة الإعمار.

وكجزء من إدارة وتنظيم أعمالها تقوم المنظمة بتسجيل بيانات تفصيلية عن المستفيدين والعاملين والمتطوعين لديها وتحتفظ لهم بالسجلات والبيانات المطلوبة من الجوانب القانونية وجوانب إدارة الموارد البشرية. وتسعى المنظمة لتوفير الحماية اللازمة لهذه البيانات كونها تُعتَبر مهمّة وحساسة لأنها تتضمن طَيف واسع من المعلومات الشخصية والطبية والمالية والقانونية وغيرها.

٣,٣. الوضع الحالي

بهدف معرفة وضع المنظمَة الحالي المتعلّق بدرجة نُضجها في التعامل مع قضايا أمن المعلومات فقد تم إعداد استبيان خاص بذلك ثم عرضه ومناقشته مع المسؤول عن تقانة وأمن المعلومات في المنظمة (الملحق ١) وأخذ إجاباته على الأبعاد الأربعة الرئيسية التالية المرتبطة بتطبيق برنامج أمن المعلومات في المنظمة:

- حوكمة أمن المعلومات

- إدارة مخاطر أمن المعلومات
- موارد أمن المعلومات
- الامتثال والالتزام

وكانت النتائج كما يلي:

١,٣,٣. حَوكمة أمن المعلومات

النتائج (جدول (٣): نتائج استبيان أسئلة حوكمة أمن المعلومات):

الرقم	السؤال	الجواب
١	هل يوجد سياسات أمن معلومات مكتوبة في المنظمة؟	يتم العمل حالياً على إعداد سياسات وإجراءات
٢	ما الجوانب التي تغطيها هذه السياسات؟ (مثال: الأمن المادي، إدارة الدخول للموارد، الأمن البشري،...)	السياسات الأساسية مثل سياسة التغيير وإدارة الحوادث والاستخدام المقبول والأمن المادي، لوحظ عدم وجود بعض السياسات المُهمة مثل سياسة أمن الموارد البشرية
٣	كم عددها مصنفة إلى سياسات، إجراءات، دليل عمل، معايير أو غير ذلك؟	١٨ مقسمة إلى سياسات وإجراءات– لا يوجد معايير تقنية وأدلة عمل
٤	هل يتم إجراء مراجعة دورية وتحديث للسياسات؟	يتم وضعها حالياً لأول مرة
٥	هل يتم اعتماد السياسات من قبل الإدارة العليا للمنظمة بشكل دوري؟	يتم وضعها حالياً لأول مرة
٦	كيف يتعهد الموظفون رسمياً بالالتزام بسياسة أمن المعلومات؟	لا يوجد تعهد رسمي
٧	هل يوجد فريق متخصص بمتابعة التعديل والتحديث على السياسات الخاصة بأمن المعلومات لتلائم تطور أعمال المنظمة؟	فريق تقانة المعلومات نفسه
٨	ممن يتكون الفريق المشرف على سياسات أمن المعلومات (عدد موظفين وهيكلية وظيفية)؟	فريق تقانة المعلومات نفسه ١١ موظف إدارة عامة و١٣ دعم تقني في الفروع (هيكلية فريق تقانة المعلومات في ملحق ٢)
٩	كيف يتم تقديم مدى نضج المنظمة في مستوى أمن المعلومات للإدارة العليا ومجلس الإدارة ؟	عن طريق مهام وتقارير تدقيق خارجية
١٠	هل يوجد لجنة توجيهية لأمن المعلومات Security Steering Committee أو أي فريق يقود توجهات أمن المعلومات بمستوى عال في المنظمة؟	يتم تأسيس لجنة لهذا الغرض حالياً
١١	هل تضم اللجنة التوجيهية ممثلين من كافة أقسام المنظمة وأصحاب المصلحة؟	تضم حالياً تقانة المعلومات ورئاسة المنظمة وقسم التطوير الاستراتيجي

١٢	في حال عدم وجود لجنة توجيهية لأمن المعلومات، كيف يتم تنسيق احتياجات ونشاطات أمن المعلومات على مستوى المنظمة دون حدوث تعارض مع الأهداف الاستراتيجية والتشغيلية لها؟	يتم تحديد الاحتياجات بشكل سنوي في الشهر التاسع ومناقشتها مع رئاسة المنظمة وقسم التخطيط الاستراتيجي وتضمينها ضمن ميزانية السنة التالية بعد الموافقة عليها من الرئاسة
١٣	ما هي اللجان/الجهات التي تناقش وتعتمد مشاريع وخطط أمن المعلومات في المنظمة؟	يتم مناقشة المشاريع المخططة ضمن الميزانية مع المانحين من قبل مدير تقانة المعلومات لتأمين التمويل اللازم لها. لا يتم التنفيذ حتى يتم الحصول على موافقة على التمويل من قبل أحد المانحين
١٤	هل يتم اعتماد وثائق مكتوبة رسمية لتحديد نطاق عمل ومسؤولية وميثاق نشاطات أمن المعلومات (أي صيغة تفاهم مع الإدارة العليا حول هذه القضايا)؟	لا يوجد حالياً
١٥	ما هو الإجراء المعتمد لتطبيق التغييرات ضمن بيئة تكنولوجيا المعلومات (إجراء إدارة التغيير)؟	إبلاغ إدارة المنظمة عبر البريد الإلكتروني في حال وجود تأثير محتمل على الأعمال بسبب التغيير المنفذ
١٦	ما هو الإجراء المعتمد للاستجابة للحوادث المتعلقة بأمن المعلومات؟	يوجد خطة لإنشاء موقع استعادة من الكوارث
١٧	ما هو الإجراء المعتمد للإبلاغ ورفع التقارير المتعلقة بأمن المعلومات لأصحاب المصلحة والإدارة العليا ومجلس الإدارة؟	حسب الحاجة عن طريق البريد الإلكتروني أو الاجتماعات
١٨	هل يوجد خطة موثقة ومعتمدة للاستعادة من الكوارث؟	لا يوجد
١٩	هل يتم اختبار خطط الاستعادة من الكوارث دورياً؟	لا يوجد
٢٠	ما هو الإجراء المعتمد لمنح صلاحيات الوصول واستخدام الموارد التقنية للموظفين (إدارة الصلاحيات والوصول للموارد التقنية)؟	بريد إلكتروني من قسم الموارد البشرية لإنشاء الحساب وبريد آخر من إدارة الموظف لمنح الصلاحيات المطلوبة – لا يوجد نظام إدارة صلاحيات
٢١	كيف يتم تقييم نجاح/فشل نشاطات ومشاريع أمن المعلومات والعائد منها؟	من قبل فريق تقانة المعلومات
٢٢	هل يتم وضع خطط استراتيجية لتنفيذ نشاطات أو مشاريع متعلقة بأمن معلومات لعدة سنوات مقبلة بشكل مرتبط بخطط المنظمة ككل؟	يتم وضع الخطط بشكل سنوي لتأمين تمويل من المانحين – لا يوجد خطط لعدة سنوات
٢٣	كيف تحصل مثل هذه الخطط على الدعم اللازم من الإدارة والأطراف ذات العلاقة لتحويلها إلى واقع؟	موافقة من الإدارة – تأمين تمويل من المانحين – تنفيذ
٢٤	هل يوجد سياسة خاصة بالاستخدام المقبول للموارد التقنية من قبل المستخدم النهائي؟	قيد الإعداد حالياً

٢٥	هل يوجد سياسة معتمدة تضمن تطبيق أفضل المعايير والممارسات والإعدادات الآمنة على الأنظمة التقنية المختلفة؟	لا يوجد – يتم تطبيق المعايير وفق الاجتهاد الشخصي لكل موظف

تحليل النتائج:

من الواضح وجود ضَعف في حوكمة أمن المعلومات في المنظمة واعتمادها في الأغلب على مبدأ التنفيذ عند الحاجة أو عند الطّلب بشكل عام مع وجود بعض الاستثناءات. لذلك فمن الملاحظ أن درجة نُضج الحوكمة مُنخفضة حيث أن النشاطات المتعلقة بحوكمة أمن المعلومات في المنظمة هي عشوائية وغير منتظمة عموماً.

وعليه فالنقاط الأساسية التي يجب تداركها لتحسين واقع المنظمة من حيث حوكمة أمن المعلومات هي:

- تشكيل سياسات وإجراءات ومعايير تُغطّي كافة الجوانب المهمة لأمن المعلومات ومراجعتها واعتمادها بشكل دوري من قبل فريق متخصص
- تعهُّد كافة الوظفين بالالتزام بهذه السياسات بعد اطلاعهم عليها وفهمَهم لها
- إنشاء لجنة توجيهية على مستوى الإدارة العليا وممثلين من قبل أصحاب المصلحة تهدُف للإشراف ومتابعة نشاطات أمن المعلومات وتُخَطط لها
- إعداد ميثاق خاص بأمن المعلومات يُحدِد نطاق عمل ومسؤولية فريق أمن المعلومات واعتماده من قبل الإدارة
- التركيز على خطط الاستعادة من الكوراث واستمرارية العمل
- وضع خطط استراتيجية لعدة سنوات متعلقة بمشاريع ونشاطات أمن المعلومات ضمن برنامج متكامل

٢,٣,٣. إدارة مخاطر أمن المعلومات

النتائج (جدول (٤): نتائج استبيان أسئلة إدارة مخاطر أمن المعلومات):

الرقم	السؤال	الجواب
١	ما التأثير المتوقع من حصول حادثة تسريب/ سرقة بيانات حساسة لخارج المنظمة؟	تأثير على سمعة المنظمة، وقف تمويل من قبل الجهات المانحة، معاقبة الموظفين المتسببين، قد يتم رفع دعوى قضائية للتعويض من قبل المتضررين
٢	ما التأثير المتوقع من حصول حادثة ضياع/ فقدان بيانات حساسة؟	تأثير على سمعة المنظمة، جهد ووقت كبيرين لإعادة جمع البيانات (كلفة)

