توجهات أمن وشفافية المعلومات

في ظل الحكومة الإلكترونية

أ. د. محمد محمد الهادي

المستخلص

في نطاق مجتمع المعلومات الذي يمثل البيئة الاقتصادية والاجتماعية التي تطبق الاستخدام الأفضل لتكنولوجيا المعلومات والاتصالات المتقدمة بما في ذلك شبكة الإنترنت، أصبحت الحكومات في معظم أو كل دول العالم تلعب دورا قياديا في تحسين المدى الذي تستفيد منه الأعمال والمجتمع بمواطنيه من الفرص التي تقدمها هذه التكنولوجيات المعلوماتية الجديدة للمساعدة في تحويل أنشطة الحكومة من الطرق التقليدية إلي خدمات الحكومة الإلكترونية كما تتضمن عملية توصيل خدمات الحكومة من خلال الاستخدام المناسب لهذه التكنولوجيات الجديدة مما يسمح لها بالقدرة علي توفير تركيز ونفاذ أوسع للمواطنين، وتوافر قدر أكبر للمعلومات المحسنة، وكفاءات أحسن مما هو متاح تقليديا. وسوف يستتبع كل ذلك من تحسين حياة أفضل ومريحة للمواطنين ومنظمات الأعمال المختلفة من خلال توصيل خدمات وتطبيقات حكومية محسنة بتكلفة وجهد أقل وبعدالة وتوازن بغض النظر عن المسافة والوقت؛ وتحقيق كفاءة وعائد أكبر علي الاستثمار؛ توصيل الخدمات الحكومية التي تستجيب لاحتياجات المستخدمين؛ وبناء ثقتهم في الخدمات الحكومية الموجهة لهم.

وقد أصبح أمن وشفافية تطبيقات وخدمات الحكومية الإلكترونية تحظى باهتمام متزايد من قبل مصمميها ومنفذيها حتى يمكن حفظ سرية البيانات المقدمة وسلامتها وتوافرها بدرجة عالية الثقة والمصداقية. ويركز هذا العمل علي البعد المرتبط بأمن وشفافية المعلومات ونظمها وتطبيقاتها في البيئة الرقمية المحملة علي شبكات الكمبيوتر، وعلي وجه خاص شبكات الإنترانت Intranet للمصالح والهيئات الحكومية، وشبكات المعلومات العريضة Wide Area Networks (WANs) وما تمثلها من شبكات الإكسترانت والإنترنت. ويتضمن العرض المقدم عدة محاور ترتبط بالتوسع في استخدامات نظم وتطبيقات وخدمات المعلومات الحكومية التي تتاح علي شبكات المعلومات التي صارت تتسم بالاعتمادية، وقابليتها للتعرض للضرر والخطر، وحاجتها لاكتساب الثقة في التعامل معها من قبل المواطنين؛ أمن نظم المعلومات وتطبيقاتها وخدماتها في بيئة المصالح والمنظمات الحكومية ذات الطابع الرقمي التي يجب أن تصون حماية سرية معاملاتها

الإلكترونية وسلامتها وتوافرها فيما يتصل بالتهديدات المطلوب مواجهتها والاعتبارات العامة التي تشكل معالم شفافيتها من العمليات والبشر والتكنولوجيا والثقافة المؤسسية المتاحة والأمن الطبيعي والمنطقي والفني والسيكولوجي لها؛ ومتطلبات الأمن الطبيعي للمعلومات، واعتبارات وأبعاد أمن المعلومات؛ وتوجيهات ومعايير أمن نظم المعلومات التي تتضمن المبادئ الرئيسية لأمن المعلومات؛ والتوجيهات والمعايير المرتبطة بأمن المعلومات فيما يتعلق بالأغراض والمجال والأهداف؛ وتنفيذ نظم أمن وشفافية المعلومات المرتبطة بتطوير السياسة الخاصة بنظام الأمن والتعليم والتدريب المصاحب لتطوير النظام وتبادل المعلومات والتعاون في معلومات أمن نظم المعلومات وتطبيقاتها وخدماتها؛ ويختتم هذا العمل بالخلاصة التي تشتمل علي النتائج والتوصيات.

الكلمات الرئيسية: الحكومة الإلكترونية، أمن المعلومات، شفافية المعلومات، معايير الأمن، التشفير،الجرائم المعلوماتية.

1. المقدمة:

يشكل كل من الحاسب الآلي والبرمجيات والبيانات العناصر الأساسية لنظام المعلومات في البيئة الرقمية المرتبطة بالحكومة الإلكترونية. وقد يرتبط الحاسب الآلي بواسطة أجهزة وخدمات الاتصال في شبكة بنهايات طرفية أو حسابات أخرى أو تسهيلات اتصال معينة. وقد تكون شبكة الحاسبات شبكة محلية LAN أو شبكة خاصة ممتدة علي نطاق المصلحة الحكومية أو الوزارة المعنية كشبكة الإنترانت، أو شبكة المجال العريض WAN كشبكة الإكسترانت أو شبكة معلومات دولية كالإنترنت، كما قد تكون وصلة اتصال خارجية مفتوحة لأي فرد مزود بالوسائل التكنولوجية التي تمكنه في الوصول إليها.

وتشتمل كثير من شبكات المعلومات علي تجميع من الوصلات الداخلية والخارجية، كما تتضمن شبكات الاتصال علي بيانات اتصال، بالإضافة لتليفون وفاكس موديم. ومن الأجهزة الأخرى قد ترتبط الطابعات بأجهزة الحاسبات والاتصالات. وقد تتضمن برمجيات الحاسبات نظم تشغيل وبرمجيات التطبيقات التي تصمم خصيصا لعميل معين كمصلحة أو جهاز حكومي معين. وقد تركب البرمجيات في الحاسب الآلي أو تخزن علي أقراص مدمجة CD-ROMs، أو أي وسائل تخزين أخري متاحة. وتساند الأدلة الورقية والتوثيقية أو المحمولة والمقروءة إلكترونيا تشغيل الأجهزة والبرمجيات واستخدامها وصيانتها.

وينشأ هذا الهيكل الكامل لنظم وتطبيقات المعلومات في البيئة الرقمية بهدف تخزين البيانات والمعلومات ومعالجتها واسترجاعها وإرسالها أو نقلها للمستخدم المستهدف. وتجمع كل هذه العناصر المختلفة والعديدة معا لتشكل نظام المعلومات في البيئة الرقمية مما يمثل ديناميكية تكنولوجيا المعلومات والاتصالات المتقدمة في دعم ومساندة البيئة الرقمية وما يرتبط بها من تطورات كالحكومة الإلكتروني والتعلم الإلكتروني والعلاج عن بعد، الخ.

وفي هذا الإطار يمكن تحديد العوامل الحاكمة التالية:

1. زيادة استخدام وفعالية قيمة الحاسبات الآلية، وتسهيلات الاتصال، وشبكات الحاسبات والاتصالات، والبيانات والمعلومات التي تخزن وتعالج وتسترجع وترسل بواسطتها متضمنة البرامج والمواصفات والإجراءات.
2. الطابع العالمي لنظم وتطبيقات المعلومات وانتشارها علي كافة المستويات المحلية والقومية والدولية.
3. نتيجة لزيادة دور نظم وتطبيقات المعلومات المتزايد الأهمية والاعتماد المتنامي عليها في الاقتصاد والتجارة والإدارة والتعلم أي في كافة أوجه الحياة الاجتماعية والثقافية والسياسية، فقد أدي ذلك إلي بذل جهود خاصة لضمان الثقة والمصداقية لهذه النظم والتطبيقات من حيث أمنها وشفافيتها للمستخدمين.
4. للبيانات والمعلومات المتوافرة في نظم وتطبيقات المعلومات الإلكترونية مزايا إضافية تجعلها مختلفة ومتميزة عن النظم الورقية أو الوثائقية التقليدية، ويحتم ذلك ضرورة توافر ما يلي:

- طرق ملائمة لزيادة الوعي بالمخاطر المحيطة بنظم وتطبيقات المعلومات,
- توجيهات ومعايير وأساليب مقننة لحماية أمن وشفافية المعلومات ونظماها وتطبيقاتها في البيئة الرقمية،
- إجراءات مناسبة تجرم المساس بسرية وخصوصية وتوافر البيانات والمعلومات لمستخدميها،
- مقاييس وإجراءات تعكس المبادئ التي تخص أمن المعلومات الإلكترونية،

وعلي هذا الأساس فإن تعزيز الثقة والأمن في استعمال تكنولوجيا المعلومات والاتصالات سوف يعزز إطار الطمأنينة الذي يشمل أمن المعلومات وأمن الشيكات وصون الخصوصية

والسرية وحماية المواطن المستخدم مما يعتبر شرطا مسبقا لإنشاء مشروعات الحكومة الإلكترونية لتنمية مجتمع المعلومات لبناء الثقة بين مستخدمي تكنولوجيا المعلومات والاتصالات.

ويتضمن هذا العمل عدة محاور ترتبط بالتوسع في استخدامات نظم وتطبيقات وخدمات المعلومات الرقمية الحكومية التي تتاح علي شبكات المعلومات التي صارت تتسم بالاعتمادية، وقابليتها للتعرض للضرر والخطر، وحاجتها لاكتساب الثقة في التعامل معها من قبل المواطنين؛ وأمن نظم المعلومات وتطبيقاتها وخدماتها في بيئة المصالح والمنظمات الحكومية الرقمية التي يجب أن تمثل حماية سريتها وسلامتها وتوافرها فيما يتصل بالتهديدات المطلوب مواجهتها والاعتبارات العامة التي تشكل معالم شفافيتها من العمليات والبشر والتكنولوجيا والثقافة المؤسسية المتاحة؛ ومتطلبات الأمن الطبيعي والمنطقي والفني والسيكولوجي للمعلومات التي تحدد عمليات التحقق من الأمن المستهدفة (التعريف، الاعتماد، الإدارة، والمراجعة)، وتفهم استخدام أمن نظم المعلومات، ومحاسبة إدارة الأمن وتنفيذ أدوات ومنتجات الأمن؛ واعتبارات وأبعاد أمن المعلومات؛ وتوجيهات ومعايير أمن نظم المعلومات من حيث غرضها العام ومجالها وتعاريفها وأهدافها والمبادئ الخاصة بأمن المعلومات؛ وتنفيذ نظم أمن وشفافية المعلومات المرتبط بتطوير السياسة الخاصة بنظام الأمن والتعليم والتدريب المصاحب لتطوير النظام وتبادل المعلومات والتعاون في المعلومات الأمنية لنظم المعلومات وتطبيقاتها وخدماتها. ويختتم هذا العمل بالخلاصة التي تتضمن النتائج والتوصيات المتوصل إليها.

2. التوسع في استخدامات تطبيقات وخدمات ونظم المعلومات في البيئة الرقمية:

لقد تقبل المجتمع المعاصر أهمية تكنولوجيا الحاسبات والاتصالات اقتصاديا واجتماعيا وسياسيا. وتعتبر هذه التكنولوجيات المتقدمة جوهرية وأساسية لا من أجلها فحسب، ولكن أيضا بما تمثله كقاطرة لكل الأنشطة والمكونات الأخرى التي ترتبط بالمنتجات والخدمات النابعة منها.

وقد شهد المجتمع المعاصر كثير من التطورات التي منها المعالم التالية:

- انتشار الحاسبات الآلية وتشعبها وانتشارها في كل أوجه حياة المجتمع المعاصر.
- تلاحم وتشابك تكنولوجيات المعلومات والاتصالات.
- تواصل أعظم لتكنولوجيا الحاسبات والاتصالات والتشغيل المتداخل لنظمها وتطبيقاتها.
- زيادة لا مركزية وظائف الحاسبات والاتصالات.

- نمو استخدام الحاسبات إلي المدى الذي يعتبر كل فرد مستخدم فعلي أو متوقع لشبكات المعلومات والاتصالات وخاصة في الدول المتقدمة تكنولوجيا.

إن العالم المعاصر يتجه بخطي حثيثة ومتأنية نحو مجتمع المعلومات الذي عقدت له الأمم المتحدة بالتعاون مع الاتحاد الدولي للاتصالات ITU الجولة الأولي لمؤتمر القمة العالمي لمجتمع المعلومات، جنيف: ديسمبر 2003، وسوف تعقد الجولة الثانية لهذا المؤتمر في تونس عام 2005. ويتسم مجتمع المعلومات بأنه مجتمع لا حدود له غير متأثر بالمسافة أو الوقت،

كما تعتبر اقتصاديات وسياسات ومجتمعات اليوم مبنية أقل علي البنية الأساسية الجغرافية والطبيعية عما كانت عليه في الماضي، وصارت حاليا تعتمد بزيادة مطردة علي البنية الأساسية لنظم وتطبيقات المعلومات في البيئة الرقمية التي أصبحت تفيد الحكومات والمنظمات والمنشآت والأفراد علي حد سواء.

وقد صارت هذه النظم والتطبيقات المعلوماتية تمثل جزءا مكملا وأساسيا لأنشطة الأمن والإدارة والتجارة والتمويل القومية والدولية، كما أصبحت تستخدم بتوسع. وعلي هذا الأساس صارت هذه النظم والتطبيقات الرقمية تستخدم في أداء كثير من الخدمات والأنشطة الحكومية من خلال الحكومات الإلكترونية E-Government، التعلم الإلكتروني E-Learning، الخ.

وتقدم استخدامات تطبيقات وخدمات ونظم المعلومات مدى واسع وممتد من الإمكانيات في الوصول الأعظم للموارد والخبرة والتعلم والمشاركة في الحياة المدنية والثقافية للمواطن العادي. وتتسم نظم وتطبيقات وشبكات المعلومات الحديثة بالعوامل أو الخصائص الثلاثة التالية:

أولا: الاعتمادية Dependency

يتأثر كل شخص، منشأة أو مصلحة حكومية مباشرة بتطبيقات ونظم المعلومات الرقمية، ويصبح معتمدا علي وظائفها المختلفة التي تلائم استخداماته المتنوعة. علي سبيل المثال لا الحصر، إن استخدام نظم المعلومات المتزايد قد ساهم في تعميق التغييرات الأساسية التي تحدث في الإجراءات التنظيمية الداخلية في أي منظمة مما أدى إلي تبديل وتغيير الطريقة التي تتفاعل بها مع جمهور المتعاملين معها. أما في حالة فشل أي نظام معلومات، يصبح من المستحيل الاستمرار في الإجراءات الحالية بدون هذه النظم، كما يصبح من الصعب العودة مرة أخري إلي الطرق والإجراءات القديمة التقليدية. وأصبح غير كافي تواجد سجلات ورقية، أو الاعتماد فقط علي مهارات العاملين اليدوية، أو حتى توافر عدد كبير من القوي العاملة لكي يسمح للمنظمة أو

المؤسسة المعنية من الاستمرار في أداء وظائفها بمعدلات إنتاجية عالية وجودة أحسن بنفس المدى الذي قد تعمل به مع تواجد نظم وتطبيقات المعلومات الرقمية الحديثة حتى يمكن من مواجهة المنافسين في عالم مفتوح يتسم بالعو لمة. فعلي سبيل المثال أيضا، في الإمكان ملاحظة تأثير فشل نظام المعلومات الإلكتروني علي الأداء وفعالية الخدمات وانتظام حركة المعاملات علي شركات خطوط الطيران والبنوك وغيرها من المؤسسات التي لا تستطيع الاستغناء علي التطبيقات والخدمات والنظم الإلكترونية المتقدمة. مما سبق يمكن استنباط مدى نمو الاعتماد علي نظم وخدمات المعلومات الرقمية بمعدلات كبيرة غير مسبوقة. وقد صاحب هذا الاعتماد المتنامي بزوغ الحاجة الملحة لتوفير الثقة والشفافية لهذه النظم المستمرة في التطوير والتواجد في المستقبل.