٣	ما التأثير المتوقع من حصول حادثة تلاعب/ تعديل غير مشروع ببيانات حساسة؟	قد يؤدي التلاعب إلى حدوث خسارة مالية تأثير على سمعة المنظمة
٤	ما التأثير المتوقع من حصول حادثة خروج أنظمة تقنية عن الخدمة لفترة طويلة نسبياً؟	توقف جزء كبير من نشاطات وأعمال المنظمة الإغاثية والمتعلقة بالدعم الطبي، توقف التعاملات المالية كصرف الشيكات
٥	كيف يتم تحديد مستوى مخاطر أمن المعلومات المقبول من قبل الإدارة العليا ومجلس الإدارة؟	عن طريق مهام وتقارير تدقيق خارجية
٦	كيف يتم مراجعة وتسجيل ومتابعة المخاطر المتعلقة بأمن المعلومات؟	لا يوجد
٧	هل يوجد إجراء معتمد حول إدارة مخاطر أمن وتكنولوجيا المعلومات؟	لا يوجد
٨	هل يوجد فريق متخصص بمتابعة مخاطر أمن وتكنولوجيا المعلومات (العدد والهيكلية والدور الذي يلعبه في حال وجوده)؟	لا يوجد
٩	كيف تنظم العلاقة مع الموردين الخارجيين الذين يقدمون خدمات متعلقة بالأنظمة المعلوماتية (توريد أو دعم فني أو تشغيل أو إدارة أنظمة أو غيرها من الخدمات الخارجية)؟	عن طريق توقيع عقود رسمية واتفاقيات مستوى خدمة Service Level Agreement (SLA)
١٠	كيف يتم تنظيم العلاقة مع الموردين الذين تقوم المنظمة بتعهيد وظائف تكنولوجيا المعلومات لهم أو استضافة بيانات أو أنظمة تقنية لديهم في حال وجودهم؟	عن طريق الاستعانة بجهة خارجية لمراجعة وتدقيق ضوابط أمن المعلومات
١١	كيف يتم اكتشاف وتصحيح الثغرات الأمنية ضمن الأنظمة المعلوماتية؟	لا يوجد طريقة متبعة حالياً
١٢	كيف يتم التعامل مع نتائج نشاطات التدقيق أو فحص الاختراق الذي تنفذه أطراف خارجية مستقلة؟	يتم العمل على تصحيحها وإغلاقها حسب درجة خطورتها
١٣	كيف يتم التعامل مع المخاطر التي تتجاوز المستوى المقبول أو تنتهك سياسات أمن المعلومات المعتمدة؟	يتم إعلام إدارة المنظمة عبر البريد الإلكتروني

تحليل النتائج:

يُولي فريق المُنظمة اهتماماً مقبولاً تجاه مخاطِر أمن المعلومات رغم أن ذلك يجري بطريقة غير مُنَظمة بالقدر الكافي. ومن الواضح أن لحوادث أمن المعلومات (في حال وقوعها) تأثير بالغ الخطورة على مصَالح المنظمة وأعمالها ما قد يطَال جوانب مالية وقانونية (قضائية) بالإضافة لأثرها المباشر على سُمعة المنظمة ومكانتها خاصة أمام المستفيدين والمانحين.

لتحسين وضع المنظمة في هذا الجانب لا بد من النظر في الأمور الآتية:

- تشكيل إجراء معتمد لإدارة مخاطر أمن المعلومات ومراجعته واعتماده بشكل دوري.

- إسناد مهام إدارة مخاطر أمن المعلومات إلى فريق متخصص بإدارة هذه الأنواع من المخاطر يقوم بالمتابعة والبحث واكتشاف أية مخاطر جديدة تتعرض لها المنظمة.
- الاحتفاظ بسجل يحوي كافة مخاطر أمن المعلومات المُكتشفة التي تهدد المنظمة ودرجة خطورة كل منها ومراجعته وتحديثه باستمرار.
- التركيز على المخاطر ذات التأثير الأعلى كالمخاطر المتعلقة بالعمل مع موردين خارجيين وإدارة ثغرات أمن المعلومات ضمن الأنظمة التقنية أو غيرها من المخاطر التي تعتبرها المنظمة ذات تأثير كبير على أداء نشاطاتها.
- إبقاء إدارة المنظمة العليا واللجنة التوجيهية لأمن المعلومات على اطلاع دائم على مخاطر أمن المعلومات التي تهدد المنظمة والطرق المتَّبعة في التعامل معها.

٣,٣,٣. موارد أمن المعلومات

النتائج (جدول (٥): نتائج استبيان أسئلة موارد أمن المعلومات):

الرقم	السؤال	الجواب
١	هل يوجد فريق متخصص بأمن المعلومات في المنظمة أم تسند مهام أمن المعلومات لموظفين لهم أدوار أخرى؟	لا يوجد فريق مختص، يقوم فريق تقانة المعلومات بمهام فريق أمن المعلومات
٢	ما الأدوار الوظيفية التي يمارسها فريق أمن المعلومات؟	مراجعة حسابات المستخدمين بشكل أساسي
٣	هل يوجد توصيف وظيفي مكتوب لكل دور وماذا يتضمن في حال وجوده؟	لا يوجد
٤	هل يتبع فريق أمن المعلومات تنظيمياً لإدارة التكنولوجيا أو أي إدارة تشغيلية أخرى؟	نفس موظفي قسم تقانة المعلومات
٥	هل يوجد تصنيف لأنظمة تقانة المعلومات والبيانات حسب أهميتها لأعمال المنظمة؟	نعم يوجد تصنيف لتمييز الأصول المهمة بالنسبة للمنظمة
٦	هل هناك تحديد ملكية واضح ورسمي للأصول التقنية والمعلومات ضمن المنظمة؟	نعم يوجد تحديد ملكية للأصول التقنية والمعلومات
٧	هل تستثمر المنظمة حالياً أياً من أنظمة/ضوابط أمن المعلومات التالية: Endpoint security Firewalls Intrusion detection/preventing systems Data encryption (at rest in transit and in use) Multi factor authentication VPN for remote access	 نعم نعم ضمن وظائف الجدار الناري نفسه نعم لا نعم

	Security information and event management SIEM	يوجد خطة للحصول على SIEM system قريباً
	Vulnerability scanning and penetration testing tools	يتم الحصول عليها كخدمة من قبل جهة خارجية
	Data leak prevention DLP	لا
	Identity and access management systems	لا
	Endpoint Detection and Response (EDR)	لا
	Email Security Gateway	نعم
	Web Application Firewall (WAF)	تحت التطبيق حالياً
	Proxy Server	تحت التطبيق حالياً
	Privileged Access Management (PAM)	لا
	Network Access Control (NAC)	لا
	Physical access controls	نعم – جهاز بصمة للدخول وكاميرات مراقبة
٨	هل يوجد ميزانية سنوية معتمدة مستقلة ومخصصة لتنفيذ خطط مشاريع ونشاطات متعلقة بأمن المعلومات؟	نعم يوجد ميزانية سنوية معتمدة لكنها مشروطة بموافقة المانحين على التمويل
٩	ما الآلية أو الإجراء المتبع لتحديد ميزانية أمن المعلومات السنوية والموافقة عليها؟	يتم إعداد الميزانية خلال آخر ٣ أشهر من كل سنة ميلادية ويتم التنفيذ حسب توافر التمويل من قبل الجهات المانحة
١٠	ما درجة صعوبة إقناع إدارة المنظمة بتمويل مشاريع ونشاطات أمن المعلومات؟	إدارة داعمة تقتنع بضرورة الحصول على التمويل اللازم لتنفيذ مشاريع أمن المعلومات
١١	هل يتم تحديد التمويل اللازم وفق خطط استرتيجية متفق عليها مع الإدارة أو بشكل منفرد لكل نشاط أو مشروع حسب الحاجة أو استجابة لمتطلبات آنية؟	بشكل منفرد بالتنسيق مع قسم التطوير الاستراتيجي في المنظمة
١٢	ما العوامل التي تؤثر على قبول أو رفض مشاريع أو نشاطات أمن المعلومات من قبل الإدارة العليا أو اللجنة المختصة؟ الرجاء ترتيبها وفق الأهمية	توافر التمويل اللازم، العقوبات والحظر المفروض على سوريا

تحليل النتائج:

تشير الهيكلية الإدارية ومهام أمن المعلومات الموكّلة لموظفي قسم تقنية المعلومات الذين ينفذون مهام متعلقة بأمن المعلومات بالإضافة لمهامهم التشغيلية أن أدوار أمن المعلومات لا تزال ثانوية وهامشية ضمن المنظمة وهي عُرضة لتضارب كبير في المصالح لأنه عادةً ما تكون لفريق أمن المعلومات دور رقابي على نشاطات تقانة المعلومات ضمن أي منظمة.

ومن الجانب التقني تمتلك المنظمة بعض أنظمة أمن المعلومات المهمة إلا أنها بحاجة لتوفير التمويل اللازم لبعض الأنظمة الضرورية الأخرى ضمن خطة زمنية تُراعي الأهمية.

فيما يلي النقاط التي يجب التركيز عليها لتحسين وضع المنظمة فيما يتعلق بموارد أمن المعلومات:

- توظيف فريق مختص لمتابعة مشاريع ونشاطات أمن المعلومات وعادة ما يعتبر قسم أمن المعلومات على أنه من الوظائف التنظيمية وقدرته على العمل بشكل فعّال يتعارض مع كونه تابعاً لوظائف من المفترض أن يكون رقيباً عليها لذلك يوصى بأن يكون قسم أمن المعلومات مستقل عن الوظائف التي تتعارض مع أداء نشاطه بفعالية.
- إنشاء أدوار وتوصيف وظيفي واضح لقسم أمن المعلومات
- إطلاق مشاريع لتوريد وتركيب أنظمة أمن المعلومات التالية:
  - Multi factor authentication
  - SIEM
  - Vulnerability scanning and penetration testing tools
  - Data leak prevention DLP
  - Identity and access management systems
  - Endpoint Detection and Response (EDR)
  - Privileged Access Management (PAM)
  - Network Access Control (NAC)
- وضع خطة استراتيجية لعدة سنوات وأخذ موافقة إدارة المنظمة واللجنة التوجيهية للحصول على الموارد اللازمة لبرنامج أمن المعلومات المقترح وتسهيل تمويلها.

٤,٣,٣. الامتثال والالتزام

النتائج (جدول (٦): نتائج استبيان أسئلة الامتثال والالتزام):

الرقم	السؤال	الجواب
١	هل تم تنفيذ فحص اختراق للأنظمة التقنية خلال آخر ١٢ شهر وما تقييمكم للنتائج في حال وجودها؟	لم يتم تنفيذ فحص اختراق للأنظمة التقنية خلال الفترة الأخيرة
٢	هل يتم تنفيذ فحص الاختراق للأنظمة التقنية بشكل دوري أم عند الطلب فقط؟	يتم التنفيذ عند الطلب فقط
٣	ما المستويات التي يتم تنفيذ فحص الاختراق للأنظمة التقنية عليها ؟ (مثال: داخلي – خارجي – لاسلكي – تطبيقات ...)	لم يتم تنفيذ أي فحص اختراق مؤخراً
٤	هل يتم تنفيذ فحص الاختراق للأنظمة التقنية من قبل جهة مستقلة أو فريق داخلي؟	لم يتم تنفيذ أي فحص اختراق مؤخراً
٥	هل تم تنفيذ تدقيق على أنظمة المعلومات خلال آخر ١٢ شهر وما تقييمكم لنتائج آخر تدقيق في حال وجودها؟	نعم – يوجد عدد كبير من التوصيات التي يتم العمل على تحقيقها تتلخص بوضع سياسات

		وإجراءات، إغلاق الثغرات التي ظهرت عند مسح الأنظمة التقنية وتطبيق برنامج SIEM
٦	هل يتم تنفيذ تدقيق على أنظمة المعلومات دورياً أم عند الطلب فقط؟	يتم التنفيذ بشكل دوري كجزء من التدقيق المالي للمنظمة
٧	هل يتم تنفيذ تدقيق على أنظمة المعلومات من قبل جهة مستقلة خارجية أو فريق داخلي ضمن المنظمة؟	من قبل جهة خارجية مستقلة
٨	هل يوجد فريق تدقيق تكنولوجيا معلومات داخلي متخصص ضمن المنظمة؟	لا يوجد فريق تدقيق تكنولوجيا معلومات داخلي
٩	ما الدور الذي يلعبه فريق التدقيق الداخلي في التحقق من الالتزام بالسياسات الخاصة بأمن المعلومات في المنظمة؟	لا يوجد فريق تدقيق تكنولوجيا معلومات داخلي
١٠	كيف يتم إجراء مراجعات لحسابات المستخدمين على أنظمة تقانة المعلومات؟	بشكل دوري من قبل فريق تقانة المعلومات
١١	هل يتم إجراء مراجعات لحسابات المستخدمين على أنظمة تقانة المعلومات بشكل دوري أم عند الحاجة فقط؟	بشكل دوري من قبل فريق تقانة المعلومات وكذلك عند الحاجة
١٢	كيف يتم إجراء مراجعات إعدادات الأنظمة التقنية؟	تتم من قبل فريق تقانة المعلومات
١٣	هل يتم إجراء مراجعات إعدادات الأنظمة التقنية بشكل دوري أم عند الحاجة فقط؟	عند الحاجة فقط
١٤	ما الطرق المتبعة للتحقق من الالتزام بالسياسات الموضوعة؟	لا يوجد طرق محددة للتحقق من ذلك حالياً
١٥	ما الجهود التي تبذل في سبيل نشر ثقافة أمن معلومات لدى كل الموظفين على مستوى المنظمة؟	لا يوجد جهود مركزة على ذلك حالياً
١٦	كيف يتم ضمان التزام الموظفين الجدد بسياسات أمن المعلومات؟	يتم حالياً وضع برنامج تدريب متعلق بأمن المعلومات للموظفين الجدد
١٧	هل يتم إبلاغ الفريق المسؤول عن أمن المعلومات بحالات خروقات مشتبهة من قبل المستخدمين النهائيين؟	عادة يتم الإبلاغ من قبل المستخدمين النهائيين عند وجود أي شك
١٨	ما عدد إبلاغات المستخدمين النهائيين عن حالات متعلقة بأمن المعلومات خلال النصف الأول من السنة الحالية؟	حوالي ١٢
١٩	كيف يطّلع الموظفون على سياسات أمن المعلومات في المنظمة؟	يتم التخطيط لذلك عند جهوزية السياسات
٢٠	ما هي نشاطات التدريب الداخلية أو الخارجية المنفذة للموظفين حول أمن المعلومات؟ هل يشمل التدريب المتعلق بأمن المعلومات فئة معينة من الموظفين أم يغطي كافة موظفي المنظمة؟	تدريب لكل موظفين الإدارة العامة خلال النصف الأول من السنة الحالية على معايير أمن المعلومات ISO27001، وتدريب خاص متقدم لفريق تقنية المعلومات
٢١	هل يوجد أية معايير متبعة في سياسات أمن المعلومات (مثال ISO 27001)	يتم حالياً البدء بتطبيقها من خلال السياسات التي يجري وضعها

٢٢	هل يتم الاحتفاظ بنسخ احتياطية من البيانات الحساسة في مكان آمن وخارج مركز المعلومات بشكل دوري؟	لا يتم حالياً
٢٣	ما الطرق المتبعة لتقييم ومراجعة التقدم أو التطور في مشاريع ونشاطات أمن المعلومات في المنظمة؟	تقييم شخصي من قبل فريق تقانة المعلومات
٢٤	هل يتم مشاركة الإدارة العليا وأصحاب المصلحة بتطور مشاريع ونشاطات أمن المعلومات دورياً؟	نعم يتم ذلك
٢٥	ما آلية التواصل المتبعة لمشاركة المعلومات المتعلقة بتطور مشاريع ونشاطات أمن المعلومات مع الإدارة العليا وأصحاب المصلحة داخل المنظمة؟	عن طريق البريد الإلكتروني أو الاجتماعات عند الضرورة

تحليل النتائج:

يتبيَّن من خلال الإجابات على الاستبيان وجود محدودية في الالتزام والامتثال للسياسات والإجراءات والمعايير وذلك بسبب عدم وجود نسخ نهائية مُعتَمدة ومُطبقة من هذه السياسات من جهة وضَعف في الوعي العام لدى موظفي المنظمة تجاه مخاطر أمن المعلومات وكيفية التعامل معها.

لتحسين وضع الالتزام والامتثال ضمن المنظمة من الضروري أن يتم تحقيق ما يلي:

- الانتهاء بالسرعة القصوى من إعداد السياسات والإجراءات والمعايير واعتمادها (يفضل أن تكون مبنية على معايير مُعتَمَدة عالمياً وفق أفضل الممارسات) وشرح ما يلزم منها للموظفين حسب احتياجات كل موقع وظيفي وتوقيع كل موظف على تَعهُّد بالتزامه بهذه السياسات.
- وضع خطة دورية لتنفيذ عمليات تقييم أمن المعلومات من قبل جهة مستقلة بما في ذلك المراجعات الداخلية المتنوعة (مثل مراجعة حسابات المستخدمين وإعدادات الأنظمة ..)، فحوصات الاختراق، تدقيق أنظمة المعلومات وغيرها من النشاطات التي تُعزز الامتثال والالتزام بالسياسات والمعايير المُعتمَدة.
- إنشاء برنامج توعية مُستمر يسعى لنشر ثقافة أمن المعلومات على مستوى المنظمة ككل وفق مبدأ (أمن المعلومات هو مسؤولية الجميع في المنظمة)، ويمكن أن يتم ذلك بطرق متنوعة كجلسات التدريب ورسائل التوعية وغيرها. يجب أن يتضمن هذا البرنامج جزء خاص بالموظفين الجدد لرفع سوية الوعي تجاه أمن المعلومات لديهم بما يتماشى مع السياسات المُعتمدة.
- إبقاء إدارة المنظمة واللجنة التوجيهية لأمن المعلومات على اطلاع دائم بنشاطات ومشاريع أمن المعلومات المتعلقة بتعزيز الالتزام والامتثال.

٤,٣. نتائج الدراسات

بناء على ما تَقدَّم توجَّبَ وضع الدراسات التالية لتطبيق برنامج أمن معلومات فعّال ضمن المنظمة ينقلها من الوضع الراهن إلى الوضع المستقبلي المنشود لمستوى أفضل من أمن المعلومات:

١,٤,٣. الدراسة التسويقية

تتعلق احتمالية رفض اقتراح الاستثمار في أمن المعلومات في مرحلة اتخاذ القرار بأساليب وقدرات المنظمة على تحديد ومناقشة هذا الاقتراح، ومستوى المعرفة حول أمن المعلومات لدى الإدارة. لذلك فمن المهم تسويق نشاطات ومشاريع أمن المعلومات بالشكل الأمثل أمام متَّخذي القرار والمانحين للحصول على دعمِهم المُستمر لهذه النشاطات.