ثانيا: قابلية تعرض النظم والتطبيقات للضرر Vulnerability

كما أن استخدام تطبيقات وخدمات ونظم المعلومات الرقمية قد زاد بطريقة هائلة مما أدي إلي بزوغ فوائد ومزايا كبيرة عادت بالنفع علي المنظمات والأفراد المستخدمين لها، إلا أنها أدت إلي تواجد فجوة كبيرة بين الحاجة لحماية هذه النظم والتطبيقات ودرجة الأمن الموفرة والموظفة لها بالفعل. فقد أصبح مجتمع المعلومات الحديث المتضمن الأعمال والخدمات العامة والأفراد معتمدا بصفة كبيرة علي تكنولوجيات المعلومات والاتصالات الغير موثوق منها لحد كبير. وتعتبر كل استخدامات نظم المعلومات وتطبيقاتها الرقمية المحملة علي شبكات الحاسبات معرضة للهجمات الضارة أو للفشل فيما يتصل بإفشاء سرية معلوماتها أو عدم حفظ خصوصية بيانات الهيئات والمتعاملين معها أو التأخر في توافرها في الوقت الملائم لمن يحتاج إليها بسرعة، أي توجد مخاطر جمة من الوصول غير المعتمد والاستخدام غير الملائم وغير المخصص أو فشل النظم ذاتها بأسباب عرضية جانبية، مع العلم بأن كثير من نظم وتطبيقات المعلومات سوء كانت عامة أو خاصة كتلك المستخدمة في الأغراض الحربية والأمنية والبنوك والمستشفيات وغيرها تمثل أرضية خصبة للإرهاب المعلوماتي المتنامي اليوم.

وفي إطار التطورات المتلاحقة المتمثلة في تزايد الحاسبات الآلية، زيادة قدرة وقوة الحاسبات، التواصلية المتداخلة، اللامركزية، نمو الشبكات وعدد مستخدميها المتنامي، تعزيز نفعية نظم المعلومات مع زيادة قابليتها للتعرض للضرر والخطر، كل ذلك جعل من الصعوبة تحديد موقع المشكلات التي يتعرض لها النظام وتحديد أسبابها للعمل علي تصحيحها بطريقة متوازنة مع وظائف ومتطلبات النظام الأخرى حتى يمكن منع تكرار حدوثها أو ارتدادها.

وكما تصبح نظم المعلومات وتطبيقاتها لامركزية وتنمو بطريقة متناهية، فمن المهم مراعاة اعتماد مكوناتها وملحقاتها وتداخلها معا الموردة والمباعة من قبل موردين وبائعين ومن مصادر مختلفة ومتعددة. إضافة لما تقدم، فإن نمو تواصلية نظم شبكات المعلومات واستخدامات الشبكات الخارجية أدي إلي مضاعفة أوجه الفشل والقصور الممكنة. وتقع هذه المظاهر الخارجية خارج نطاق رقابة عمليات وحقوق ومهام الأطراف المتضمنة والمتعاملة مباشرة مع النظم، وخاصة في حلة حدوث أي هجمات وتجاوزات غير مسموح بها.

وفي نفس الوقت، يكون التغيير الفني غير متوازي مع تطوير النظم، ويتخطى بعض الميادين، بينما يتأخر حدوثه في البعض الآخر. كما أن عدم القدرة في التكيف واستيعاب التطورات التكنولوجية بنفس المعدل الذي تحدث فيه التي تحدث مثلا في حالة الفشل الملائم لاختيار أو تنسيق متغيرات النظام، قد يؤدي إلي حدوث مشكلات علي النظام. وقد تنجز التطورات التكنولوجية قبل تشعبها ونتائجها ومواقعها تجاه التكنولوجيات القائمة بالفعل مما يعتبر شيئا مألوفا ومفهوما. وقد يغطي توزيع قدرات النظام بطريقة غير متساوية غير متساوية في الرقابة والوصول لنظم المعلومات بدلا مما هو مطلوب أو متوقع. كما أن زيادة عدد المستخدمين في الوصول لنظم المعلومات مع تقليل الرقابة المباشرة عليهم من قبل الشركات الموردة أو المنظمات المستخدمة قد يؤدي إلي خسارة مالية مباشرة كالخسارة في طلبات العملاء إلي جانب الخسارة غير المباشرة التي قد تتمثل في إفشاء خصوصية المعلومات الشخصية أو المعلومات السرية المهمة أو تلك المعلومات ذات الطابع التنافسي أو الحساسة لتواجد المنظمة ذاتها.

ومن الملاحظ أيضا أن تطور الأوجه القانونية والتشريعية قد لا تكون دائما بخطى موازية مع التقدم التكنولوجي' ففي بعض الحيان يعتبر ذلك غير كافي علي المستوى القومي إلي جانب من تواجد عدد من الحالات غير المطورة حتى الآن علي المستوى الدولي. إن تناسق وانسجام القوانين والتشريعات المرتبطة بنظم المعلومات يعتبر من الأهداف الهامة التي يجب مراعاتها والعمل علي سنها بصفة مستمرة.

ثالثا: بناء الثقة Building Confidence

يجب أن يثق مستخدمي نظم المعلومات وتطبيقاتها في البيئة الرقمية للمنظمة المعنية في أنها تشغل وفقا لما هو مقرر لها بدون أي أعطال، أخطاء، فشل أو مشكلات غير متوقعة. وفيما عدى ذلك، فإن النظم والتكنولوجيات المرتبطة بها قد لا تكتشف في المدى الممكن لاكتشافها كما أن النمو والإبداع اللاحق قد يحجب. وعلي ذلك، فإن الوصول لتأمين الشبكات وإعداد توجيهات ومعايير أمن حاكمة قد تنبع نتيجة لمتطلبات المستخدمين ذاتهم, وأن فقد الثقة في النظام والتطبيق القائم عليه قد ينبع من سوء الاستخدام، من عدم تلبية التوقعات، أو عدم التأكد الذي قد يتوصل إليه. وعلي ذلك، تحتاج نظم المعلومات الرقمية إلي توفير وبناء إجراءات وقواعد مقبولة لكل الأطراف المتعاملة معها حتى تقدم أوضاعا تزيد من الثقة والمصداقية في هذه النظم.

ويجب ملاحظة أن مسئولية الفشل في تطوير وتشغيل واستخدام النظم تقع علي كاهل مطوريها ومشغليها ومستخدميها في المقام الأول. وعلي هذا الأساس، يجب تحديد مسئولياتهم والتزاماتهم وحقوقهم تجاه هذه النظم من خلال وضع قواعد واضحة وموحدة لتسهيل وتشجيع نمو واستغلال النظم.

ويمثل أمن المعلومات ونظمها والقدرة علي تطويرها وتشغيلها واستخدامها قضية عالمية لأن نظم المعلومات غالبا ما تتعدى الحدود القومية أو الوطنية المحدودة، فهي مشكلة تتطلب تعاونا دوليا مكثفا للتغلب عليها. وفي الواقع، فإنه بافتراض تجاهل نظم المعلومات للحدود الجغرافية والتشريعية تعتبر من المعاهدات والاتفاقات الأحسن قبولا ودعما علي المستوي العالمي.

وتتضمن الخبرات المكتسبة في القطاعات الأخرى أن التكنولوجيات المتقدمة الجديدة التي تحتمل أخطار الأضرار تؤدي غلي تحديات ثلاثة تتمثل في:

1. تطوير التكنولوجيا وتطبيقها،
2. تجنب ومجابهة فشل التكنولوجيا،
3. كسب المساندة العامة والموافقة علي استخدام التكنولوجيا.

وفي هذا الإطار، يمكن اعتبار أن صناعة الطيران ناجحة في تنفيذ أساليب ومتطلبات السلامة الملاحية الجوي، حيث أنها تسهل الأداء السلس الآمن للنقل الجوي وتبعث علي إضفاء الثقة لدي الجمهور المتعامل معه. وبصفة متشابهة للمثال السابق، تستخدم صناعة السفن نظم اعتماد

وسلامة لبناء السفن بنجاح . من هذا المنطلق، يجب أن يكو الهدف من صناعة المعلومات والاتصالات شبيها للمثالين السابقين يرتبط بتجنب أي قصور أو فشل يرتبط بها وتجنبه بقدر الإمكان بدرجة كبيرة من الموثوقية تختص بمنع التطفل والوصول غير المعتمد لنظم المعلومات في البيئة الرقمية.

3. أمن المعلومات ونظمها في البيئة الرقمية:

يمثل أمن المعلومات ونظمها في البيئة الرقمية حماية المعلومات من حيث توافرها وإضفاء الثقة فيها وسلامتها. ويعبر توافر Availability المعلومات علي خاصية من خصائص نظم المعلومات الممكن الوصول إليه واستخدامه علي أساس فوري في إطار نمط محدد ومطلوب، كما يصبح في الإمكان الوصول إلي النظام عندما يطلب بكيان معتمد ووفقا لمواصفات ملائمة لهذا للنظام؛ وتعتبر السرية Confidentiality خاصية ترتبط بعدم تغيير البيانات والمعلومات أو فقدها أو إهدارها وإتاحتها فقط لأشخاص وكيانات معتمدة ومصرح لها فقط باستخدام المعلومات، وتتضمن علي العمليات التي تستخدم أساليب التشفير والحجب لمحتويات البيانات والمعلومات أو السماح بها في أوقات وفي طرق معتمدة. أما السلامة Integrity فهي خاصية البيانات والمعلومات الدقيقة والكاملة التي تحفظ بدرجة كبيرة من الدقة والاكتمال. وتتنوع الأولوية والأهمية النسبية لتوافر المعلومات وسريتها وسلامتها طبقا لنظام المعلومات المتاح.

والعرض التالي يوضح معالم أمن نظام المعلومات وإطار الأمن ومكوناته أو معالمه والتهديدات المختلفة التي يتعرض لها نظام المعلومات:

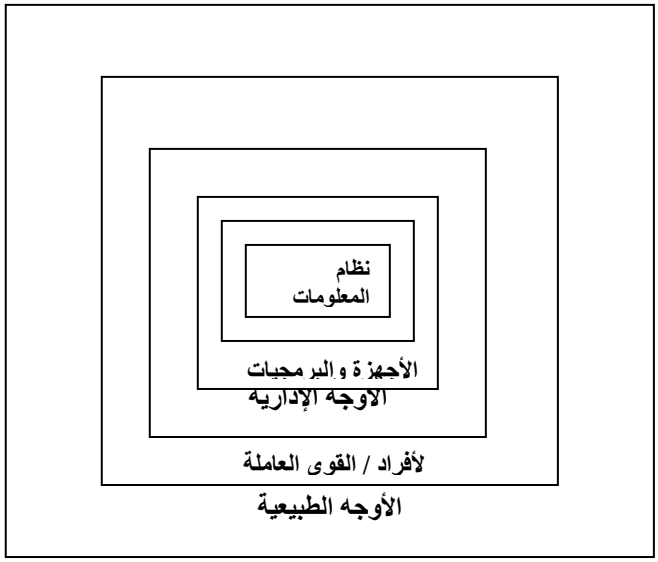
3-ا أمن نظام المعلومات:

يمثل الهدف من أي برنامج أمن بعد لنظام المعلومات في حماية معلومات المنظمة أو المنشأة المعنية بتقليل مخاطر توافر المعلومات وسريتها وسلامتها بمستوي مقبول ومحدد.

ويتضمن برنامج أمن المعلومات الجيد توافر عنصرين رئيسيين، يتمثلان في تحليل المخاطرة وإدارة المخاطرة.

وفي مرحلة تحليل المخاطرة يراعي مستودع البيانات والمعلومات لكل النظم المتوافرة في المنظمة. وينشأ كل نظام من نظم المعلومات قيمة خاصة للمنظمة والدرجة التي تقرر لتعرض المنظمة للمخاطرة. أما إدارة المخاطرة فهي من جهة أخري تتضمن أساليب الرقابة ومقاييس الأمن التي تقلل تعرض المنظمة لمستوي مقبول ومسموح به من المخاطرة. ولكي يكون أمن نظام

المعلومات فعالا وكفء ويعكس الإحساس المشترك، يجب أن تعمل إدارة المخاطرة مع إطار الأمن، حيث تكمل مقاييس أمن المعلومات من خلال القوي العاملة المهنية في تكنولوجيا المعلومات والاتصالات والإدارة إلي جانب مقاييس الأمن الطبيعية كما في الشكل التالي:



شكل رقم (1) طبقات أمن المعلومات المتممة بعضها ببعض

ومن خلال الشكل السابق، يتضح أن إدارة أمن المعلومات هي قضية إدارية في المقام الأول، حيث يتوصل فيها إلي توازن بين قيمة المعلومات للمنظمة من جهة وتكلفة الأفراد والمقاييس الإدارية والتكنولوجية من جهة أخرى. وتضع مقاييس الأمن الحاجة في التوصل إلي أقل تكلفة من المخاطر أو الأضرار التي قد تسبب فقد سرية المعلومات وتحد من سلامتها وتوافرها.