من المهم زيادة الوعي لدى الإدارة بأهمية تبني برنامج أمن المعلومات عن طريق التواصل المستمر مع متخذي القرار وتزويدهم بكل ما هو جديد عالمياً فيما يتعلق بتطورات ومخاطر أمن المعلومات. فعلى سبيل المثال يمكن طرح بعض من الاحصائيات المنشورة رسمياً من قبل بعض المؤسسات والجهات المختصة دولياً كالإشارة إلى أن خسائر العالم من جرائم الإنترنت المسجلة خلال عام ٢٠٢١ بلغت ٦,٩ مليار دولار أمريكي، وأن الجرائم المالية الإلكترونية قفزت بنسبة ٦٤% في ٢٠٢١، وأن متوسط الوقت اللازم لتحديد الخرق واحتوائه هو ٢٨٧ يوم، وغيرها العديد من الأمثلة التي تدعم موقف الإدارة في تبنيها لبرامج أمن المعلومات. ومن جانبٍ آخر، فقد بلغ متوسط كلفة حوادث تسريب البيانات على المؤسسات في سنة ٢٠٢١ (وفق تقرير Cost of a Data Breach Report 2021 – IBM) ٤,٢٤ مليون دولار أمريكي، كما أن متوسط كلفة حوادث فقدان بيانات المؤسسات في سنة ٢٠٢١ عن طريق الإصابة بفايروس الفدية فقط (وفق نفس التقرير) هو ٤,٦٢ مليون دولار أمريكي. فإذا اتخذنا من هذه الأرقام قيماً مرجعية فسوف نلاحظ أن وقوع حادثة واحدة من هذا النوع سيُكلّف المنظمة ما يقارب ثلاثة أضعاف الكلف التقديرية التي تم وضعها لتمويل برنامج أمن المعلومات المقترح تطبيقه على مدى أربع سنوات.

لذلك فما ينبغي الاهتمام بتنفيذه وتحويله إلى واقع في الإطار التسويقي يتضمن:

- تشكيل سياسات وإجراءات ومعايير:

تُعتبر سياسات أمن المعلومات المعتمَدة في المنظمة الهيكل الأساسي لبنية برنامج أمن المعلومات ويتم بناء كل المشاريع والنشاطات المختلفة عليها. كما أنها تساعد في إيضاح وإبراز تبنّي الإدارة

العليا لنشاطات أمن المعلومات على مستوى المنظمة ككل وهذا سيساهم حتماً بتسهيل مهام الفريق المسؤول عن تطبيق وتنفيذ وفرض سياسات ونشاطات أمن المعلومات ضمن المنظمة.
تقوم المنظمة حالياً بإنشاء عدد من السياسات والإجراءات بمساعدة جهة خارجية متعاقد معها لإنجاز ذلك ومن ثم اعتمادها والبدء بتطبيقها، حيث يتطلب ذلك جهود مستمرة لمراجعة وتعديل واعتماد هذه السياسات دورياً وإضافة ما يلزم منها مستقبلاً للحصول على إطار حوكمة متكامل ضمن المنظمة. لذلك فقد تم إضافة كلف تقديرية سنوية لتغطية مثل هذه الخدمات ضمن الدراسة المالية.

- توقيع تعهد كافة الموظفين بالالتزام بهذه السياسات:

عادة ما يتم ذلك من خلال التنسيق مع قسم الموارد البشرية لإضافة هذا الضابط وتطبيقه على كل الموظفين العاملين ضمن المنظمة وحتى على بعض الجهات الخارجية التي توفد موظفيها للعمل ضمن بيئة المنظمة التقنية وفق عقود محددة. يُساعد ذلك المنظمة في جانبين: الأول هو الجانب القانوني حيث يُمَّكنها ذلك من محاسبة أي منتهكين لسياساتها المعتمدة من الموظفين ومواجهة ذلك قضائياً عند اللزوم، والثاني هو تحفيزي يساعد في تحريض الموظفين على الاطلاع على سياسات المنظمة المعتمدة وفهمها والالتزام بها، ونشر الثقافة التي تسوِّق إلى أن أمن المعلومات هو مسؤولية كل العاملين ضمن المنظمة وليس جزء منهم فقط، وهو ما يمكن اعتباره جانب تسويقي لنشاطات برنامج أمن المعلومات على مستوى كافة الموظفين يدفعهم لرفع درجة وعيهم الأمني تجاه تلك النشاطات والمساهمة الفعّالة فيها.

- إنشاء لجنة توجيهية لأمن المعلومات وإعداد ميثاق خاص بأمن المعلومات:

وجود ميثاق مكتوب ومتفق عليه مع إدارة المنظمة واللجنة التوجيهية لتحديد نطاق عمل ونشاطات فريق أمن المعلومات ضمن المنظمة يساهم بشكل جدّي في تنظيم تلك النشاطات ومنح الفريق المختص الصلاحيات الضرورية لفرض السياسات عند اللزوم. ويساعد ذلك أيضاً في إظهار اهتمام الإدارة وتبنيها لتلك النشاطات وهو بحد ذاته ما يُعتبَر جانب تسويقي هام تجاه كافة العاملين ضمن المنظمة بالإضافة إلى أنه يضمن التوافق الاستراتيجي ما بين نشاطات أمن المعلومات من جهة وأهداف المنظمة وخططها من جهة أخرى وذلك من خلال مناقشة كل ما يتعلق بأمن المعلومات ضمن اجتماعات اللجنة التوجيهية وأخذ ملاحظات كافة الأطراف ذات العلاقة عليها بعين الاعتبار.

- وضع خطط استراتيجية لعدة سنوات:

بالإضافة للجانب التنظيمي لوضع خطط استراتيجية طويلة الأمد تغطي كل فترة تطبيق البرنامج، فإن ذلك من جهة ثانية يساعد في تسويق نشاطات ومشاريع أمن المعلومات أمام الجهات المانحة صاحبة القرار بالتمويل ويعطي الإنطباع الثابت بأن المنظمة تسير باتجاه واضح ضمن الخطط المرافقة لبرنامج أمن المعلومات مما يُسهّل الحصول على موافقات التمويل على عدة سنوات متلاحقة.

- وضع هيكلية وتوصيف وظيفي واضح لوظائف أمن المعلومات:

بالإضافة لدعمه الجانب الإداري والتنظيمي، يساهم ذلك في إسناد المسؤوليات بشكل واضح لعناصر الفريق المكلف بمتابعة نشاطات أمن المعلومات وفق الدور المُسند لكل منهم ومحاسبتهم لاحقاً وفق مصفوفة تقييم أداء مُتَّفق عليها معهم بشكل مسبق مما يمنح هؤلاء رؤية واضحة للمهام الموكلة إليهم وطُرق تقييم نتائجها.

- توعية، تدريب وتأهيل:

حتى الآن يعتبر العامل البشري الحلقة الأضعف ضمن سلسلة ضوابط أمن المعلومات لذلك فإن وضع خطط تدريب مستمر على مستويين الأول يشمل كافة موظفي المنظمة بهدف نشر الثقافة الجديدة ورفع الوعي الأمني لديهم والثاني للموظفين التقنيين المختصين بهدف رفع مهاراتهم وتمكينهم من مواكبة كل جديد في مجال عملهم. لقد تم إضافة ميزانية سنوية مخصصة للتدريب ضمن الخطة المالية.

٢,٤,٣. الدراسة التقنية

تتضمَّن الدراسة التقنية لبرنامج أمن المعلومات المقترح للمنظمة ما يلي:

- موارد بشرية تقنية – توظيف خمسة مهندسي أمن معلومات:

سوف يعمل مهندسو أمن المعلومات على تغطية الأدوار الأساسية التالية ضمن نشاطات برنامج أمن المعلومات في المنظمة (يمكن أن يُسنَد للفريق أدوار أخرى ضرورية حسب الحاجة أثناء التقدم في تطبيق البرنامج):

١. متابعة المهام المتعلقة بحوكمة وإدارة مخاطر أمن المعلومات بما في ذلك المراجعة والاعتماد الدوري للسياسات والإجراءات والمعايير والتحديث المستمر لسجل المخاطر المتعلقة بأمن المعلومات.

٢. تشغيل وضبط وتحديث أنظمة أمن المعلومات التقنية المستخدمة ضمن المنظمة والمساهمة في تطبيق الأنظمة الجديدة المقترحة ضمن البرنامج وتشغيلها.

٣. تعزيز ثقافة أمن المعلومات على مستوى المنظمة ككل من خلال برامج توعية مخططة ومدروسة ومستمرة مع التركيز على الموظفين الجدد.
٤. المراقبة المستمرة لمعطيات الأنظمة والشبكات المعلوماتية ضمن المنظمة وتحليلها لاكتشاف أية نشاطات مشبوهة واتخاذ الإجراءات اللازمة لتفادي أية حوادث أمنية مرتبطة بها قبل حدوثها.
٥. المشاركة مع الفِرَق التقنية المختصة بالاستجابة لحوادث أمن المعلومات واستعادة الوضع الطبيعي.
٦. تجهيز ورفع تقارير دورية للإدارات ذات الصلة في المنظمة حول مخاطر أمن المعلومات التي تتعرض لها المنظمة ومستوياتها الحالية وطرق وخطط التعامل معها.
٧. تعزيز الامتثال والالتزام بسياسات أمن المعلومات وأفضل الممارسات المُعتمَدة من خلال تنفيذ المراجعات الدورية المستمرة على أنظمة وعناصر وإعدادات بيئة العمل الفعلية والتأكد من تطبيقها بشكل صحيح وآمن.

يمكن أن يتم توظيف مهندسي أمن المعلومات المختصين بشكل تدريجي مع التقدم بتطبيق برنامج أمن المعلومات وازدياد متطلباته، ومن المقترح أن يتم البدء بتوظيف مهندسَين اثنين في كل من السنة الأولى والثانية من بدء تطبيق البرنامج ومهندس واحد إضافي في السنة الثالثة.

سيكون التركيز ضمن السنة الأولى على الأدوار من ١ إلى ٣ المشار لها أعلاه وفي السنة الثانية سيتم إضافة بقية الأدوار من ٤ إلى ٧ تدريجياً مما يتطلب الزيادة المذكورة في الموارد البشرية لتلبية متطلبات البرنامج المتصاعدة.