وتتطلب كثير من المناهج المتبعة في تحليل المخاطرة الرسمية خبرة فنية عالية في مجال تكنولوجيا المعلومات وأساليب رقابة متوافقة وتوافر تكرار أحداث الخطر المحتملة التي قد تكون خارج نطاق عمليات المراجعة التقليدية المتبعة. ويتمثل الهدف من تحليل المخاطرة بناء خبرات وموارد مكتسبة بمرور الوقت,

2-3 إطار أمن المعلومات:

يمثل أمن المعلومات أحد عناصر البنية الأساسية التي يجب أن تتاح لأمن نظام المعلومات، وعلي ذلك يجب إلا يفحص من فراغ، كما يجب وجود إطار سياسات أمن يختص بكل أوجه الأمن

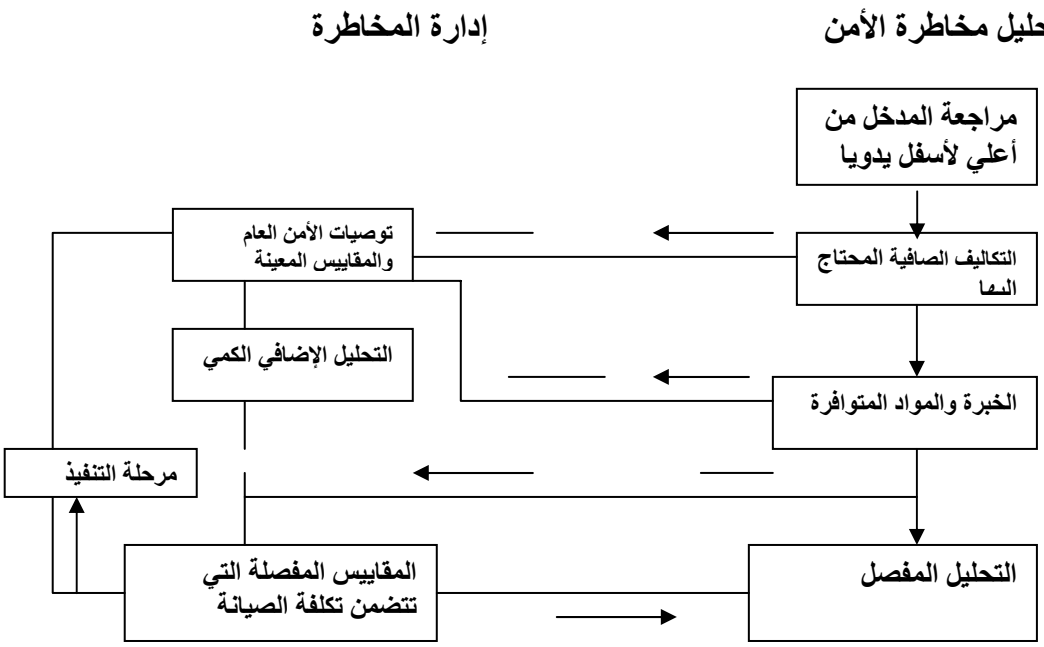
الطبيعي وأمن الأفراد وأمن المعلومات، بالإضافة إلي وجود أدوار ومسئوليات واضحة للمستخدمين وأفراد الأمن وأعضاء لجنة إدارة نظم المعلومات.

ويشتمل برنامج أمن المعلومات علي كل الأوجه الحساسة لمعلومات المنظمة التي تتضمن سريتها وسلامتها وتوافرها. كما يجب أن يحدد أيضا برنامج أمن المعلومات برنامج للتوعية يوضع موضع التنفيذ ويذكر كل العاملين بالمنظمة المعنية بالمخاطر والهجمات الممكنة ومسئولياتهم في حفظ معلومات المنظمة. وإلي جانب الإشارة للشكل رقم (1) السابق يمثل أمن المعلومات مجموعة من المقاييس المختلفة علي كافة المستويات الطبيعية وتلك المتعلقة بالأفراد والمقاييس الإدارية لمستويات نظام المعلومات المتكاملة معا، ويمثل أمن المعلومات مقاييس الرقابة الإدارية الجيدة، وعند وجود أي قصور في أحد المستويات يمكن أن يهدد كل المستويات الأخرى. علي سبيل المثال، إذا كانت سياسات أمن الأفراد غير متضمنة وبالتالي غير منفذة يصبح أمن المعلومات باهظ التكلفة أو علي الأقل غير ممكن مساندته. ومن جهة أخري، يجب أن تؤكد المقاييس المخططة لكل المستويات حد أدنى من حماية المعلومات علي أن تكون مخاطرة الأمن محسوبة ومقبولة من قبل الإدارة المعنية.

وتوجد بعض الأوضاع المعينة التي يمكن لمقاييس الأمن في أحد مستويات نظام المعلومات أن تعوض ضعف الأمن في مستويات أخرى. علي سبيل المثال، تضيف عملية التشفير Encryption حتى في الحالات التي تكون فيها مقاييس الأمن الطبيعية أو تلك المتعلقة بالأفراد أو المقاييس الإدارية ضعيفة، حيث يصبح التشفير أحد معالم الدفاع الأخيرة للمساعدة في حماية أي أخطار تواجه سرية المعلومات.

وعند التخطيط لأمن المعلومات، يجب توازن قيمة المعلومات لإدارة المنظمة مع الحجم النسبي لأنواع المعلومات الأخرى في مواجهة حد الأمن المتوسط في الأساس. وفي كثير من المصالح والأجهزة الحكومية، يجب توافر متطلبات أمن صارمة لمعالجة وتخزين واسترجاع المعلومات ونقلها بطريقة تحمي سريتها وسلامتها في مستودعاتها المقروءة آليا.

وفيما يتصل بإطار المعلومات، يمكن ملاحظة تواجد مدخلا يتضمن طبقتين لمراجعة أمن المعلومات. ويرتكز هذا المدخل علي توظيف الإدراك المشترك والسليم في توازن تكلفة الأمن المبنية في نظام لقيمة المعلومات المتدفقة في نظام المعلومات. والشكل التالي رقم (2) يمثل هذا المدخل المرتبط بتحليل وإدارة مخاطرة الأمن:



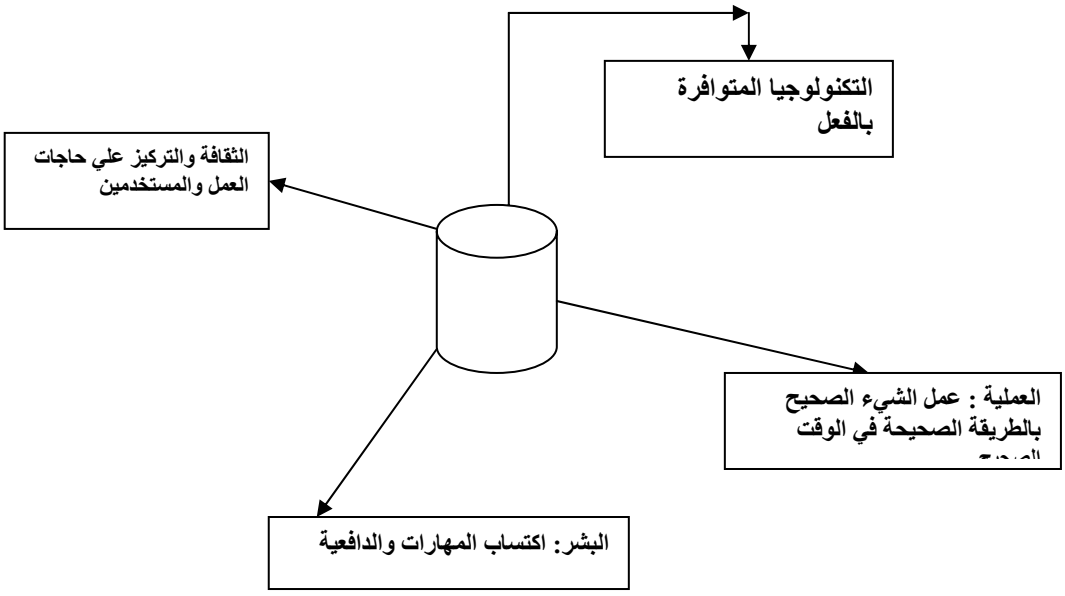
شكل رقم (2) مدخل الطبقتين لتحليل وإدارة مخاطرة الأمن

وتشتمل الطبقة الأولي من هذا المدخل الخاصة بتحليل المخاطرة علي المراجعة من أعلي لأسفل، وتحديد التكاليف الصافية المحتاج إليها، والخبرة والموارد المتوافرة، والتحليل المفصل. أما الطبقة الثانية المرتبطة بإدارة المخاطرة فتتضمن توصيا الأمن العام والمقاييس المعينة، والتحليل الإضافي الكمي، ومرحلة التنفيذ المتعلقة بالمقاييس المفصلة المتضمنة تكلفة الصيانة.

3-3 مكونات ومحاور أمن المعلومات:

تنفيذ وتشغيل نظام أمن المعلومات يمثل طريقة حياة تعتمد علي أربع مكونات أساسية كل منها كل منها مهم ولا يمكن التعامل معه بصفة فردية مستقلة.

ويحدد الشكل التالي رقم (3) معلم مكونات نظام أمن المعلومات:



شكل رقم (3) مكونات نظام أمن المعلومات

1. **العمليات: Possesses** تعتبر العمليات لا غني عنها لأي نظام أمن، فهي جوهرية وذات طبيعة مستمرة. ويحكم أداة عمليات أمن المعلومات مجموعة من المعايير كتلك التي قررتها المنظمة الدولية للتوحيد القياسي ISO التي تعتبر ذات قيمة كبيرة لأي نظام أمن معلومات. وتطبق العمليات بطريقة منظمة كما تراجع باستمرار في إطار الخبرة المتراكمة بغية استبعاد الأخطاء والمخاطر.

2. **البشر: People** الذين يمثلون العاملين، المستشارين، المتعاقدين، والفنيين , وينجزون كل العمليات والخدمات، يحتاج إلي تواجدهم بأعداد وتخصصات ملائمة وبمهارات وخبرات ودافعية مناسبة.

3. **التكنولوجيا: Technology** تعتبر متوافرة وجاهزة، ولمنتجاتها دورات حياة قصيرة نسبيا. وتعتبر سوق التكنولوجيا ذات طبعة تنافسية، يتوافر لها عدد كبير من المنتجين و الموردين والبائعين والموزعين الذين يأتون ويذهبون، وقد يندمجون في شركات أكبر أو قد يخسرون

ويخرجون من سوق الأعمال. ويجعل ذلك من الصعب تقييم التكنولوجيا عما كانت عليه في الماضي.

4. **الثقافة: Culture** ترتبط بتفسير بيئة الأعمال وتتعلق بأخلاقيات المنظمة تجاه المجتمع، حيث يكون لإدارة المنظمة دورا رئيسيا يؤدونه في حفظ ثقافة المنظمة المتوافقة مع ثقافة مجتمعها. ومن أمثلة الثقافات الناجحة في إدارة أمن المعلومات يمكن تتبعها في مجالين رئيسيين:

- الاستخبارات، الأمن والدفاع.
- الصرافة، التبادل الخارجي والتأمين.

وتشتمل الأوجه القافية ذات الطبيعة الحرجة في إدارة نظام أمن المعلومات الناجح علي التالي:

- المساندة والالتزام الكامل تجاه أمن المعلومات من قبل الإدارة العليا بالمنظمة.
- الانضباط التنظيمي القوي.
- السياسة الموثقة والموصلة بوضوح لكل العاملين.
- العمليات الموثقة والمساندة بواسطة المراجعات المستمرة.
- توافق عمليات المراجعة المستمرة.
- الاختبارات والمراجعات العادية الدورية.

4-3 تهديدات أمن نظم المعلومات: Threats to Information Systems

توجد كثير من التحديات تؤثر علي الأداء السليم لوظائف نظم المعلومات، التي منها: التطورات التكنولوجية المتسارعة، المشكلات الفنية المتزايدة، الأحداث البيئية المتغيرة، الضعف البشري، وعدم ملاءمة المؤسسات الاجتماعية والسياسية والاقتصادية الراهنة للمتغيرات المتلاحقة، الخ. وتتبع التهديدات والمخاطر التي تواجه نظم المعلومات من الأفعال والتصرفات المقصودة وغير المقصودة علي السواء التي قد ترد من مصادر داخلية أو خارجية، كما أنها تتراوح من أحداث مفاجئة أو أحداث ثانوية تؤدي إلي عدم الكفاءة اليومية المتوقعة. علي سبيل المثال، قد تنتج الأعطال من أعطال كبيرة تؤدي إلي توقف العمل، أو إبطاء العمل بصفة دائمة، أو تقلل قيمة

النظام وتفسخ خدماته.وفي هذه الحالة يجب مراعاة توقيتات الأعطال والتشويش الذي يتعرض له النظام عند التخطيط لأمن المعلومات من البداية.

والعوامل الفنية التي تؤدي لفشل نظم المعلومات عديدة ومتنوعة، كما قد تعتبر غير مفهومة في بعض الأحيان، أو تتغير علي الدوام.

وقد تكون أخطاء النظام نابعة من سوء استخدام الأجهزة والبرمجيات، الأخطاء الكامنة Bugs، التحميل الزائد أو المشكلات التشغيلية وغير ذلك. وقد تظهر الصعوبة في مكون النظام الداخلي (كما في أجهزة وملحقات النظام المتعلقة بوحدة الذاكرة، تجميع نظام الحسابات الشبكي أو النظام الموزع؛ أو في برمجيات نظم التشغيل والتطبيقات مثل المحرر Editor، الجامع Compiler، شبكة الكمبيوتر المحلية LAN). وقد تكون الصعوبة نابعة من مكون النظام الخارجي (كما في حالة دوائر الاتصالات عن بعد أو الأقمار الصناعية)، أو نتيجة لتواصل وترابط مكونات النظام المختلفة معا.

وقد تتسبب المشكلات الفنية نتيجة للهجمات المختلفة التي يتعرض لها النظام. فغالبا تدخل الفيروسات Viruses في النظام من خلال البرمجيات المصابة Infected، المتطفلين Parasites، أبواب الشراك Trap Doors، الديدان Warms، أو القنابل المنطقية Logic Bombs، الخ. التي تمثل بعض الوسائل الفنية المستخدمة لتعطيل النظام وتشويه، إتلاف أو تحريف بياناته ووظائفه المختلفة.

والصعوبة في صيانة وحماية أمن المعلومات والنظم والشبكات قد تنبع من تواجد بيئات متعددة من الأطراف المرتبطة بها كالمتعهدين، الموردين، البائعين، الخ. علي سبيل المثال، توجد مشكلة جوهرية تتعلق بعدم توافر برمجيات تحكم ورقابة علي الوصول المعتمد التي يتفق عليها كل الأطراف المعنية. ومن مقاييس الأمن الشائعة ضرورة توافق البرمجيات في بيئة الموردين المتعددة. وحتى يمكن التوصل لذلك، يصبح من الضروري موافقة منظمات التوحيد القياسي،والموردين، والمنظمات ومستخدمي نظم المعلومات علي المعايير والتوجيهات الحاكمة لقياسات الأمن ذات الطابع الدولي.

وتقع التهديدات الطبيعية لنظم المعلومات في مجموعتين عريضتين: الأحداث البيئية الجسيمة، وأوضاع التجهيزات الطبيعية المعكوسة. وتشتمل **الأحداث البيئية الجسيمة** علي الحرائق، الزلازل، الفيضانات، العواصف الكهربائية، الموجات الحرارية المرتفعة، والرطوبة

الزائدة وما شابه ذلك. وقد يقع نظام المعلومات يضم الحاسبات الآلية وخطوط الاتصال، حيث قد يكرس له حجرات للحاسبات الآلية وحجرات تخزين البيانات لها ارتباطات وتجهيزات للطاقة الكهربائية والاتصالات تتعرض كلها للأحداث البيئية الجسيمة عند حدوثها. أما **أوضاع التجهيزات الطبيعية المعكوسة** فقد تظهر من خلال اختراق مقاييس الأمن الطبيعية في حالات انقطاع التيار الكهربائي، سوء استخدام أجهزة التكييف، تسر المياه، أو بسبب الغبار والأتربة، الخ. وقد يتأثر نظام المعلومات من الإهمال المباشر في الأماكن المخصصة له، أو غير المباشر في نقاط الربط الجوهرية خارج المنظمة كما في إمداد الكهرباء أو قنوات الاتصال عن بعد. كما يساهم البشر وما ينشئونه من مؤسسات مختلفة اقتصادية، سياسية أو اجتماعية في قصور قيمتها وأدائها مما ينجم عنه مشكلات أمنية أيضا. وقد يؤدي التنوع الكبير لمستخدمي نظام المعلومات والمتعاملين معه (العاملون، المستشارون، العملاء، المنافسون والجمهور العام) فيما يتعلق بتوعيتهم وتدريبهم واهتماماتهم المختلفة والمتفرقة في ظهور صعوبات خاصة بأمن المعلومات ونظمها.

إن نقص التدريب والتوعية الملائمة عن أمن المعلومات وأهميته تسهم في الجهل باستخدام نظم المعلومات المناسبة. وبدون تنظيم دورات تدريب ملائمة، قد يجهل كثير من العاملين والمستخدمين بأعراض الأضرار النابعة من سوء استخدام نظم المعلومات، كما قد لا يستخدمون أي مقاييس أمن حتى البدائية منها، مما قد يؤدي إلي مزاولات تعود بالإساءة لأمن المعلومات. ويقدم اختيار كلمة المرور Password الذي يمثل نشاط المستخدم في كل أنحاء العالم بل يمثل النشاط الرئيسي لأي نظام معلومات مثالا واضحا لأمن المعلومات. فعلي الرغم من أن كلمات المرور تطبق عادة لرقابة الوصول إلي معظم نظم المعلومات، لا زال عدد قليل جدا من المستخدمين يعلم بأهمية الحاجة لأمن كلمة المرور بالطريقة التي تتمثل في تحديد أو إنشاء كلمة المرور ومن العواقب التي تتمثل في سوء استخدام النظام.

علي أنه بدون تدريب أو توجيه، يستطيع كثير من المستخدمين اختيار كلمات مرور واضحة يسهل تذكرها والتحقق منها مثل أسماء العائلة، الأسماء القصيرة، أو الكلمات المرتبطة بالمهام، الخ. وبعد الدخول أو الولوج في النظام، قد يترك المستخدمون غير المدربين كلمات المرور الخاصة بهم معروضة وغير مستخدمة علي النهايات الطرفية النشطة المرتبطة بنظم الشبكة، كما يفشلون في إنشاء ملفات بيانات إضافية مساندة، ويشتركون في رموز التعريف وكلمات المرور، ويتركون منافذ الرقابة والوصول مفتوحة في مواقع الأمن مما يعرضها للاختراق. وكل

ذلك يمثل مشكلات الأمن التي تظهر من الدخول علي ملفات الحاسب لآلي، التحويل علي الحاسبات أو النهايات الطرفية وامتلاك كلمات المرور وسوء استخدامها.

وقد تحدث الأخطاء والاختراقات في تجميع البيانات والمعلومات ومعالجتها وتخزينها وإرسالها وحذفها. كما أن فشل عمل نسخ بديلة ومساندة للملفات والبرمجيات ذات الطبيعة الحرجة يضاعف من آثار الأخطاء والاختراقات ذات الطابع السلبي. وعندما لا توجد سياسة أمن للمنظم المعينة تتصل بإعداد وحفظ نسخ إضافية مساندة لملفات المعلومات والبرمجيات التي تمتلكها، فإنها سوف تتحمل نفقات وخسائر واضحة ترتبط بالوقت والجهد والمال الذي ينفق في إعادة إنشائها من جديد.

إن سوء الاستخدام المقصود للنظام والوصول غير المعتمد له بغرض التطفل والنزوع للأذى وتعمد التخريب والتدمير والاحتيال أو السرقة تعتبر مخاطر وتهديدات خطيرة تؤثر سلبيا علي قابلية نمو حياة النظام و المنظمة المالكة له بل تؤثر أيضا علي القابلية للبقاء والتواجد. علي سبيل المثال، استنساخ البرمجيات غير المعتمد المنتشر علي نطاق واسع قد يؤدي إلي خسائر كبيرة علي النظم والمنظمات.

ومن المألوف أن جزءا أعظم من التهديدات التي تواجه نظم المعلومات يأتي غالبا من المصادر الخارجية. كما أنه علي النقيض من ذلك، فإن الأشخاص الذين منحوا حق الوصول المعتمد للنظام قد يعرضون تهديدات أعظم تواجه نظم المعلومات أيضا. فعلي الرغم من أنهم قد يكونوا مؤتمنين أو عاملين من ذوي النوايا الحسنة فإنهم للتعب أو الإرهاق أو التدريب غير الملائم قد يقترفون أفعال غير متعمدة قد تسهم في حذف كميات كبيرة من البيانات الهامة للمنظمة العاملين بها. وفي حالة كون الأشخاص غير مؤتمنين فإنهم يسيئون استخدام نظم المعلومات أو يتعمدون الوصول المعتمد علي العبث والتلاعب في النظام بطرق متعمدة بغية الاستغلال أو الثراء الذاتي للإضرار بالمنظمة التي يعملون بها.

وبرامج الحاسبات التي تمثل عنصرا مهما من عناصر نظام المعلومات، من المحتمل أن تكون مجالا خصبا للتهديدات التي يتعرض لها النظام. حيث قد تشتمل هذه البرامج علي فيروسات الحاسبات الوالجة في النظام مما قد يعرض سرية بياناته وخصوصيتها وتوافرها للخطر المتزايد. بالإضافة لذلك فإن التحميل المتزايد للبيانات والمعلومات في النظام، أو تحويرها وتغييرها، وانتهاكات اتفاقيات الترخيص الممنوحة قد تعرض أمن نظام المعلومات للخطر الإضافي. علي

سبيل المثال، فإن تبديل البرنامج المرخص به بطريقة غير معتمدة، فد يؤدي إلي قصور الأداء عند تفاعل البرمجيات المعدلة والمراجعة مع أجزاء النظام الأخرى. كما أن إفشاء البيانات الضمنية قد يضر بالوضع التنافسي للمنظمة مما يؤدي إلي خسارتها بل وبقائها.

من هذا المنطلق، يجب أن تمتد إجراءات الأمن الملائمة لما بعد النهايات الطرفية وخطوط الاتصال إلي مجال نظام المعلومات بالكامل. فعلي سبيل المثال، عدم ملاءمة تداول وسائل تخزين البيانات والمعلومات (سواء كانت ورقية، ممغنطة، ضوئية، الخ)، بالإضافة إلي عدم ملاءمة طريقة التخلص أو تدمير التقارير التي تمثل مخرجات النظام تؤدي إلي ثغرات أمنية مكلفة. فمثلا قد تشتمل مخرجات الحاسبات الورقية علي معلومات ضمنية أو تنافسية أو مفاتيح تخص الوصول للنظام وأصوله، كما أن كثيرا من الشركات أو المؤسسات المختلفة لا يتوافر لها سياسات واضحة للتخلص أو لاستبعاد أصولها المعلوماتية مما يجعل أمن المعلومات سهلا في الاختراق.

وقد يؤدي عدم وجود سياسات واضحة لاستخدام نظام المعلومات إلي مشكلات أمن ضخمة يتعرض لها النظام، كما في حالة أعمال الصيانة والسلامة عند نقص الأفراد المؤهلين، أو بسبب تغيير ودوران العمالة، أو إدخال تكنولوجيات متقدمة تتطلب مهارات جديدة، أو إبطاء العمل أو توقفه التي يجب مراعاتها من بدء التخطيط لنظم الأمن والشفافية المطلوبة.

ومن الملاحظ أن كثيرا من المؤسسات أو المنظمات السياسية والاقتصادية والاجتماعية القائمة حاليا وخاصة في المجتمعات النامية لم تجاري حتى الآن التطور والنمو التكنولوجي المرتبط باستخدام نظم المعلومات وتأمينها، فلا يزال يوجد قصور واضح ونقص كبير في التقنين والتوحيد لعدم الأخذ بالمعايير الدولية والتشفير الخاص بالمزاولة الأحسن، إلي جانب قصور الإرشاد والتوعية والحقوق والالتزامات القانونية، مما يزيد في النفقات ويسبب تأخير الأعمال وعدم تكامل البيانات. السماح باستمرار الوضع الراهن يحد من النمو المستقبلي ويؤخر في اللحاق عصر المعلومات والمعرفة المستهدف.

5-3 الأضرار الناجمة من قصور أمن المعلومات:

الأضرار التي تنجم عن قصور وفشل إجراءات الأمن تؤدي إلي خسارة مباشرة تعود بالضرر علي المنظمة المعنية. علي سبيل المثال، تتمثل الخسارة المباشرة في المصالح أو الأجهزة الحكومية علي المعالجات، محطات العمل، الطابعات، الأقراص والأشرطة وأجهزة الاتصالات؛ البرامج المتضمنة في نظم التشغيل وبرمجيات التطبيقات؛ التوثيق المتضمن المواصفات وأدلة

المستخدم وإجراءات التشغيل؛ والقوي العاملة المشتملة علي المشغلين والعاملين الفنيين والمساندين للنظام والمستخدمين؛ إلي جانب البيئة الطبيعية المتضمنة حجرات الحاسبات والاتصالات وأجهزة التكييف وإمداد الطاقة الكهربائية. وعلي الرغم من أن الخسارة المباشرة قد تشكل نسبة صغيرة من الخسارة الكلية النابعة من فشل إجراءات الأمن، إلا أن الاستثمار الكامل من تطوير وتشكيل النظام يعتبر جوهريا في العادة. ويتطلب نظام المعلومات حماية تختص بحقوقه من أصول المعلومات المخزنة في أوعيته وقنواته المختلفة والمتعددة. وتتصل الحاجة لحماية النظام والطريقة التي يعمل بها بالأسلوب المرتبط بحماية البيانات والمعلومات التي يقوم النظام بتخزينها ومعالجتها ونقلها لكي يحافظ علي توافرها وسريتها وخصوصيتها، وبما يمنع تبديل أوعيتها أو قنواتها التي يدخل من خلالها البيانات والمعلومات أو تصبح عرضة للفيروسات ذات التأثير الضار والمدمر علي تشغيل واستخدام النظام.

وقد تحدث الخسارة الناجمة عن ذلك، عند فشل نظام المعلومات في تحقيق الأهداف المتوقعة وأداء الأنشطة والمهام والخدمات المطلوبة منه. وتشتمل الخسارة النابعة من فشل إجراءات أمن النظام علي:

- خسارة السلع، الأصول الملموسة الأخرى، الاعتمادات أو الملكية الفكرية؛ خسارة معلومات قيمة.
- خسارة الرغبة في العمل الجيد والحميد للعملاء أو الموردين.
- خسارة المطالبة بالعقوبات من الانتهاكات الضارة وعدم الالتزام بالاتفاقات والتشريعات القانونية المنظمة.
- إلي جانب الخسارة والأضرار النابعة من ارتباك الأعمال وعدم مصداقيتها أمام الرأي العام والأجهزة الرقابية المسئولة.

في ضوء كل ذلك تصبح مهمة حماية وتأمين البيانات والمعلومات لها الأولوية القصوى والمطلقة في تخطيط وعمل نظم المعلومات علي كافة أنواعها وتوجهاتها.

3-6 تعزيز أمن النظم:

يجب موازنة أغراض السرية والسلامة والتوافر في مواجهة الأولويات التنظيمية الأخرى مثل فعالية التكلفة ضد انتهاكات الأمن السلبية. ويجب ألا تتعدى التكلفة العائد المتوقع. وعلي ذلك يجب أن تكون أساليب الرقابة علي الأمن كافية لمنع المتطفلين والمخربين الذين يحاولون دخول نظم المعلومات لرؤية المعلومات غير المصرح بها أو الحصول عليها أو تداولها، حيث أن استخراج أو استخلاص التكاليف وكمية الوقت المطلوب تعتبر أعظم من القيمة التي الممكنة التي تكسب من الاقتحام غير المعتمد.

وتساعد المقاييس الملائمة لأمن نظم المعلومات في تأكيد دقة وسلاسة الأداء الوظيفي لنظم المعلومات. وإلي جانب ذلك، فيما يتصل بالعوائد التي تعود بالنفع علي نظم المعلومات التجارية، فإن أمن نظم المعلومات قد يساعد في حماية البيانات والخصوصية الشخصية والملكية الفكرية لهذه النظم التي قد تخدم أيضا في تعزيز إجراءات الأمن المستهدفة. كما أنه من جهة أخري، أدي استخدام نظم المعلومات التجارية في جمع البيانات الشخصية وتخزينها وإحالتها أو الاتجار فيها إلي بزوغ الحاجة الملحة لحماية تلك النظم من الوصول إليها والاستخدام غير المعتمد لها. وتشتمل طرق حماية نظم المعلومات علي ضرورة التحقق من المستخدم لإضفاء الشرعية والصلاحية له، إلي جانب الرقابة علي الوصول لملفات البيانات وعلي التحكم في النهايات الطرفية وعلي مراجعة شبكة المعلومات. وفي العادة تساهم تلك المقاييس علي أمن نظم المعلومات وحماية البيانات والخصوصية الشخصية.

ومن الممكن أن يساء استخدام بعض المقاييس المطبقة والمكيفة لأمن المعلومات فيما يتصل بانتهاك الخصوصية الشخصية. علي سبيل المثال، من المحتمل أن الشخص المستخدم لنظام المعلومات أن ترصد بياناته لغرض غير مرتبط بالأمن للحصول علي معلومات عنه قد ترتبط ببياناته المالية والوظيفية والطبية وغيرها من البيانات الشخصية. وتعطي المبادئ والتوجيهات والمعايير التي تحدد لأمن وحماية خصوصية المعلومات الشخصية وتدفقها عبر حدود النظم بل والأمم توجيهات محددة في تحقيق واقع متوافق مع أهداف أمن نظم المعلومات وحماية خصوصية البيانات الشخصية، كما سوف يتعرض له في هذا العمل لاحقا.

وكما سبق بيانه، تتضمن نظم المعلومات الأجهزة،برامج الحاسب، قواعد البيانات، تصميمات ترتيب شرائح أشباه المعالجات Semiconductors، البيانات والمعلومات، إلي جانب العناصر التي تحمى بواسطة قوانين الملكية الفكرية والصناعية. وتعتبر الملكية الفكرية في نظم المعلومات غير محسوسة وتتخطى الحدود الافتراضية غير المدركة وعرضة للهجمات الضارة،

كما قد يقوي أمن نظم المعلومات حماية الملكية الفكرية بقصرها علي الوصول المعتمد والمصرح به لمكونات النظام كالبرمجيات أو المعلومات ذات الطابع التنافسي.