- موارد تقنية – توريد أنظمة تقنية:

يوجد طيف واسع من الأنظمة التقنية التي تساعد في تعزيز أمن المعلومات في المنظمة وتنتقل بها إلى موقع استباقي في مواجهة مخاطر حوادث أمن المعلومات ولعلَّ من أهم الأنظمة الضرورية للمنظمة خلال السنوات الأولى من تطبيق برنامج أمن المعلومات ما يلي:

Multi factor authentication	هي طريقة مصادقة إلكترونية يتم فيها السماح للمستخدم بالوصول إلى الموارد التقنية فقط بعد تقديمه دليلين أو أكثر من آليات المصادقة من طبيعة مختلفة مما يعزز ضبط الوصول للموارد من قبل المصرح لهم فقط.
SIEM	برنامج يقوم بتجميع المعلومات الأمنية وسجلات الأحداث من مصادر مختلفة ومتنوعة ضمن البيئة التقنية وتنظيمها وتحليلها

	واستنتاج تنبيهات الأمان في الوقت الفعلي غالباً مما يساعد في اكتشاف التهديدات والحوادث الأمنية ومعالجتها.
Vulnerability scanning tools	ماسح الثغرات الأمنية هو نظام تقني مصمم لمراجعة أنظمة التشغيل أو الشبكات أو التطبيقات بحثاً عن نقاط ضعف معروفة ضمن هذه العناصر التقنية وتصحيحها تفادياً لاستغلالها من قبل المخترقين.
Data leak prevention DLP	يكتشف هذا البرنامج عمليات نقل البيانات الحساسة بالنسبة للمنظمة ويمنع محاولات تسريبها للخارج من خلال مراقبة واكتشاف وحظر أية عملية مشبوهة أثناء الاستخدام والنسخ والتخزين للبيانات.
Identity and access management systems	تسهل أنظمة إدارة الهوية والوصول (IAM) إدارة الهويات الإلكترونية أو الرقمية. وتُمكّن مشرفي تكنولوجيا المعلومات من التحكم في وصول المستخدمين إلى المعلومات الحساسة داخل المنظمة.
Endpoint Detection and Response (EDR)	هو نظام يقوم بجمع وتحليل المعلومات المتعلقة بالتهديدات الأمنية من أجهزة الحواسب والطرفيات الأخرى، بهدف العثور على أية خروقات أمنية فور حدوثها وتسهيل الاستجابة السريعة للتهديدات المكتشفة أو المحتملة.
Privileged Access Management (PAM)	هو نظام لأمن المعلومات تحمي الحسابات ذات صلاحيات الوصول الخاصة أو ذات القدرات التي تتجاوز المستخدمين العاديين وتحد من قدرتها على التخريب أو الاستخدام الخاطئ مثل حسابات مدراء الأنظمة.
Network Access Control (NAC)	يحظر هذا النظام الوصول من الأجهزة الطرفية التي لا تتوافق مع سياسات أمن المنظمة ويضمن بذلك عدم تمكن البرمجيات الخبيثة من الدخول إلى الشبكة من جهاز لا ينتمي لشبكة المؤسسة.

ونظراً للتكاليف المرتفعة المرافقة للحصول على مثل هذه الأنظمة التقنية وتفادياً للمُمانعة التي قد تنشأ لعدم توفُّر التمويل اللازم فقد تم توزيع توريدها على أربع سنوات ميلادية تبدأ منذ إطلاق برنامج أمن المعلومات المُخَطّط (كما هو موضح تفصيلاً في فقرة الدراسة المالية اللاحقة)، مما يساهم في تخفيض الميزانية السنوية المطلوبة لتنفيذ البرنامج ويعزز فرص الحصول على التمويل اللازم.

- موارد بشرية تقنية إضافية – عقود أمن معلومات خارجية:

يتضمن ذلك الاستعانة بالخبرات والخدمات اللازمة لتنفيذ مهام برنامج أمن المعلومات المخططة من خلال اتفاقيات أو عقود مع مزودي خدمات خارجيين وشركات متخصصة بخدمات أمن المعلومات لتقديم ما يلي بشكل دوري أو عند الطلب:

- الدعم الفني والتقني الضروري لعمل أنظمة أمن المعلومات التقنية
- فحوصات الاختراق للأنظمة التقنية
- تدقيق أنظمة المعلومات وتقييم المخاطر
- الاستجابة لحوادث أمن المعلومات التي قد تحتاج لتدخل من قبل أشخاص ذوي خبرات غير متوفرة ضمن فريق عمل المنظمة
- الاستشارات المتعلقة بمواضيع أمن المعلومات

- إدارة مخاطر – إنشاء مركز استعادة من الكوراث:

مركز الاستعادة من الكوراث هو مكان مُجهَّز مسبقاً يُمَكّن المنظمة من الانتقال إليه مؤقتاً بعد حادثة أمن معلومات أو كارثة طبيعية أدت لخروج المركز الرئيسي عن العمل. ويُعتبر هذا الموقع عادة أحد الأجزاء المهمة من خطة المنظمة لاستعادة القدرة على العمل بعد الكوارث أو ما تدعى أحياناً بخطة استمرارية الأعمال.

يتم إنشاء مركز الاستعادة من الكوراث هذا بحيث يلبي احتياجات المنظمة الأساسية ويضمن استمرارية الخدمات والأنظمة التقنية الأكثر أهمية بالنسبة لها والتي تؤدي في حال توقفها إلى تبعات لا يمكن تجاوزها بسهولة بالنسبة للأعمال في المنظمة. ويتم تحديد الخدمات والأنظمة التي سيغطيها هذا المركز بالاعتماد على الاستراتيجية التي تتبناها المنظمة في خطتها للاستعادة من الكوارث والتي يتم تطويرها بالاعتماد على تحليل أثر الكوراث على الأعمال (business impact analysis) في المنظمة. ومن المهم مراعاة المعايير العالمية عند إنشاء هذا المركز كأن يتم اختيار الموقع بدرجة مناسبة من البُعد بحيث لا تؤثر نفس الكوارث على الموقعين معاً مع السماح لفريق العمل بالوصول بيُسر لموقع الاستعادة.

لنتمكن من تقدير الموارد اللازمة لإنشاء مركز استعادة من الكوراث افترضنا أن المنظمة بحاجة لإنشاء موقع في محافظة أخرى (تم اقتراح طرطوس أو حمص) وتجهيزه مبدئياً بخمسة مخدمات بالإضافة للتجهيزات الشبكية واللوجستية والبرمجيات اللازمة.

٣,٤,٣. الدراسة المالية

جدول (٧): الدراسة المالية وفق خطة زمنية مقترحة لتطبيق البرنامج ضمن ٤ سنوات ميلادية

	السنة الأولى	السنة الثانية	السنة الثالثة	السنة الرابعة
تقنياً	– توظيف ٢ مهندس أمن معلومات – إعداد دراسة مركز الاستعادة من الكوارث – مشاريع لتوريد الأنظمة: • SIEM • Network Access Control (NAC) – تنفيذ فحص اختراق ومراجعة مخاطر أمن المعلومات	– توظيف ٢ مهندس أمن معلومات – تنفيذ مركز الاستعادة من الكوارث – مشاريع لتوريد الأنظمة: • Data leak prevention DLP • Identity and access management systems – تنفيذ تدقيق أنظمة ومراجعة مخاطر أمن المعلومات	– توظيف مهندس أمن معلومات واحد – مشاريع لتوريد الأنظمة: • Endpoint Detection and Response (EDR) • Vulnerability scanning tools – تنفيذ فحص اختراق ومراجعة مخاطر أمن المعلومات	– مشاريع لتوريد الأنظمة: • Multi factor authentication • Privileged Access Management (PAM) – تنفيذ تدقيق أنظمة ومراجعة مخاطر أمن المعلومات
تسويقياً	– تشكيل سياسات وإجراءات ومعايير – توقيع تعهد كافة الموظفين بالالتزام بهذه السياسات – إنشاء لجنة توجيهية لأمن المعلومات – إعداد ميثاق خاص بأمن المعلومات – وضع هيكلية وتوصيف وظيفي واضح لوظائف أمن المعلومات – حملات توعية وتأهيل وتدريب	– مراجعة سياسات وإجراءات ومعايير – توقيع تعهد الموظفين الجدد بالالتزام بهذه السياسات – وضع خطة استراتيجية لعدة سنوات – حملات توعية وتأهيل وتدريب	– مراجعة سياسات وإجراءات ومعايير – توقيع تعهد الموظفين الجدد بالالتزام بهذه السياسات – حملات توعية وتأهيل وتدريب	– مراجعة سياسات وإجراءات ومعايير – توقيع تعهد الموظفين الجدد بالالتزام بهذه السياسات – حملات توعية وتأهيل وتدريب
مالياً (كلفة تقديرية ل.س) "التفاصيل في ملحق ٣"	١,٤٢٤,٠٠٠,٠٠٠	١,٦٧٠,٠٠٠,٠٠٠	١,٤٦٠,٠٠٠,٠٠٠	١,٥١٠,٠٠٠,٠٠٠

قياس العائد الاستثماري:

من الصعوبة بمكان قياس العائد الاستثماري ضمن المنظمات الإنسانية غير الربحية على عكس الحال في المنظمات التجارية الربحية. ويُمكن في مثل حالة المنظمة الإنسانية موضوع بحثنا هذا تقسيم العائد إلى قسمين أساسيين:

- الداخلي: يتضمَّن حساب عائد تطبيق برنامج أمن المعلومات على المستوى الداخلي للموظفين ضمن المنظمة وقياس الأداء الإداري حيث أنه من الممكن قياس الأبعاد التالية التي يؤدي ضبطها إلى زيادة مؤكدة في الإنتاجية مما سينعكس إيجاباً على العائد الاجتماعي على الاستثمار المقدم للمستفيدين:
  - درجة التزام العاملين بمعايير برنامج أمن المعلومات المطبقة
  - درجة تحسين جودة الخدمات المقدمة من خلال ضمان استمرارية الأعمال وفق الأطر المطبقة (تقليل عدد حوادث أمن المعلومات)
  - تخفيف الوقت الضائع الناتج عن انقطاعات الخدمات نتيجة حوادث أمن المعلومات

  كما يوجد عدد من الفوائد التي لا يمكن قياسها منها ما يأخذ شكل: ارتفاع في الروح المعنوية وفي مستوى الثقة بالنفس لدى الأفراد، وزيادة في مستوى رضاهم عن العمل، وفرص ترقيتهم الوظيفية نتيجة التحسن العام في ثقافة ومستوى أمن المعلومات ضمن المنظمة.