4. متطلبات الأمن الطبيعي لنظم المعلومات:

4-1 الأمن الطبيعي:

كما هو الحال مع مقاييس الأمن الأساسية المستخدمة في الأعمال المنزلية العادية، فإن الأمن الطبيعي لنظم المعلومات يعتبر متطلبا رئيسيا لابد من توافره لخدمة إنشاء بيئة وثقافة وصول مراقبة وممكنة ومعدة لحماية تعطل أو توقف نظام المعلومات بمكوناته المختلفة. وتتطلب المزاولات الأحسن لنظم أمن المعلومات تعريف التالي:

- الأفراد الذين يدخلون مواقع نظام المعلومات كحجرة الكمبيوتر أو مركز المعلومات سواء كانوا يعملون بها أو مترددين عليها لوحدهم أو بطريقة جماعية في بعض الوقت أو كله.
- الشروط والمزاولات المتعلقة باستبعاد أي من مكونات النظام التي لا تستخدم.
- الشروط المحددة لنقل وتخزين الوسائل أو الوسائط الطبيعية كالأشرطة أو الأقراص الممغنطة، الأقراص المدمجة أو أقراص الفيديو الرقمية، الخ.

إضافة لما تقدم يجب تقديم المتطلبات الفورية للنظم مثل:

- معدات الرقابة علي الوصول أو كروت التعريف والهوية.
- أبواب ونقاط وصول أخرى مؤمنة.
- مكتشفات الحرائق والمياه والدخان والإضاءة والدوائر التليفزيونية المغلقة.
- إمدادات الطاقة المؤمنة والمساندة الملائمة.
- الدواليب المغلقة وأدراج الكابلات وغير ذلك من المزاولات الهندسية المناسبة الأخرى.

وتعتبر هذه الأمور مهمة بصفة معينة عند توافر خدمات الحاسبات الآلية أو مراكز المعلومات من مصادر خارجية تختص بظاهرة "التعهيد Outsourcing". وعلي أي حال فإن مراقبة أو مراجعة مقدم أو مورد الخدمة تصبح من المتطلبات والشروط الهامة التي يجب مراعاتها.

وكما سبق ذكره، يجب ألا يتطلب أمن المعلومات السماح للمتطفلين أو المهاجمين من الاتصال الطبيعي مع الحاسب الآلي وملحقاته. ويتحقق الأمن الطبيعي عندما تستخدم آليات إضافية عديدة في نمط فعال.

والأمن الطبيعي يكمل مع الترتيبات الطبيعية بواسطة تقديم إجراءات وأدوات وبرمجيات تتمثل في التالي:

- هيكلة كيف يمكن الوصول للبيانات والمعلومات وبواسطة من.
- إعداد نسخ إضافية مساندة لكل البرمجيات وملفات البيانات حتى تساند استعادتها مرة أخرى عند حدوث الكوارث أو الفقد.
- تطبيق آليات تشفير ملائمة.
- اكتشاف ثغرات وانتهاكات الأمن.
- اكتشاف البرمجيات المعيارية المتعلقة بالنظم والبريد الإلكتروني والوسائل المختلفة.

2-4 عمليات التحقق من الأمن المستهدف:

يمكن تحديد أربع أبعاد رئيسية تستهدفه نظم أمن المعلومات المختلفة التي تتمثل في التالي:

(1) التعريف: Identification and Authentication

من يسمح له دخول النظام؟ يجب التحقق من ذلك من خلال ثلاث مداخل أساسية وممكنة هي:

1. ضرورة إعلام أو إخبار الحاسب الآلي عن شي معرف: أسم الشخص أو كلمة المرور Password. وعلي الرغم من أن كلمات المرور سهلة التطبيق والتنفيذ، إلا أنها تشتمل علي بعض القصور، حيث يمكن إعطائها لطرف ثالث. كما يمكن أن تكون موضوعا لقواعد معقدة ترتبط بعدد الحروف والأعداد، وتتغير بصفة كل فترة زمنية، الخ. وفي هذه الحالات يوجد توجه قوي في كتابة كلمات المرور التي يمكنها البقاء وعدم إفشاء محتواها حتى عندما يعثر عليه شخص آخر.

2. تقديم شيء ما مملوك للشخص للدخول في النظام كبطاقة هوية أو تعريف شخصي أو رمز ما، حيث يمكن أن يزداد أمن النظام بأن يطلب إضافة إلي كلمة المرور بعض أنواع المعدات الطبيعية ككارت أو بطاقة هوية أو رمز إلكتروني معين للسماح بالدخول.

3. إعطاء النظام شيء ما خاص بالمستخدم يرتبط بالخواص الشخصية مثل بصمة الإصبع أو نمط ذبذبة الصوت الشخصي التي يطلق عليها القياسات البيولوجية Biometrics حيث يمكن استخدامها في بيئة مؤمنة, وعلي الرغم من أن التكنولوجيا المرتبطة بذلك معقدة وباهظة التكلفة، إلا أن استخدامها في تزايد مستمر.

(2) **الاعتماد: Authorization**

بمجرد معرفة النظام بالمستخدم الحقيقي، فإن السؤال التالي الطبيعي هو ما يسمح به لهذا الشخص؟ وعلي ذلك فإن عملية الاعتماد تعتمد الوصول إلي الموارد لهذا المستخدم. علي سبيل المثال، تحديد المعاملات أو البيانات التي يسمح له بها، وتلك التي يمكن للمستخدم تعديلها أو إضافتها. وتبني مزايا الوصول المعتمد علي تحديد دور المستخدم ومسئولياته وحقوقه قبل النظام. وفي حالة مقدمي الخدمات المعلوماتية كالمكتبات، شركات التجارة الإلكترونية، الخ تقرر هذه المزايا بمعايير محددة تحددها العقود، الاتفاقات، الاشتراكات، أو حقوق الائتمان،الخ.

(3) الإدارة: Administration

تمثل الإدارة عملية حفظ سمات المستخدمين، بالإضافة إلي تعريف أمن مورد معين.ويشتمل ذلك علي أنشطة مثل استبعاد مزايا وصول مستخدم أو موظف ترك الخدمة، تغيير السمات، تحديد قائمة النظام لما يسمح به لمستخدم معين بعد الترقية أو النقل، الخ.

(4) **المراجعة: Audit**

تمثل عملية المراجعة التأكد من أن مقاييس الأمن مقبولة في نظام عمل محدد. وفي هذا الصدد، لا توجد طريقة معينة لمعرفة مدي تجاوز المستخدم الاعتماد أو الاعتراف الممنوح له بدون تلك المراجعات، كما لا توجد طريقة أخري أيضا توضح أن مقاييس الأمن يجب أن تحدد وتقوى بدون معرفة أولية لنواحي القصور التي قد تتواجد فيها، وبذلك تعتبر عملية المراجعة تكملة أساسية لكل مقاييس الأمن. وفي نفس الوقت، لن تكون أي من المقاييس فعالة بدون توافر عدد من الخصائص ذات التوجه البشري التي تتمثل في التالي:

- مساند الإدارة والإدارة العليا بصفة خاصة لسياسات ومقاييس وعمليات أمن المعلومات، ويجب عليهم الإلزام الكامل بها قبل إعداد الأمن وإدارته.
- ضرورة إلمام كل العاملين في كل مستويات الإدارة بالمخاطر المرتبطة بأمن المعلومات وبأهميتها لمنظمتهم.
- أهمية توافق وترابط كل برامج التدريب والتوعية عن أمن المعلومات مع حاجات المنظمة.
- ضرورة مراعاة التزام الأفراد الآخرين (كأفراد الصيانة، المستشارين، المتعاقدين، القوى العاملة المؤقتة، عمال النظافة، الخ) المتعاملين مع المنظمة والمتاح لهم الوصول إلي أصول معلومات المنظمة بقواعد وشروط الأمن الموافق عليا.

3-4 تفهم استخدام أمن نظم وتكنولوجيا المعلومات:

لا يجب أن يكون فهم استخدام نظم وتكنولوجيا المعلومات من منظور فني صرف لمن يستخدمون البرمجيات، تحديد نوع الأجهزة المتوافرة ومواصفاته الفنية، بل إن المطلوب فهمة ومعرفته عند استخدام النظم والتكنولوجيات يتمثل في التالي:

- ما الذي سوف يكون عليه تأثير حدث أمن رئيسي علي سمعة وشهرة المنظمة؟ وعلي أدائها المالي والتشغيلي، الخ؟
- كيف يصبح حرجا علي المنظمة وتوابعها التي تساند نظم وتسهيلات المعلومات مثل شبكة الويب، والبريد الإلكتروني، وتسهيلات الوسائل أو الوسائط المتعددة، الخ؟

كيف تستجيب المنظمة جيدا لقوانين ولتشريعات الملائمة(كما في حالة قوانين الملكية الفكرية، التجارة الإلكترونية والتوقيع الإلكتروني)؟

- ما مسئوليات المنظمة القانونية المرتبطة بأمن المعلومات؟

وحتى يمكن للمنظمة تطوير سياسات فعالة لأمن المعلومات، يجب عليها القيام بالمتطلبات والشروط المرتبطة بتقدير المخاطرة والبحث عن الأبعاد المعرضة للأخطار والهجمات المختلفة. ويجب أداء هذه العملية علي أساس دوري للبحث عن المشكلات الظاهرة وغير الظاهرة كما في حالات المزاولات السيئة المرتبطة بكلمات المرور، حذف التحديثات والحزم في تسهيلات البنية الأساسية، أجهزة الموديم للمكالمات غير المعتمدة وغير ذلك من مخاطر ترتبط بشبكة معلومات المنظمة.

4-4 تطوير سياسة أمن المعلومات:

يمثل هذا النشاط التطلب الأول لمعيار المنظمة الدولية للتوحيد القياسي ISO 177799 الخاص بإدارة أمن المعلومات. وتعتبر السياسة الموثقة لأمن المعلومات جوهرية وضرورية، وخاصة إذا قصد نجاح أمن المعلومات، حيث أنها تمثل الطريقة الفعالة للتعامل مع الأعذار المساقة بعدم المعرفة عن الأشياء أو المهام.

وتبني سياسة أمن المعلومات علي حاجات العمل أو المنظمة وترتبط بالمخاطر التي تصادفها أو تتعرض لها المنظمة المعنية ويتحتم عليها ضرورة فهمها والالتزام بأهمية تطبيقها. وفي هذه الحالة، يجب إعادة تأكيد أن أمن المعلومات ليس أمرا فنيا فقط يمكن تصحيحه والتغلب عليه بتركيب حائط نيران Firewall. من هذا المنطلق، يجب القوي العاملة بالمنظمة والأطراف الأخرى المتعاونة معها الاعتراف باستلام تقرير سياسة أمن المعلومات والتعهد بتطبيق ما جاء به من مبادئ ومعايير وقبول مقاييس صارمة في حالة عدم الالتزام بذلك.

وكأي عملية توثيق موجهة، توجد مخاطر في أن إعداد هذه السياسة وصيانتها وتوزيعها قد ينتج عنها بيروقراطية في حد ذاتها، لذلك يصبح الكم الجيد والصائب علي الأمور المتضمنة ضروري فيما يتصل بالنسب التي يجب تبنيها والأخذ بها، إلي جانب عدم التقليل في تقدير الجهد الذي بذل في إعداد هذه السياسة وحفظها أو صيانتها. وتتوافر كثير من المبادئ والأسس لإعداد سياسة أمن المعلومات التي يجب يمكن أن تصبح مفيدة ، إلا أن قيمتها المضافة سوف تقرر كيفية النجاح التي توصل بها ويعمل علي تطبيقا ومتابعته المستمرة. علما أن وثيقة أو تقرير سياسة الأمن المبنية علي أسس معينة وتحفظ أو تخزن علي أحد رفوف المكتبة أو أحد أدراج الحفظ لا تعني وجود سياسة أمن ولكنها لا تلبي أي قيمة للعمل، بل يجب تعميمها والتدريب عليها وتطبيقها ومراجعتها باستمرار. لذلك يجب أن يساند نشر تقرير سياسة أمن المعلومات حملة توعية عن الأمن لإعلام القوي العاملة بالمنظمة والأطراف الأخرى المتعاملة معها بأهمية تطبيق سياسة الأمن الموثقة، حيث يعتبر ذلك خطوة مهمة عند تدريب وتوعية العاملين الجدد في المنظمة.

5-4 محاسبة إدارة أمن المعلومات:

يمكن في هذا الإطار عدم تحديد مدي محاسبة ومسئولية القائمين علي أي عمل في وقت معين بالعناصر الأربع المتمثلة في: أي شخص، شخص ما، كل شخص، لا شخص. والتي يمكن

تعريفها بأن كل شخص فكر أن شخصا ما سوف يقوم بالعمل أو المهمة المعينة التي في الحقيقة يمكن لأي شخص أن يؤديها،إلا أنه في النهاية لم يقم بأدائها أي شخص.

ويمثل هذا القول الشائع حجم الكارثة عند إدارة أمن المعلومات بهذه الطريقة. ويتطلب تجنب هذه الحالة التعرف علي أن أمن المعلومات لا يمثل مشكلة من مشكلات تكنولوجيا المعلومات، بل يمثل مشكلة للمديرين أنفسهم لا يمكنهم التنازل عن مسئولياتهم تجاهها.

لذلك يجب علي الإدارة العليا بأي منظمة التعرف علي حاجات الأعمال وقيمة الأصول المطلوب حمايتها وتأمينها، وجعل الموارد متوافرة لنشر الأمن الضروري لها، واختبارها وإدارتها وصيانتها باستمرار.

وعلي هذا الأساس، يجب ان يقوم مديرو تكنولوجيا المعلومات أو مراكز المعلومات بأداء الأدوار التالية:

- قادة المبادرة في وضع مقاييس أمن المعلومات.
- منسقون رئيسيين لأعمال الأمن في المنظمة بكل قطاعاتها وإداراتها وأقسامها.

وبذلك يصبح في الإمكان محاسبة المديرين المختصين عن الطريقة التي تنفذ وتشغل بها كل الأوجه الفنية والأمنية التي تتضمن الخيارات المستخدمة، وكيف ومتي يرجع فيها لسياسة الأمن المطبقة، وما هي الموارد التي تصب في المهام التي يكلفون بأدائها وكيفية أدائها بطريقة جيدة. أما مسئولياتهم الأخرى فتختص بمدي الترتيب للدخول للتطبيقات والنظم والشبكات المتاحة، وإعداد الاختبارات لتعريف نقاط الضعف ونواحي القصور في إجراءات الأمن المطبقة، والقيام بتطوير وتحسين سبل اكتشاف البرامج والشفرات والأعمال المتطلبة لتقليل الإنذارات الزائفة، إلي جانب تنظيم وإدارة الأمن وتنفيذ مقاييسه المتفق عليها حتى يمكن تأكيد أن مصادر معلومات المنظمة آمنة من أي هجمات أو مخاطر داخلية أو خارجية.