- الخارجي: إن وجود برنامج أمن معلومات مُحقَّق ضمن المنظمة ومُؤكَّد من قبل جهات مستقلة معتمدة دولياً سوف يزيد بكل تأكيد الثقة التي تمنحها الجهات المُمَوِلة للمنظمة نتيجة الضمانات المقدمة من قبل المنظمة في الحفاظ على أمن بيانات عملائها وشركائها وعلى جودة تلك البيانات ونزاهتها. إن ذلك سينعكس بدون شك على قرارات التمويل الخارجي وسيساهم بشكل من الأشكال في زيادة التمويل وتوسيع رقعة الممولين الراغبين بتقديم خدماتهم ضمن مستوى مخاطر مقبول لهم تجاه بيانات التمويل وتفاصيله.

إن قياس العائد من هذا الاستثمار في تطبيق برنامج أمن معلومات ضمن منظمة يمثل مشكلة وقضية حرِجَة لسنوات عديدة كونه يُساهم في الفائدة المالية التي تعود على المنظمة في فترة لا يمكن حصرها لأن مثل تلك البرامج تتميز باستمراريتها وعدم تحديدها بنطاق زمني للاستثمار، بالإضافة لصعوبة ترجمة وتحويل نتائج الاستثمار في برنامج أمن المعلومات إلى أرقام مالية وبشكل خاص ضمن المنظمات الإنسانية غير الربحية، فالعوائد هنا لا يمكن قياسها مادياً أو ترجمة آثارها إلى أرقام مالية.

وبالرغم من وجود نماذج عديدة لقياس العائد من الاستثمار في تطبيق برامج ضبط المخاطر المتعلقة بأمن المعلومات، وتعدد المناهج التي تهتم بتقيّيمها وتحديد تأثير ومنافع تلك البرامج على المنظمات وعلى أصولها، إلا أنه لا يوجد نموذج مُحدَّد مُتَّفق عليه، هذا ما جَعل البحث مستمراً لإيجاد إطار عام يُلّم بكل النماذج ويحصر أثر تطبيق برنامج أمن المعلومات إلى درجة كبيرة لتَعُم الفائدة على المنظمات وعلى الأفراد والجهات المتعاملة معها.

وعليه فمن الممكن، بعد البدء بتطبيق برنامج أمن المعلومات المُقترح وبنهاية كل سنة من سنوات التطبيق، أن يتم تنفيذ استبيان دوري يتم من خلاله مراجعة النشاطات المتعلقة بالبرنامج وقياس مدى التقدُّم في الأداء وانعكاساته الداخلية والخارجية على زيادة معدلات الاستثمار ودرجة التوافق مع أعمال المنظمة التشغيلية وأهدافها الاستراتيجية.

النتائج والتوصيات

١,٤. النتائج

تمخَّضت عن هذا البحث النتائج التالية:

١. وجود ضَعف واضح في حوكمة أمن المعلومات في المنظمة ودرجة مُنخفضة من النُضج حيث أن النشاطات المتعلقة بحوكمة أمن المعلومات في أغلبها عشوائية وغير منتظمة.
٢. يوجد لدى المنظمة اهتماماً مقبولاً تجاه مخاطِر أمن المعلومات رغم أن ذلك يجري بطريقة غير مُنَظمة بالقدر الكافي.
٣. لحوادث أمن المعلومات (في حال وقوعها) أثر بالغ الخطورة على مصَالح المنظمة وأعمالها ما قد يطَال جوانب مالية وقانونية (قضائية) بالإضافة لأثرها المباشر على سُمعة المنظمة ومكانتها خاصة أمام المستفيدين والمانحين.
٤. أدوار وظائف أمن المعلومات لا تزال ثانوية وهامشية ضمن المنظمة وهي عُرضة لتضارب كبير في المصالح كونها تتم من خلال موظفي قسم تقانة المعلومات حالياً.
٥. تمتلك المنظمة بعض أنظمة أمن المعلومات التقنية المهمة إلا أنها بحاجة لتوفير التمويل اللازم لبعض الأنظمة الضرورية الأخرى ضمن خطة زمنية وفق أهميتها.
٦. لدى المنظمة محدودية في الالتزام والامتثال للسياسات والإجراءات والمعايير وذلك كنتيجة حتمية لضعف الحوكمة والوعي العام لدى موظفي المنظمة بمخاطر أمن المعلومات وكيفية التعامل معها.
٧. يوجد لدى إدارة المنظمة بشكل عام ولدى إدارة قسم تقانة المعلومات خاصة رغبة حقيقية بتطوير واقع أمن المعلومات في المنظمة والانتقال به من الوضع الراهن إلى حالة مستقبلية توفر درجة متقدمة من النُضج الأمني بهدف تخفيض مستوى الخطر المتعلق بأمن المعلومات لمستويات مقبولة بالنسبة للإدارة.
٨. يحتاج أصحاب القرار لدى المنظمة إلى مزيد من التوجيه والتوضيح والمعرفة المتعلقة بنشاطات ومخاطر أمن المعلومات ليتمكنوا من توفير الدعم الضروري وترتيب أولويات الاستثمار في أمن المعلومات بدءاً بالأكثر تأثيراً على مصالح المنظمة وأعمالها.

٢,٤. التوصيات

١. يوصي البحث بضرورة بناء برنامج استراتيجي متكامل لأمن المعلومات في المنظمة بأسرع وقت ومناقشته واعتماده من قبل إدارة المنظمة ووضع الخطط الملائمة لتمويله وتنفيذه.

٢. يوصي البحث بتأمين الموارد الضرورية لتنفيذ برنامج أمن المعلومات سواء كانت تقنية أو بشرية أو مالية.

٣. يحث البحث على تحسين وضع المنظمة المتعلق بحوكمة أمن المعلومات وإدارة المخاطر المتعلقة بأمن المعلومات.

٤. يحث البحث على المراجعة الدورية لنشاطات برنامج أمن المعلومات وإجراء التعديلات الملائمة عليه بما يضمن دعمه الدائم لأعمال المنظمة التشغيلية وأهدافها الاستراتيجية.

٥. نوه البحث على ضرورة تطوير ثقافة المنظمة تجاه الاهتمام بنشاطات أمن المعلومات وزيادة الوعي الأمني لدى كافة العاملين فيها.

٦. يوصي البحث بتنفيذ دراسات أو استبيانات مستقبلية دورية تتناول استنتاجات حول العائد الاستثماري من تطبيق برنامج أمن المعلومات في المنظمة أثناء وبعد تطبيقه.

مراجع البحث

مواقع شبكة الإنترنت

- https://www.isaca.org/ 23/02/2022
- https://securityboulevard.com/ 14/03/2022
- https://insights.integrity360.com 18/03/2022
- https://en.wikipedia.org/wiki 25/03/2022
- https://sarc.sy/ 04/04/2022
- https://mawdoo3.com 30/05/2022
- /https://www.linkedin.com 01/08/2022
- /https://www.weforum.org 05/08/2022
- /https://blog.cloudflare.com 05/08/2022

المراجع الأجنبية

- CISM Review Manual – 14th Edition by ISACA
- CISA Review Manual 2015 by ISACA
- CRISC Review Manual – 16th Edition by ISACA
- COBIT Process Assessment Model: Using COBIT 5 by ISACA
- ISACA, (2012), "COBIT 5 for Information Security"
- Kissel.R, Editor, May 2013, "Glossary of key information security Terms", National Institnte of Standard and technology
- ISO/IEC 27002:2013, "Information Technology_ Security Techniques_ Code of Practice for Information Security Management", Geneva: ISO, 2013.
- NIST Special Publication 800-100, (2006), "Information Security Handbook: A Guide for Managers"
- "Whitman, M.E &Mattord, H.J; (2011), "Principles of Information Security
- European Union (2018) General Data Protection Regulation (GDPR), Available at: https://gdpr.eu/tag/gdpr

- IT Governance (2020) The Cyber Essentials Scheme, Available at: https://www.itgovernance.eu/en-ie/cyber-essentials-ie

المراجع العربية

- دراسات الجدوى التجارية والاقتصادية والاجتماعية مع مشروعات Bot، عبد القادر محمد عبد القادر عطية، الدار الجامعية، الإسكندرية، ٢٠١٤
- دراسات الجدوى الاقتصادية لاتخاذ القرارات الاستثمارية، د.عبد المطلب عبد الحميد، الدار الجامعية، الإسكندرية، مصر، ٢٠٠٦
- إعداد دراسات الجدوى وتقييم المشروعات، د. نبيل شاكر ،مكتبة عين شمس ، القاهرة، ١٩٩٨
- اقتصاديات المشروعات، د. محمد الصاريف، مؤسسة حورس الدولية للنشر والتوزيع، الإسكندرية، القاهرة، الطبعة الأولى، ٢٠٠٥
- الجدوى الاقتصادية للمشروعات، د. طلال محمود كداوي، الحامد للنشر والتوزيع، الطبعة الأولى، عمان، الأردن، ٢٠٠٢
- دراسات الجدوى الاقتصادية وتقييم المشروعات الاستثمارية، شقيري نوري موسى، أسامة عزمي سلام، دار الميسر للنشر والتوزيع والطباعة، الطبعة الأولى، عمان، الأدن،٢٠٠٩
- دور وأهمية الكفاءة التسويقية في تحسين أداء المؤسسة الصناعية، أباي ولد الداي، مذكرة لنيل شهادة الماجستير، جامعة الجزائر، ٢٠٠١
- دراسات الجدوى الاقتصادية، د. بهاء الدين أمين، دار زهران للنشر والتوزيع، الطبعة الأولى، عمان، ٢٠١٣
- دراسات الجدوى الاقتصادية وتدقيق المشروعات، سمير محمد عبد العزيز، مؤسسة دار الجامعة، الإسكندرية، ١٩٩٤.
- مخاطر أمن نظم المعلومات المحاسبية المحوسبة: دراسة ميدانية على القطاع الصناعي الأردني، حامد، عاصم نائل رشيد والحمود، تركي راجي موسى، رسالة ماجستير، كلية الاقتصاد والعلوم الإدارية- جامعة اليرموك – الأردن، ٢٠٠٩
- الدور التأثيري لحوكمة أمن المعلومات في الحد من مخاطر نظم المعلومات المحاسبية الإلكترونية: دراسة ميدانية، خليل، علي محمود مصطفى وابراهيم، مني مغربي محمد، كلية التجارة- جامعة بنها، ٢٠١٦