6-4 تنفيذ أدوات ومنتجات الأمن الملائمة:

يتطلب تنفيذ الأمن الفني اختيار وتوريد تنوع كبير من المنتجات والأدوات المحتاج إليه والتي يجب إعداد وحفظ سجل فعالية خاص بها. ولهذه الأدوات والمنتجات قيمة محدودة أن لم تركب وتوضع موضع التنفيذ بطريقة ملائمة.

ويلاحظ أن الأداء الشائع لموردي هذه الأدوات والمنتجات، توريدها في مكونات معمارية يشار إليها بألفاظ مثل: "Cut of the Box" or " Shrink-Wrapped" التي تتضمن من بين الأوجه الأخرى: رقم تعريف تمهيدي للمستخدم Initial User ID، وكلمة المرور Password لمدير أو إداري الأمن الذي قد يكون معروفا للمتطفلين Hackers. لذلك يجب تغيير هذه القيم بمعايير محددة موافق عليها قبل استخدام هذه المنتجات.

ويكون مديرو أمن المعلومات المهنيين مسئولين مباشرة عن تطوير وإدخال وإدارة العمليات التي تساند إدارة ومراجعة عقود التوريد مع سياسات الأمن المطبقة لكي يستجاب لشروطها وقواعدها المتفق عليها. وتشتمل هذه العمليات علي مهمة مراجعة الحالات، الأحداث والاتجاهات بالإضافة إلي الإشعارات والإنذارات الصناعية.

وتبني المزاولة الأحسن Best Practice لتلك العمليات علي استخدام مركزية إدارة أمن المعلومات التي تأكد التوريد المركزي وتوزيع التسهيلات علي النقاط المحددة مع تأكيد حصول المستخدمين النهائيين علي أي تحديث للبرمجيات المخصصة لحماية البيانات والبرامج من الفيروسات الضارة مثلا.

5. اعتبارات وأبعاد أمن المعلومات:

يستعرض في هذا الجزء اعتبارات وأبعاد أمن المعلومات التي تشكل مع المتطلبات السابق الإشارة إليها المدخل الرئيسي لأمن وشفافية المعلومات.

5-1 اعتبارات أمن المعلومات:

يمكن تحديد ثلاث أبعاد رئيسية لأمن المعلومات هي:

(1) عدم تواجد أمن محقق بالكامل:

إي نظام أو أداة معلومات لا توجد طريقة واحدة لاعتماده. وتقتصر معرفة كيف استخدام النظام أو الأداة علي عدد محدود جدا من الأفراد، حيث لا تظهر أو تكتشف للكثيرين غير المؤهلين والمدربين. وفي مجال أمن المعلومات الذي لا يتقبل 100% من الصناعة، يمكن ملاحظة التالي:

- بينما تصمم البرمجيات لأداء وظائف معينة، فإن الخبراء المطورين (ومنهم المتطفلين مثل كل من Hackers، و Crackers) يمكنهم عمل ذلك لأداء أشياء أخري أيضا.
- لا توجد حتى الآن برمجيات كاملة الإتقان 100%، حيث أن كل البرمجيات تشتمل علي أخطاء Bugs في التشفير أو الترميز في برامج الحاسبات.

وتعتبر العبارات الأربع التالية صحيحة بطريقة عملية في الواقع الفعلي:

- البرمجيات الجديدة تتضمن وتعني أخطاء جديدة.
- الأخطاء القديمة لا تصلح دائما.
- لا تطبق التصحيحات Fixes دائما.
- قد تشتمل التصحيحات علي أخطاء جديدة.

(2) الموازنة بين المخاطرة والتكلفة:

كل من يأخذ الإجراءات المختلفة لحماية الممتلكات والأنفس والدرجة التي تنفذ بها هذه الإجراءات تتأثر بواسطة مدي التقدير بالمخاطر المحيطة والرغبة لقبول القيود التي سوف تفرضها هذه الإجراءات في حياتنا اليومية وتكلفتها.

ويجب التعرف علي أنه في الحياة الحقيقية يمكن حدوث التالي:

- علي الرغم من إجراءات الحماية التي نتخذها، لا يوجد ضمان بأنها لا تكون فعالة كل الوقت.
- تتغير المخاطر بمرور الوقت ضد ما نسعى إليه من إجراءات لحماية أنفسنا. وتحتاج عملية التقويم وإجراءات الحماية المتخذة لأمن المعلومات إلي أن تتغير بالتبعية حتى تكون فعالة.
- تشتمل إجراءات الأمن علي استثمارات ونفقات مستمرة.

ويتمثل مكون مزاولة أمن المعلومات الجوهرية في تقويم وتقدير قيمة الأصول المطلوب حمايتها مع التهديدات المعرضة لها وأثار هذه الاختراقات والثغرات علي أمن المعلومات. وعلي ذلك، يصبح من الضروري تعريف مستوي المخاطرة الكامنة الممكن تقبلها.

(3) توازن الحاجة للأمن وعدم الرضى عن الوضع القائم:

كما سبق ذكره، لا يوجد في عالم اليوم شئ كامل ومتقن كلية. ويعتبر ذلك صحيحا وحقيقيا فيما يتصل بالمعلومات والممتلكات والأنفس. ويتضمن كل إجراء أمن مضاف عملية أو نشاط إضافي موجه لمستخدمين نهائيين. وكلما تضاف هذه الإجراءات فق تصبح، في نفس الوقت، معوقات يجب التغلب عليها بواسطة كل مستخدم نهائي بغض النظر عن تذكره لكلمات مرور عديدة وما شابه ذلك من إجراءات أمنية. ونتيجة لذلك، يزداد تحميل مدير أو إداري النظام بأعباء جديدة عليه استيعابها وتنفيذها.

2-5 أبعاد أمن المعلومات:

عند التعرض للإبعاد المختلفة لأمن المعلومات، بمكن استقرائها من تحليل معايير أمن المعلومات وخاصة ما أصدرته المنظمة الدولية للتوحيد القياسي ISO من معيار ISO 177799 الصادر عام 1999 المبني علي معيار معهد المعايرة البريطاني BS 7799 الصادر عام 1995 ويعتبر كأساس نظام إدارة أمن المعلومات. ويمكن أن يلاحظ أن هذا المعيار يتسم بالتالي:

- عدم ذكر ضرورة وجود حائط نيران Firewall ولكن بدلا من ذلك يبين التحفظات المطلوبة لمنع دخول برمجيات مصابة ومعدية Malicious واكتشافها بسرعة.
- التمييز بين النظم المختلفة وعدم وجود نظام واحد يطبق في كل المنظمات، لذلك يصبح من الضروري تعرف كل منظمة علي متطلبات الأمن الخاصة بنظم معلوماتها.

من هذا المنطلق، يمكن تحديد الأبعاد والمكونات التالية لأمن المعلومات:

(1) سياسة الأمن:

الغرض لسياسة أمن المعلومات يتصل بتقديم توجيه مناسب ومساندة إدارية لأمن المعلومات والتوصية بما يلي:

- إنشاء منتدى لأمن المعلومات علي مستوي الإدارة العليا في المنظمة.
- تقديم حملات وبرامج للتوعية والتدريب علي أمن المعلومات.
- إدارة المخاطرة كمدخل من مداخل العملية الإدارية في المنظمة.

- التوافق مع القوانين والتشريعات الملائمة.

وعلي هذا الأساس، فإن أي وثيقة أو تقرير سياسة أمن يجب أن تتضمن التالي:

- حاجة المنظمة لخطة طوارئ Contingency Plan.
- الحاجة لمساندة حفظ بياناتها بفعالية وكفاءة.
- تجنب البرمجيات المصابة.
- توفير إجراءات رقابة الوصول لنظم المعلومات وبياناتها.
- الحاجة لتقرير الأحداث التي تتعرض لها المنظمة فيما يخص أمن معلوماتها.
- تحديد الإجراءات المطلوب اتخاذها عند حدوث عدم التوافق مع السياسة، النشاط المصاب، الاستخدام غير المناسب، الخ.

(2) تنظيم الأمن:

يهدف هذا البعد علي تركيز إدارة أمن المعلومات في المنظمة علي التالي:

1. صيانة أمن تسهيلات معالجة المعلومات التنظيمية وأصول الوصول إليها من قبل الأطراف الثالثة.
2. صيانة أمن المعلومات فيما يتعلق بمسئولية معالجة المعلومات وخدمات إتاحتها أو إمدادها المتعاقد عليها خارجيا من خلال "التعهيد Outsourcing".

ويحتاج تنظيم الأمن إلي إمداد المعالم التالية علي الأقل:

- إنشاء منتدى داخلي لأمن المعلومات.
- إقامة الترتيبات المختلفة لتنسيق أمن المعلومات.
- تخصيص مسئوليات أمن المعلومات للوظائف أو القوي العاملة المختصة.
- تعريف المخاطر المصاحبة لأمن المعلومات مع إمكانيات وصول الطرف الثالث للبيانات والمعلومات.
- تأكيد أن متطلبات الأمن قد حددت في العقود والتعاقدات مع الأطراف الثالثة.
- تضمين متطلبات الأمن مع التعاقدات الخارجية.

(3) تصنيف الأصول ورقابتها:

يهدف هذا البعد غلي تعريف مجال إدارة أمن المعلومات وتأكيد أن أصول المعلومات قد أعطيت مستوى ملائم من الحماية. والمنظمة التي تطبق معيار ISP 177799 تقرر أي من أصول المعلومات يكون له تأثير علي تشغيل وإتاحة أنشطة المنظمة أو العمل. ويتطلب ذلك تحليل احتمالية تقرير المخاطرة، وأن الأخطار المعينة تكتشف ضعف أو قصور معين يؤدي إلي إتلاف أو توقف أصل أو مجموعة من الأصول عن العمل. وتعرف المخاطرة بواسطة تجميع قيمة قابلية التعرض للهجوم أو الأخطار. وتعرف وتحدد كل الأصول المرتبطة بمجال أمن المعلومات والقائمين علي حفظها وصيانتها.

(4) أمن الأفراد:

الغرض من بعد أمن الأفراد تقليل مخاطر الأخطاء البشرية، السرقات، الاختلاسات أو سوء استخدام التسهيلات الخاطئ وبصفة معينة التالي:

1. تأكيد أن كل المستخدمين النهائيين ملمين بمخاطر وقضايا أمن المعلومات يمكنهم مساندة سياسات أمن المنظمة في بيان أعمالها العادية الجارية.

2. تقلي الأعطال والأضرار التي تسبب من القصور في أداء الأمن بالإضافة إلي التعلم من هذه الأحداث. والمهام المطلوب اتخاذها لتلبية هذا المتطلب تتمثل في التالي:

- تضمين اعتبارات ومسئوليات الأمن في توصيف الوظائف وإعداد عقودهم.
- تدريب المستخدمين النهائيين.
- تحديد تهديدات ومزاولات الاستجابة في حالات العجز عن الأداء وأحداث الأمن.

(5) الأمن الطبيعي والبيئي:

الغرض من هذا البعد يتمثل في تأكيد صحة وأمن تسهيلات معالجة المعلومات التي تتمثل في التالي:

1. تقليل مخاطر فشل النظم وتوقفها.
2. حماية سلامة البرمجيات والمعلومات.
3. صيانة وحفظ سلامة وتوافر معالجة المعلومات وتسهيلات الاتصالات.

4. تأكيد حماية البنية الأساسية أو التحتية المساندة.
5. تأكيد حماية المعلومات في الشبكات.
6. منع تحطم أتلاف الأصول الخاصة بنظام المعلومات.
7. عرض ضياع المعلومات، تعديلها أو سوء تبادلها بين المنظمات.

وتتمثل المكونات الدنيا لهذه المزاولات في التالي:

- الإجراءات التشغيلية الموثقة بالكامل(وتشتمل بصفة خاصة الأداء، إدارة الحدث، المشكلة والرقابة علي التغيير وإدارة المكونات، الخ).
- تكليفات مسئوليات واضحة للأفراد.
- الحماية في مواجهة البرمجيات المصابة.
- الأعمال الجارية (مثل: تسجيل وصيانة سجلات المستخدمين، استخدامات الموارد والمستودعات).
- إدارة شبكات المعلومات وتقليل المخاطر الناجمة مكنها.
- تداول وسائل أو وسائط المعلومات وتأكيد أمنها.
- تبادل المعلومات والبرمجيات مع الأطراف الأخرى.

(6) الرقابة علي الوصول:

الغرض من الرقابة علي الوصول Access Control لنظم المعلومات يتمثل في التالي:

1. منع الوصول غير المعتمد لنظم المعلومات.
2. تأكيد حماية الخدمات الشبكية.
3. اكتشاف الأنشطة الضارة أو غير المعتمدة.
4. تأكيد أمن المعلومات عند استخدام تسهيلات الحاسبات أو العمل عن بعد.

وفي هذا الصدد، يمكن ملاحظة أنه حتى الاستخدامات الفردية قد يكون لها وصول قانوني لنظم المنظمة، والبيانات والمعلومات، كما أن حقوقهم قد لا تتضمن وصولا عالميا لكل أصول المعلومات المتاحة.

وتحتاج أي منظمة لتعريف من له حقوق الوصول، إلي ماذا ومتي؟ ويمكن تحديد الأنشطة العادية المصاحبة للرقابة علي الوصول في التالي:

- تفسير متطلبات الرقابة علي الوصول (التركيز علي السرية والخصوصية)
- إدارة حقوق وصول المستخدمين الفردية.
- تفسير مسئوليات المستخدمين الفردية,
- تفسير الآليات الملائمة للوصول لشبكة المعلومات، التطبيق المعين ونظام التشغيل المستخدم.
- تحديد السياسات والمزاولات المختلفة لمراجعة الوصول إلي النظام واستخدامه.
- توضيح السياسات والمزاولات لمنح إمكانيات الوصول البعيد للعاملين عن بعد وللمستخدمين المعدات المحمولة.

(7) تطوير النظم وصيانتها:

يهدف هذا البعد تأكيد بناء الأمن في نظم المعلومات من حيث:

1. منع ضياع أو فقد بيانات المستخدم، تعديلها، أو الاستخدام الخاطئ لها في نظم التطبيقات المختلفة.
2. حماية سرية المعلومات وسلامتها.
3. تأكيد أن نظم المعلومات وأنشطتها المساندة تؤدي بطريقة ملائمة ومؤمنة.
4. حفظ أمن برمجيات وبيانات التطبيق المعين خلال دورة حياة النظام.

ويتطلب ذلك أداء التالي:

- تفسير متطلبات أمن نظم المعلومات وتطبيقاتها.
- تفسير دور الرقابة علي عملية التشفير Cryptography.
- تأكيد أمن ملفات النظام.
- تأكيد أمن تطوير ومساندة عمليات الأمن المختلفة.