- نظم المعلومات الإدارية مدخل معاصر من منظور إداري، النجار، فايز جمعة، دار حامد للنشر، الطبعة الأولى، الأردن ، ٢٠١٣
- مخاطر التدقيق الإلكتروني وأثرها على جودة المعلومات المحاسبية، أمين، هونر محمد، أطروحة ماجستير جامعة الجنان، طرابلس، لبنان، ٢٠١٤

التقارير

- The Global Risks Report 2021 and 2022 17th Edition (https://www.weforum.org/reports/global-risks-report-2022)
- Cost of a Data Breach Report 2021 (IBM security)
- ENISA (2020) Risk Management and Risk Assessment for SMEs, Available at: https://www.enisa.europa.eu

الملاحق

ملحق ١: أسئلة مقابلات المعنيين في المنظمة

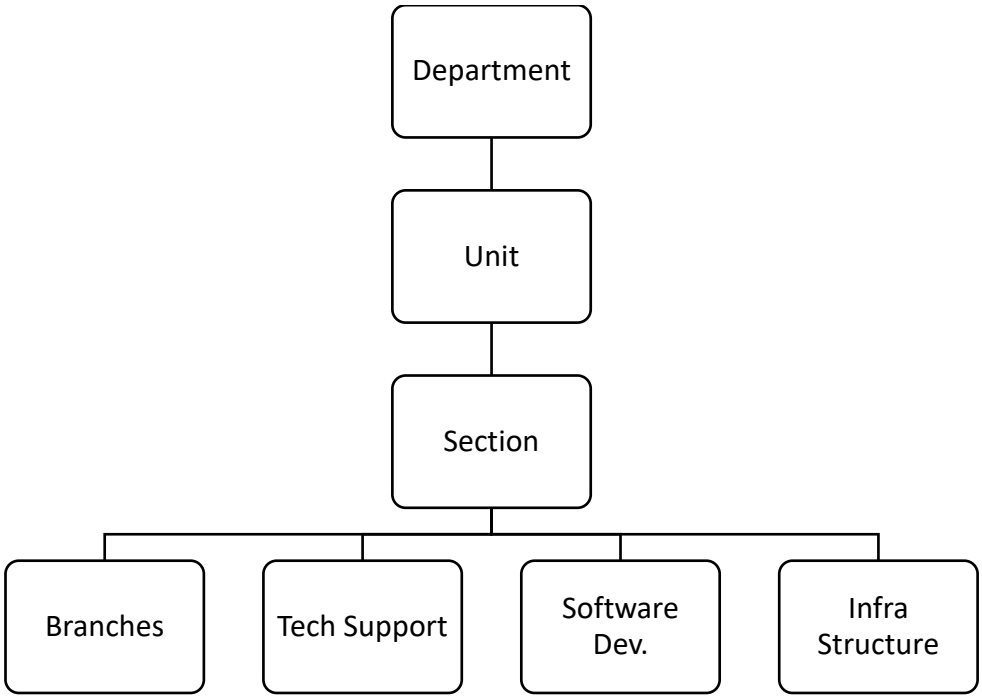
جدول (٨): أسئلة مقابلات المعنيين في المنظمة

رقم السؤال	السؤال
	حوكمة أمن المعلومات
1	هل يوجد سياسات أمن معلومات مكتوبة في المنظمة؟
2	ما الجوانب التي تغطيها هذه السياسات؟ (مثال: الامن المادي, إدارة الدخول للموارد, الأمن البشري,...)
3	كم عددها مصنفة إلى سياسات, إجراءات, دليل عمل, معايير أو غير ذلك؟
4	هل يتم إجراء مراجعة دورية وتحديث للسياسات؟
5	هل يتم اعتماد السياسات من قبل الإدارة العليا للمنظمة بشكل دوري؟
6	كيف يتعهد الموظفون رسمياً بالالتزام بسياسة أمن المعلومات؟
7	هل يوجد فريق متخصص بمتابعة التعديل والتحديث على السياسات الخاصة بأمن المعلومات لتلائم تطور أعمال المنظمة؟
8	ممن يتكون الفريق المشرف على سياسات أمن المعلومات (عدد موظفين وهيكلية وظيفية)؟
9	كيف يتم تقديم مدى نضج المنظمة في مستوى أمن المعلومات للإدارة العليا ومجلس الإدارة ؟
10	هل يوجد لجنة توجيهية لأمن المعلومات (Security Steering Committee) أو أي فريق يقود توجهات أمن المعلومات بمستوى عال في المنظمة؟
11	هل تضم اللجنة التوجيهية ممثلين من كافة أقسام المنظمة وأصحاب المصلحة؟
12	في حال عدم وجود لجنة توجيهية لأمن المعلومات, كيف يتم تنسيق احتياجات ونشاطات أمن المعلومات على مستوى المنظمة دون حدوث تعارض مع الأهداف الاستراتيجية والتشغيلية لها؟
13	ما هي اللجان/الجهات التي تناقش وتعتمد مشاريع وخطط أمن المعلومات في المنظمة؟ (الرجاء توضيح الهيكلية الإدارية التي تتولى مناقشة واعتماد خطط ومشاريع ونشاطات أمن المعلومات في المنظمة)
14	هل يتم اعتماد وثائق مكتوبة رسمية لتحديد نطاق عمل ومسؤولية وميثاق نشاطات أمن المعلومات (أي صيغة تفاهم مع الإدارة العليا حول هذه القضايا)؟
15	ما هو الإجراء المعتمد أو الآلية المتبعة لاقتراح وتخطيط واعتماد وتنفيذ مشاريع أمن المعلومات في المنظمة؟
16	ما هو الإجراء المعتمد لتطبيق التغييرات ضمن بيئة تكنولوجيا المعلومات (إجراء إدارة التغيير)؟
17	ما هو الإجراء المعتمد للاستجابة للحوادث المتعلقة بأمن المعلومات؟
18	ما هو الإجراء المعتمد للإبلاغ ورفع التقارير المتعلقة بأمن المعلومات لأصحاب المصلحة والإدارة العليا ومجلس الإدارة؟
19	هل يوجد خطة موثقة ومعتمدة للاستعادة من الكوارث؟
20	هل يتم اختبار خطط الاستعادة من الكوارث دورياً؟
21	ما هو الإجراء المعتمد لمنح صلاحيات الوصول واستخدام الموارد التقنية للموظفين (إدارة الصلاحيات والوصول للموارد التقنية)؟
22	كيف يتم تقييم نجاح/فشل نشاطات ومشاريع أمن المعلومات والعائد منها؟
23	هل يتم وضع خطط استراتيجية لتنفيذ نشاطات أو مشاريع متعلقة بأمن معلومات لعدة سنوات مقبلة بشكل مرتبط بخطط المنظمة ككل؟
24	كيف تحصل مثل هذه الخطط على الدعم اللازم من الإدارة والأطراف ذات العلاقة لتحويلها إلى واقع؟
25	هل يوجد سياسة خاصة بالاستخدام المقبول للموارد التقنية من قبل المستخدم النهائي؟
26	هل يوجد سياسة معتمدة تضمن تطبيق أفضل المعايير والممارسات والإعدادات الآمنة على الأنظمة التقنية المختلفة (secure baseline configuration)؟
	إدارة المخاطر
27	ما التأثير المتوقع من حصول حادثة تسريب/سرقة بيانات حساسة لخارج المنظمة (قانوني, سمعة, مالي, ...)؟
28	ما التأثير المتوقع من حصول حادثة ضياع/فقدان بيانات حساسة (قانوني, سمعة, مالي, ...)؟
29	ما التأثير المتوقع من حصول حادثة تلاعب/تعديل غير مشروع ببيانات حساسة (قانوني, سمعة, مالي, ...)؟
30	ما التأثير المتوقع من حصول حادثة خروج أنظمة تقنية عن الخدمة لفترة طويلة نسبياً (قانوني, سمعة, مالي, ...)؟
31	كيف يتم تحديد مستوى مخاطر أمن المعلومات المقبول من قبل الإدارة العليا ومجلس الإدارة؟
32	كيف يتم مراجعة وتسجيل ومتابعة المخاطر المتعلقة بأمن المعلومات؟
33	هل يوجد إجراء معتمد حول إدارة مخاطر أمن وتكنولوجيا المعلومات؟
34	هل يوجد فريق متخصص بمتابعة مخاطر أمن وتكنولوجيا المعلومات (العدد والهيكلية والدور الذي يلعبه في حال وجوده)؟

35	كيف تنظم العلاقة مع الموردين الخارجيين الذين يقدمون خدمات متعلقة بالأنظمة المعلوماتية (توريد أو دعم فني أو تشغيل أو إدارة أنظمة أو غيرها من الخدمات الخارجية)؟
36	كيف يتم تنظيم العلاقة مع الموردين الذين تقوم المنظمة بتعهيد وظائف تكنولوجيا المعلومات لهم (outsourcing) في حال وجودهم؟
37	كيف يتم تنظيم العلاقة مع الموردين الخارجيين الذين تقوم المنظمة باستضافة بيانات أوأنظمة تقنية لديهم (cloud computing) في حال وجودهم؟
38	كيف يتم اكتشاف وتصحيح الثغرات الأمنية ضمن الأنظمة المعلوماتية؟
39	كيف يتم التعامل مع نتائج نشاطات التدقيق أو فحص الاختراق الذي تنفذه أطراف خارجية مستقلة؟
40	كيف يتم التعامل مع المخاطر التي تتجاوز المستوى المقبول أو تنتهك سياسات أمن المعلومات المعتمدة؟
	موارد أمن المعلومات
41	هل يوجد فريق متخصص بأمن المعلومات في المنظمة أم تسند مهام أمن المعلومات لموظفين لهم أدوار أخرى؟
42	ما الأدوار الوظيفية التي يمارسها فريق أمن المعلومات؟
43	هل يوجد توصيف وظيفي مكتوب لكل دور وماذا يتضمن في حال وجوده؟
44	هل يتبع فريق أمن المعلومات تنظيمياً لإدارة التكنولوجيا أو أي إدارة تشغيلية أخرى؟ (الرجاء توضيح الهيكلية الإدارية لفريق أمن المعلومات)
45	هل يوجد تصنيف لأنظمة تقانة المعلومات والبيانات حسب أهميتها لأعمال المنظمة؟
46	هل هناك تحديد ملكية (Ownership) واضح ورسمي للأصول التقنية والمعلومات ضمن المنظمة؟
47	هل تستثمر المنظمة حالياً أياً من أنظمة/ضوابط أمن المعلومات التالية: Endpoint security Firewalls Intrusion detection/preventing systems Data encryption (at rest in transit and in use) Multi factor authentication VPN for remote access Security information and event management SIEM Vulnerability scanning and penetration testing tools Data leak prevention DLP Identity and access management systems Endpoint Detection and Response (EDR) Email Security Gateway Web Application Firewall (WAF) Proxy Server Privileged Access Management (PAM) Network Access Control (NAC) User behavioral analytics (UBA) Physical access controls Any others?
48	هل يوجد ميزانية سنوية معتمدة مستقلة ومخصصة لتنفيذ خطط مشاريع ونشاطات متعلقة بأمن المعلومات؟
49	ما الآلية أو الإجراء المتبع لتحديد ميزانية أمن المعلومات السنوية والموافقة عليها؟
50	ما درجة صعوبة اقناع إدارة المنظمة بتمويل مشاريع ونشاطات أمن المعلومات؟
51	هل يتم تحديد التمويل اللازم وفق خطط استرتيجية متفق عليها مع الإدارة أو بشكل منفرد لكل نشاط أو مشروع حسب الحاجة أو استجابة لمتطلبات آنية؟
52	ما العوامل التي تؤثر على قبول أو رفض مشاريع أو نشاطات أمن المعلومات من قبل الإدارة العليا أو اللجنة المختصة؟ الرجاء ترتيبها وفق الأهمية
	الامتثال والالتزام
53	هل تم تنفيذ فحص اختراق للأنظمة التقنية خلال آخر ١٢ شهر وما تقييمكم للنتائج في حال وجودها؟
54	هل يتم تنفيذ فحص الاختراق للأنظمة التقنية بشكل دوري أم عند الطلب فقط؟
55	ما المستويات التي يتم تنفيذ فحص الاختراق للأنظمة التقنية عليها ؟ (مثال: داخلي – خارجي – لاسلكي – تطبيقات ...)
56	هل يتم تنفيذ فحص الاختراق للأنظمة التقنية من قبل جهة مستقلة أو فريق داخلي؟
57	هل تم تنفيذ تدقيق على أنظمة المعلومات خلال آخر ١٢ شهر وما تقييمكم لنتائج آخر تدقيق في حال وجودها؟
58	هل يتم تنفيذ تدقيق على أنظمة المعلومات دورياً أم عند الطلب فقط؟
59	هل يتم تنفيذ تدقيق على أنظمة المعلومات من قبل جهة مستقلة خارجية أو فريق داخلي ضمن المنظمة؟
60	هل يوجد فريق تدقيق تكنولوجيا معلومات داخلي متخصص ضمن المنظمة؟
61	ما الدور الذي يلعبه فريق التدقيق الداخلي في التحقق من الالتزام بالسياسات الخاصة بأمن المعلومات في المنظمة؟
62	كيف يتم إجراء مراجعات لحسابات المستخدمين على أنظمة تقانة المعلومات؟
63	هل يتم إجراء مراجعات لحسابات المستخدمين على أنظمة تقانة المعلومات بشكل دوري أم عند الحاجة فقط؟

64	كيف يتم إجراء مراجعات إعدادات الأنظمة التقنية؟
65	هل يتم إجراء مراجعات إعدادات الأنظمة التقنية بشكل دوري أم عند الحاجة فقط؟
66	ما الطرق المتبعة للتحقق من الالتزام بالسياسات الموضوعة؟
67	ما الجهود التي تبذل في سبيل نشر ثقافة أمن معلومات لدى كل الموظفين على مستوى المنظمة؟
68	كيف يتم ضمان التزام الموظفين الجدد بسياسات أمن المعلومات؟
69	هل يتم إبلاغ الفريق المسؤول عن أمن المعلومات بحالات خروقات مشتبهة من قبل المستخدمين النهائيين؟
70	ما عدد إبلاغات المستخدمين النهائيين عن حالات متعلقة بأمن المعلومات خلال النصف الأول من السنة الحالية؟
71	كيف يطلع الموظفون على سياسات أمن المعلومات في المنظمة؟
72	ما هي نشاطات التدريب الداخلية أو الخارجية المنفذة للموظفين حول أمن المعلومات؟
73	هل يشمل التدريب المتعلق بأمن المعلومات فئة معينة من الموظفين أم يغطي كافة موظفي المنظمة؟
74	هل يوجد أية معايير متبعة في سياسات أمن المعلومات (مثال ISO ٢٧٠٠١)
75	هل يتم الاحتفاظ بنسخ احتياطية من البيانات الحساسة في مكان آمن وخارج مركز المعلومات بشكل دوري؟
76	ما الطرق المتبعة لتقييم ومراجعة التقدم أو التطور في مشاريع ونشاطات أمن المعلومات في المنظمة؟
77	هل يتم مشاركة الإدارة العليا وأصحاب المصلحة بتطور مشاريع ونشاطات أمن المعلومات دورياً؟
78	ما آلية التواصل المتبعة لمشاركة المعلومات المتعلقة بتطور مشاريع ونشاطات أمن المعلومات مع الإدارة العليا وأصحاب المصلحة داخل المنظمة؟

ملحق ٢: هيكلية فريق تقانة المعلومات في المنظمة



ملحق ٣: تفاصيل الدراسة المالية المقترحة على ٤ سنوات*

جدول (٩): تفاصيل الدراسة المالية المقترحة

السنة	البند	كلفة تقديرية (ل.س)
الأولى	رواتب وأجور موظفي أمن معلومات (٢)	٢٤,٠٠٠,٠٠٠
	إعداد دراسة مركز الاستعادة من الكوراث	١٠٠,٠٠٠,٠٠٠
	مشاريع لتوريد الأنظمة: • SIEM • Network Access Control (NAC)	٨٠٠,٠٠٠,٠٠٠
	تنفيذ خدمات دعم فني وخدمات أمن المعلومات خارجية	٤٠٠,٠٠٠,٠٠٠
	تشكيل سياسات وإجراءات ومعايير	٥٠,٠٠٠,٠٠٠
	حملات توعية وتأهيل وتدريب	٥٠,٠٠٠,٠٠٠
المجموع للسنة الأولى		**١,٤٢٤,٠٠٠,٠٠٠**
الثانية	رواتب وأجور موظفي أمن معلومات (٤)	٤٨,٠٠٠,٠٠٠
	تنفيذ مركز الاستعادة من الكوراث	٢٧٢,٠٠٠,٠٠٠
	مشاريع لتوريد الأنظمة: • Data leak prevention DLP • systems Identity and access management	٨٠٠,٠٠٠,٠٠٠
	تنفيذ خدمات دعم فني وخدمات أمن المعلومات خارجية	٥٠٠,٠٠٠,٠٠٠
	حملات توعية وتأهيل وتدريب	٥٠,٠٠٠,٠٠٠
المجموع للسنة الثانية		**١,٦٧٠,٠٠٠,٠٠٠**
الثالثة	رواتب وأجور موظفي أمن معلومات (٥)	٦٠,٠٠٠,٠٠٠
	مشاريع لتوريد الأنظمة: • Endpoint Detection and Response (EDR) • Vulnerability scanning tools	٨٠٠,٠٠٠,٠٠٠
	تنفيذ خدمات دعم فني وخدمات أمن المعلومات خارجية	٥٥٠,٠٠٠,٠٠٠
	حملات توعية وتأهيل وتدريب	٥٠,٠٠٠,٠٠٠
المجموع للسنة الثالثة		**١,٤٦٠,٠٠٠,٠٠٠**
الرابعة	رواتب وأجور موظفي أمن معلومات	٦٠,٠٠٠,٠٠٠
	مشاريع لتوريد الأنظمة • Multi factor authentication • Privileged Access Management (PAM)	٨٠٠,٠٠٠,٠٠٠
	تنفيذ خدمات دعم فني وخدمات أمن المعلومات خارجية	٦٠٠,٠٠٠,٠٠٠
	حملات توعية وتأهيل وتدريب	٥٠,٠٠٠,٠٠٠
المجموع للسنة الرابعة		**١,٥١٠,٠٠٠,٠٠٠**

* تعتبر هذه الأرقام تقديرية وفق متوسط الأسعار الحالية والكلف المتاحة على شبكة الإنترنت لبنود مشابهة