(8) إدارة استمرارية الأعمال:

يهدف هذا البعد إلي التخلص من تعارض العمليات وتوقفها، وحماية العملية الحرجة من الأعطال والفشل والكوارث المختلفة.وفي هذا الإطار يمكن تمييز ثلاث أنشطة هي:

1. استعادة سيناريوهات الكوارث Disaster Recovery التي يمر بها النظام وسبل التغلب عليها: ويمثل ذلك مسئولية الأطراف المختلفة التي يتعامل معها أمن النظام وتقدم الاتصالات وإدارة العمليات الفنية الأساسية التي يعتمد عليها استخدامات الآخرين عن بعد، مع تقليد البنية التحتية المناسبة لتلك السيناريوهات.
2. استمرارية الأعمال Business Continuity يمثل المستوي الثاني الخاص باستمرار أداء الأنشطة الأساسية والمفسرة جيدا من موقع لآخر. ويحدد ذلك مسئولية الإدارة العليا وعدد العاملين المطلوب الوصول إليهم علي أن يكونوا مستعدين للقيام بهذه المسئوليات عندما يطلب منهم ذلك.
3. إدارة الأزمات Crisis Management التي تعتبر من مسئوليات الإدارة العليا الأخرى. وتتضمن الاتصال مع كل الأطراف الخاصة والمهتمة بأعمال الأمن عند حدوث الأزمات المختلفة.

(9) التوافق:

يهدف التوافق أو الالتزام Compliance تجنب أي ثغرات أو اختراقات لأي قوانين أو تشريعات مدنية أو جنائية ويعرف الالتزامات المتعاقد عليها والارتباطات مع سياسات الأمن التنظيمية وفعالية عمليات مراجعة النظام والإجراءات الأمنية.

ويتطلب هذا البعد معرفة شاملة بالإطار التشريعي والقانوني الذي تعمل فيه المنظمة، بالإضافة إلي مراجعة سياسات المن من هذا المنظور. وتصبح هذه المراجعة جزءا جوهريا لعملية التوافق **والالتزام.**

6- توجيهات ومعايير أمن وشفافية نظم المعلومات:

يشتمل هذا القسم من العمل المقدم علي تحديد معالم توجيهات ومعايير أمن وشفافية نظم المعلومات وتطبيقاتها وخدماتها. وبذلك سوف يستعرض الغرض من التوجيهات والمعايير،

ومجالها، وتعاريفها وأهداف الأمن بالإضافة إلي تحديد المبادئ العامة التي تبني عليها توجيهات ومعايير أمن وشفافية نظم المعلومات.

1-6 الغرض العام من توجيهات ومعايير أمن المعلومات:

يقصد من الأغراض العامة من توجيهات Guidelines ومعايير Standards أمن المعلومات التي تشكل وتطبق من قبل الأجهزة والمنظمات المعنية بالتوحيد القياسي والمعايرة مساعدة عمليات التطوير اللاحقة لنظم المعلومات واستخدامها. وبذلك ينظر إلي هذه الأغراض المنظمة والحاكمة كضرورة لا بد منها لزيادة الوعي بالمخاطر التي تواجه نظم المعلومات وإعادة تأكيد مدى مصداقيتها وجودتها، كما تتطلب من المنظمات والمصالح المختلفة التنسيق فيما بينها لخلق إطار شامل لأمن نظم المعلومات. كما تهدف التوجيهات والمعايير إلي زيادة الوعي بأهمية أمن نظم المعلومات، ومقومة الاختراقات التي تواجها من الداخل والخارج، وتجميع إحصائيات تخص أمن المعلومات بالمنظمة المعنية.

وعلي هذا الأساس، ينظر إلي أغراض توجيهات ومعايير أمن المعلومات، علي أنها تحقق التالي:

- زيادة الوعي بالمخاطر التي تواجه نظم المعلومات وبطرق التأمين والإنقاذ المتوافرة للتغلب علي هذه المخاطر.
- خلق إطار عام لمساعدة أولئك المسئولين في المنظمات والهيئات العامة والخاصة لتطوير وتنفيذ مقاييس وإجراءات ومزاولات متناسقة مع أمن المعلومات ونظمها.
- دعم التعاون بين القطاعات والمنظمات المختلفة في تطوير وتنفيذ هذه القياسات والإجراءات والمزاولات.
- رعاية الثقة فيما يتصل بنظم المعلومات وبالطريقة التي تقدم بها للمستخدمين.
- تسهيل تطوير واستخدام نظم المعلومات علي كافة المستويات القطاعية، القومية والدولية.
- دعم التعاون الدولي في تحقيق أمن نظم المعلومات.

2-6 مجال التوجيهات والمعايير:

تتجه توجيهات ومعايير أمن المعلومات إلي التطبيق في كل نظم المعلومات، سواء كانت مملوكة، مشغلة، أو مستخدمة بواسطة كيانات أو منظمات ذات طبيعة عامة أو خاصة، أو لأغراض ذات طابع عام أو خاص. وقد تحمى عناصر هذه التوجيهات والمعايير بواسطة قوانين الملكية الفكرية أو الملكية الصناعية أو أي قوانين وتشريعات أخرى. وكما سبق تحديده، فإن الغرض من التوجيهات والمعايير يرتبط أساسا بالتطبيق الكامل لها علي كل المستويات، وتوجه لكل الأطراف المعنية المتضمنة في نظم المعلومات، وتنسق بين مدخلين مزدوجين: أحدهما لنظم المعلومات المرتبطة بالأمن القومي، والمدخل الآخر متعلق بكل نظم المعلومات الأخرى. ومن المقبول به والملاحظ حاليا، أن الحكومات في معظم دول العالم قد تجد من الضروري إصباغ السرية المطلقة علي التوجيهات والمعايير وخاصة ما يرتبط بالمدخل الأول، وخاصة في حالات الأمن القومي وحفظ وصيانة النظام العام، علي أساس أن للحكومات حق السلطة المعترف به في القانون العام لعمل ما يجب عمله واتخاذه بصفة مطلقة في هذه المجالات الحيوية. علي أن أي ابتعاد عن التوجيهات والمعايير سوف يؤثر ويرتبط أكثر يما يخص تنفيذها علما بأن التوقعات علي الرغم من قلتها، كما ترتبط بالسلطات القائمة لذلك تصبح ذات أهمية عظمى. وقد يتنبأ أن المعلومات الملائمة سواء المتضمنة في نظام معلومات عام أو خاص سوف تكون معروفة لكل أو بعض الأطراف العاملة والمتعاملة والمهتمة بالمنظمة المحددة، وفقا لسياسة الأمن المحدد بمدي التوافر والسرية والسلامة.

من هذا المنطلق، يمكن أن تخاطب توجيهات و معايير أمن المعلومات المجالات التالي:

- القطاعات العامة والخاصة.
- التطبيقات المختلفة في كل نظم المعلومات.
- القدرة علي المساندة بواسطة الإجراءات والمزاولات المتعددة.
- توافر أمن المعلومات.

3-6 تعاريف التوجيهات والمعايير:

تتضمن تعاريف وتفاسير نظم المعلومات علي ما تتضمنه هذه النظم في الموضوعات التالية:

- الحاسبات الآلية وملحقاتها المادية المختلفة المترابطة معها؛
- البرمجيات وأساليب التعبير عن برامج الحاسبات الأخرى.
- الألجوريثمات والمواصفات الأخرى سواء كانت ضمنية في نطاق النظام أو يمكن الوصول إليها بواسطة الحاسبات الآلية.
- الأدلة والتوثيقات اليدوية الورقية، الممغنطة، الضوئية أو أي وسائل أخري.
- تسهيلات الاتصال مثل أجهزة النهايات الطرفية وعلاقاتها بالعميل في موقع العمل، أو المرتبطة بنقاط نهاية في شبكة نقل الاتصالات عن بعد التي لا تقدم للجمهور بصفة عامة.
- أبعاد الرقابة علي الأمن.
- عمليات التخزين، المعالجة، الاسترجاع، الإرسال ونقل بيانات الاتصال، وشفرات ووحدات الفص وشفرات تحويل الحزم.
- بيانات ومعلومات أطراف الوصول لنظم المعلومات.
- أدلة تعريف المستخدم، مقاييس التدقيق (سواء كانت مبنية علي المعرفة أو علي الرموز، أو سلوكية التوجه، أو الإحصاءات المطبقة علي قياسات بيولوجية Biometrics، الخ).

وقد تشتمل التعاريف والتفاسير علي العناصر التي تكون مملوكة أو غير مملوكة، عامة أو خاصة، متعاملة أو غير متعاملة مع البيانات المرسلة بواسطة النظام، أو العناصر الضرورية لتشغيل واستخدام وصيانة مكوناته الأخرى. وترتبط هذه العناصر بمدي سرية وسلامة وتوافر البيانات والمعلومات.ويؤكد عنصر التوافر مدي إتاحة البيانات ولأي الأطراف المحددة. وقد تكون عناصر السرية والسلامة والتوافر مهمة لأسباب تتعلق بالميزة التنافسية، الأمن القومي أو لتحقيق الالتزامات القانونية، التشريعية أو الأخلاقية مثل واجبات الائتمان، حماية البيانات الشخصية، الخصوصية، البيانات الطبية.

وتتلخص تعاريف وتفاسير المعايير والتوجيهات في التالي:

- تعني كلمة "البيانات" تمثيل الحقائق، المفاهيم أو التعليمات في طريقة رسمية ملائمة للاتصال، الترجمة، أو المعالجة بواسطة التعامل البشري أو من خلال الوسائل الآلية.

- تمثل كلمة "معلومات" المعني المخصص للبيانات بواسطة اتفاقات ومعالجات تطبق علي البيانات.
- تعني عبارة أو مصطلح "نظم المعلومات" الحاسبات، تسهيلات الاتصال، شبكات الحاسبات والاتصال، البيانات والمعلومات التي تخزن وتعالج وتسترجع أو ترسل بواسطة التكنولوجيات السابقة ومتضمنة البرامج، المواصفات، والإجراءات التي تقوم بتشغيلها واستخدامها وصيانتها.
- يعني لفظ " التوافر" خاصية البيانات، المعلومات ونظم المعلومات الممكن الوصول إليها واستخدامها علي أساس فوري أو وقي بالطريقة المطلوبة.
- يحدد لفظ "السرية" خاصية البيانات والمعلومات التي تعرض أو تتاح فقط لأشخاص، كيانات، وعمليات معتمدة في أوقات محددة ومعتمدة أيضا وبطريقة مجازة ومعتمدة.
- أما لفظ "الخصوصية" يعني خاصية البيانات والمعلومات ذات الطابع الشخصي والمؤسسي الدقيقة والكاملة التي تعتبر ملكية خاصة ومطلقة للممتلكين لها، وبذلك يحب العناية بحفظ الدقة والاكتمال لها.

4-6 أهداف الأمن:

يمثل أمن نظم المعلومات حماية توافر موارده ومكوناته والعمل عد\ سريتها وسلامتها. وفي غياب أمن كافي لنظم وتكنولوجيات المعلومات والاتصالات فإنها لا تستخدم كل قدراتها وطاقاتها. وغياب أو نقص الأمن يؤدي إلي فقد الثقة في النظام، كما قد يؤدي إلي توقفه وعدم الاستفادة القصوى منه مما يجعله عبئا علي المنظمة. وعلي هذا الأساس يجب حماية النظام والمعلومات من الأضرار التي قد تؤدي إلي فشل النظم وتعود بالخسارة علي منظماتها والعاملين بها.

وعلي هذا الأساس، يعتبر أمن النظم من الركائز الضرورية والحاكمة في حماية الأفراد والمنظمات من الأضرار الناتجة من قصور لأمن، حيث يعتمد كل من الأفراد والمنظمات علي أداء نظم معلوماتهم من خلال ضمان أمنها بطرق دقيقة، ملائمة وموثوق منها. ومن الأمثلة الواضحة لأمن نظم المعلومات ما يمكن مشاهدته في نظم معلومات المستشفيات، نظم الرقابة علي المرور أو الملاحة الجوية، محطات القوي النووية، الخ. ويتجه الأمن إلي حفظ فعالية وكفاءة نظم المعلومات، وتأكيد مستوي مناسب لتوافرها وسريتها وسلامتها،إلي جانب تسهيل تطويرها واستخدامها من قبل الأفراد المعنيين بأغراض جديدة غير تقليدية تختلف عن تلك التي تطبق بالفعل، وتسهيل استغلال

تكنولوجيا المعلومات بأقصى طاقاتها وإمكانياتها. وبذلك يسهم مجال أمن النظم في حماية حقوق واهتمامات كل المعتمدين في التعامل معها من بحمايتها وصيانتها من الضرر الناتج من فشل توافرها وسريتها وسلامتها.

5-6 المبادئ العمة لتوجيهات ومعايير أمن المعلومات:

يعالج هذا الجزء المبادئ العامة التي يجب أن تبني عليها التوجيهات والمعايير الخاصة بأمكن المعلومات. وق أمكن تحديد تسعة مبادئ أساسية ترتبط بالتالي: المحاسبة، التوعية، الأخلاقيات، تعدد وتداخل المجالات، التناسب، التكامل، الفورية، إعادة التقويم والديمقراطية. وهي مبادئ يجب أن تراعي في تصميم وإعداد توجيهات ومعايير أمن المعلومات.

(1)المحاسبة: Accountability

يحدد مبدأ المحاسبة ضرورة التعبير والتخصيص عن المسئوليات والمحاسبة عنها في المواقف المختلفة المتصلة بأمن نظم المعلومات، من يمتلكها ومن يقدمونها ومن يستخدموها وكل الأطراف الأخرى المرتبطة والمهتمة بها. ويتضمن ذلك:

- المديرون التنفيذيين.
- المبرمجون.
- مقدمو خدمات الصيانة.
- مديرو نظام المعلومات(مثل مديري البرمجيات، التشغيل، والشبكات).
- مديرو تطوير البرمجيات.
- المديرون المسئولين عن أمن نظام المعلومات.
- مراجعو نظم المعلومات داخليا وخارجيا.
- ..الخ.

(2) التوعية: Awareness

يقصد بهذا المبدأ مساعدة من الأفراد المهتمين قانونيا بنظم الأمن علي التعلم والتعرف عن أمن نظام المعلومات. ولا يقتصر ذلك علي مجرد النجاح لنظام المعلومات أو مقاييس أمن معينة، ولا يجب أن ينشأ كاتجاه لأمن محفوف بالمخاطر. وفي هذا الإطار، فإن مستوي المعلومات التي

يسعى إليه والمطابق لهذا المبدأ، يجب المساعدة في الحصول عليه بدون تهاون في إجراءات الأمن. ويتضمن هذا المبدأ الملاك والمقدمون، حيث قد توجد حالات يحتاج فيها إلي التزود بمعلومات حول أمن النظام. علي سبيل المثال، قد يدخل مالك شبكة معلومات في اتفاق أو اشتراك في خدمة قد ترغب منظمة أخرى في استخدامها لتقديم خدمات لأطراف ثالثة. وقد يتطلب مالك النظام، كجزء من الاتفاق، أن تقدم أو تتوافر له مستويات أمن معينة. وفي هذه الحالة، قد يرغب هذا الشخص أو تلك المنظمة المالكة للنظام التعرف علي أمن نظام معلوماته. وتشبيها بذلك، قد تتعاقد أي منظمة مع مالك شبكة المعلومات أو الحاسب الآلي لتقديم خدمات معينة قد تتطلب لتأكيدات خاصة بالأمن والقدرة المستقلة في تحقيق الأمن ومراجعته بصفة مستمرة.

ويتضمن مستخدمو نظام المعلومات أيضا في مبدأ التوعية. علي سبيل المثال، المستخدم النهائي أو العميل الذي يختار بنك معين، قد يكون له اهتمام شرعي في معرفة سياسات المن لهذا البنك والبنوك الأخرى. واعتمادا علي سياسات الأمن المستخدمة تسوق وتروج الخدمات المصرفية كأداة لجذب العملاء.

وحتى يمكن اكتساب الثقة في نظام المعلومان، يجب أن يكوم الملاك ومقدمو ومستخدمو النظام قادرين وجاهزين في التوعية عن أمن المعلومات، كما يجب عليهم أيضا أن يكونوا متضمنين في حفظ وصيانة الأمن. وبذلك يصبح مبدأ التوعية هاما في اكتساب المعرفة الملائمة والتعرف علي تواجد مزاولات وإجراءات لأمن النظام.

(3) الأخلاقيات: Ethics

في الحقبة المعاصرة، صارت نظم المعلومات تتخلل مجتمعاتنا وثقافاتنا، وقد صاحب ذلك نمو التوقعات والقواعد المرتبطة بالأمن الملائم في إمداد واستخدام هذه النظم. ويساند هذا المبدأ تطوير معايير اجتماعية ترتبط بأمن المعلومات التي تمثل أوجه مهمة في التعبير عن المعايير والتوجيهات لكل أعضاء المجتمع علي كافة مستوياتهم وأعمارهم بالإضافة إلي غرسها في أذهان الطلاب والشباب والعاملين وتتضمن في الأعراف المعمول بها منذ الصغر. أي أن نظم المعلومات وأمنها يجب أن تقدم وتستخدم بالطريقة التي تحترم بها الحقوق والاهتمامات الشرعية للآخرين.

(4) المجالات المتعددة البينية والمتداخلة: Multidisciplinary

عند تصميم وصيانة مقاييس ومزاولات وإجراءات أمن نظم المعلومات، يصبح من المهم عرض ومراجعة المدى الشامل لاحتياجات ومتطلبات الأمن وخياراته المتوافرة. علي سبيل المثال،

قد يتضمن في أي منظمة استشارة الأفراد الفنيين، أفراد الإدارة والإدارة القانونية، المستخدمين وغيرهم فيما يتصل بتكامل النظم وإجراءات الأمن بطريقة متداخلة ومتعددة. مع العلم بأن لكل هذه المجموعات والأطراف المتضمنة في النظم وأمنها منظورات ومتطلبات وموارد مختلفة يجب استشارتها ومعرفتها لكي تجمع المعلومات النابعة عنها معا لإنتاج مستوي أمثل لأمن النظام المستهدف. كما أنه علي مستوي السياسة، فإن التوجيهات تسهم في إعادة تقوية الأمن بنضوج كافي.

من جهة أخرى، يعترف هذا المبدأ باستخدام نظم المعلومات لأغراض عديدة مختلفة، وبتنوع متطلبات الأمن نتيجة لذلك. علي سبيل المثال، قد تختلف حاجات المصالح الحكومية والمدنية للأمن عن المصالح الأمنية والحربية، كما يتنوع ويختلف أمن المعلومات فيما يتصل بكل نوع من قطاعات الأعمال والتجارة وغيرها.

(5)التناسبية: Proportionality

لا يتطلب كل نظام معلومات أقصى درجة من الأمن، كما أنه من المهم ألا تكون النظم آمنة بدرجة غير كافية، أي أنه من غير الجدوى أن تتعدى إجراءات الأمن المتطلبات المعقولة للنظام. وبذلك تختلف هرمية نظم المعلومات وحاجاتها الأمنية من قطاع لآخر ومن منظمة لأخرى، أي لا يوجد حل واحد لمشكلات وقضايا الأمن المختلفة والمتعددة.

وفي تقويم حاجات الأمن، يجب معرفة المعلومات المستهدفة أولا بحيث يخصص قيمة لها، كما يجب إعداد مقاييس ومزاولات وإجراءات الأمن الممكنة وتوفيرها لحماية عناصر نظام المعلومات المختلفة، وتحسب تكاليف تنفيذ وصيانة خيارات الأمن.

وعلي هذا الأساس، يجب وزن وقياس مستوي نوع الأمن المعين في مواجهة احتمال الأضرار الخطيرة التي يتعرض لها وتكلفتاه علي النظام بالإضافة إلي تكلفة مقاييس الأمن ذاتها، مع القيام بتحليل نظام المعلومات في سياق كل الإجراءات والنظم الأخرى المتطابقة.

أي أن مبدأ التناسبية يتضمن مستويات وتكاليف ومقاييس ومزاولات وإجراءات الأمن التي يجب أن تكون ملائمة ومناسبة لقيمة ودرجة اعتماد الثقة واعتما دية نظام المعلومات، وذلك في مواجهة خطورة واحتمالية ومدي الضرر الكامن في النظام كمتطلبات للأمن المطلوبة.

(6) التكامل: Integration

يعتبر أمن نظام المعلومات أحسن فاعلية وكفاءة عن\د تصميم النظام ذاته، كما قد تصاغ وتستنبط صيغة لها تختبر لتجنب عدم التوافق. وقد تقلل تكاليف الأمن الكلية، ويتطلب الأمن في كل مرحلة من مراحل دورة حياة عملية تطوير نظام المعلومات المرتبطة بجمع البيانات والمعلومات وخلقها ومعالجتها وتخزينها ونقلها واستبعادها في كل مرحلة.

وبذلك يختص مبدأ التكامل بالمقاييس والمزاولات والإجراءات الخاصة بأمن المعلومات التي يجب أن تتكامل وتنسق معا ومع غيرها من الأبعاد الأخرى في المنظمة لخلق نظام أمن معلومات متكامل ومتناسق.

(7) الفورية أو الآنية: Timeliness

في بيئة نظم المعلومات المتواصلة والمتداخلة معا تتلاشى أهمية الوقت والمكان علي مستوي العالم. ويمكن الوصول لنظم المعلومات بغض النظر عن الموقع الطبيعي لها. ويعترف مبدأ الفوري أو الآنية أنه طبقا لطبيعة نظم المعلومات المتصلة والمتداخلة والعابرة للحدود واحتمال حدوث الأضرار لهذه النظم بسرعة، قد تحتاج الأطراف المتضمنة إلي العمل معا بسرعة متناهية لمجابهة التحديات التي توجه نظم المعلومات. واعتمادا علي ثغرات الأمن. ويعترف هذا المعيار بحاجة القطاعات العامة والخاصة إلي إنشاء إجراءات للتعاون السريع الفوري والفعال استجابة لثغرات وأخطار الأمن. وعلي ذلك، يجب أن تعمل كل الأطراف المعنية بطريقة منسقة وبسرعة لمتع أي أخطار أو ثغرات في نظم المعلومات الخاصة بها.

(8) إعادة التقويم: Reassessment

يعترف هذا المبدأ بديناميكية نظم المعلومات في طبيعتها، مع العلم أن متطلبات أمن نظم المعلومات تتغير علي الدوام ولا تعتبر ثابتة في كل الأوقات. وعلي ذلك، يجب أن تمر نظم المعلومات بعملية تقييم مستمرة ودورية تتعلق بقيمتها وخطورة واحتمال ومدي الأضرار التي تتعرض لها. بالإضافة إلي متابعة مهمة التنفيذ في ضوء التطورات التكنولوجية الحديثة سواء المطبقة بواسطة الجهة المالكة للنظام أو المتوافرة للاستخدام من قبل الآخرين. أي أن أمن نظم المعلومات يجب إعادة تقييمه دوريا، حيث أن نظم المعلومات ومتطلبات أمنها تتغير خلال الوقت.

(9) الديمقراطية: Democracy

تقاس متطلبات أمن نظم المعلومات في مواجهة الاهتمامات الشرعية لكل الأطراف المعنية من مطورين ومشغلين ومستخدمين يرتبطون باستخدام المعلومات وتدفقها بهدف الوصول للتوازن

طبقا للمجتمع الديمقراطي. وقد يفترض البعض غير الملم بأمن نظم المعلومات بأن ذلك قد يؤدي إلي قيود في الوصول للبيانات والمعلومات وفي تدفقها وحركتها. علما، أنه علي العكس، يعزز الأمن الوصول للمعلومات وتدفقها من خلال توفير نظما أكثر دقة وموثوقية وتوافر. علي سبيل المثال، يساعد انسجام وتوافق توجيهات ومعايير الأمن الفنية في منع تكاثر النظم المتفرقة غير المترابطة معا، وبذلك توجد ضرورة في توافق أمن نظم المعلومات من حيث استخدامها وتدفقه بعدالة وتوازن في المجتمع الديمقراطي.

7- تنفيذ أمن المعلومات:

يجب أن تسعي الحكومات والمنظمات المعنية علي كافة توجهاتها في تأكيد أهمية الأخذ بأمن المعلومات والتوجيهات والمعايير المنظمة له، بالإضافة إلي ضرورة التواصل والتعاون والتنسيق في تنفيذ أمن المعلومات علي كافة المستويات المؤسسية والقطاعية والقومية والدولية.

1-7 تطوير السياسات: Policy Development

سبق استعراض موضوع تطوير سياسة أمن المعلومات (البند 4-4) عند استعراض موضوع متطلبات الأمن الطبيعي للمعلومات وضرورة تطوير سياسات الأمن الملائمة لذلك، إلا أن العرض التالي يرتبط ببثمان عوامل جوهرية يجب أن تتضمنها سياسة تطوير أمن المعلومات التي تتمثل في:

(1) إنسجام وتوافق توجيهات ومعايير الأمن عالميا:

توجد حاجة ملحة لإعداد توجيهات ومعايير أمن فنية ملائمة ترتبط بالمنتجات والنظم المستخدمة تراعيا انسجام التطبيق الجغرافي المتسع والممتد علي أوسع نطاق علي مدي العالم لمعايير أمن سياسات نظم المعلومات World Wide Harmonization of Standards. إن تطوير توجيهات ومعايير أمن المعلومات يمثل المنتج التعاون في نظم الأمن بين الحكومات ومنظمات التوحيد القياسي والمنتجين والموردين والمستخدمين لنظم المعلومات. وبينما يستهدف التوصل لمعايير منسجمة معا، مع مراعاة عدم وجود حل أمن واحد لكل المنظمات، فإن احتياجات الأمن تتنوع إلي حد كبير من قطاع لآخر، من شركة أو منشأة لأخرى، من إدارة أو حدة تنظيمية لأخرى، أو من نظام معلومات لآخر، الخ. ويؤدي نقص أو عدم الفهم المتوازي للمستخدمين إلي مخاطر جمة خارج نطاق التوحيد التكنولوجي المطلوب.

وعلي ذلك تتمثل الخطوة الأولي في إعداد سياسة الأمن إلي ضرورة التعرف علي التنوع الضمني لحفظ وحماية نظام المعلومات ومدى احتياجات المستخدمين المتغايرة وفهمهم لذا العامل الحاكم.

(2) ترويج الخبرة والمزاولة الأحسن:

ضرورة قيام كل الأطراف المعنية بأمن نظم المعلومات علي كافة مستوياتها وتنوعها بترويج خبراتها ومزاولاته الأحسن Promotion of Expertise and Best Practice في إعداد وتنفيذ سياسات أمن المعلومات الخاصة بها، بهدف تعزيز وترقية الخبرة والوعي بمفاهيم المزاولات الأحسن. ويشتمل ذلك علي تحديد الانطباعات الشخصية في تحليل المخاطرات وإدارتها وتأمين النظم ومراجعتها. وقد تتنوع برام إعداد سياسات الأمن المطبقة من قطاع لآخر أو من منظمة لأخرى. علي سبيل المثال، تختلف متطلبات سياسات أمن المعلومات في القطاع المصرفي عنها في القطاعات الأخرى.

(3) إبرام العقود الصحيحة:

يلاحظ أن أهداف الأطراف المختلفة المرتبطة بالمعاملات أو التصرفات الإلكترونية لا تختلف عما هو متواجد في المعاملات الورقية التقليدية لحد كبير. وبصفة عامة، فإن المشاركين في نقل المعلومات، سواء كانت إلكترونية أو ورقية، يريدون معرفة والتأكد من أن المعلومات المرسلة والمتدفقة هي المرغوبة وترد من مصادر معتمدة وموثوق منها، كما أنها تصل في الشكل المرغوب فيه غير المتغير وغير المعالج صوريا. وعلي الرغم من أن أهداف أطراف المعاملات الإلكترونية والورقية متشابهة لحد كبير، إلا أن الطريقة في تحقيق هذه الأهداف ليست متشابهة بالتبعية، حيث أنها تختلف فيما يتعلق بطرق إنشائها، استخدامها، إرسالها، تخزينها، والوصول إلي المعلومات فيها. كما تختلف أيضا الطرق المستخدمة لحماية المعلومات بها من الضرار والمخاطرة التي قد تواجهها.

وعلي ذلك، فإن التحدي الذي يواجه المؤسسات والمنظمات المختلفة يتمثل في إعادة المعاملات والتأكد من صحتها بنفس مستوي الثقة التي تتوافر حاليا للمعاملات الورقية التقليدية. وقد يتحقق ذلك من خلال عدد من الطرق منها:

- إمكانية تطبيق القواعد الحالية للمعاملات الإلكترونية.
- إمكانية تعديل القواعد الحالية وتطوير قواعد جديدة.

- إمكانية تطبيق الوسائل التكنولوجية الحديثة.
- القيام بدراسات إضافية وتحسين القوانين والتشريعات التجارية التي تتضمن المعاملات الإلكترونية.
- تقوية المسئوليات القانونية المرتبطة بصحة العقود والتعاقدات.

(4) تخصيص المخاطر والمسئولية القانونية:

تؤثر ندرة تواجد قواعد للعقوبات والجزاءات تختص بتحديد الأضرار الناتجة من مدي تدني وانخفاض الإجراءات الأمنية وترتبط بتخصيص هذه المخاطر والمسئوليات القانونية Allocation of Risks and Liabilities علي فعالية وكفاءة النظم المطبقة لأمن المعلومات. وقد تشتمل هذه القواعد علي كل الأطراف المتضمنة في إجراءات الأمن كالبائعين، الموزعين، مشغلي الاتصالات، مقدمي الخدمات، المستخدمين، الخ. كما تتضمن نظما عديدة تستخدم في نقل المعلومات التي تكون خارج سيطرة أو مراقبة معالج المعلومات المختص. وقد تكون حقوق وواجبات الأطراف المتضمنة في أمن النظام غير واضحة في حالات الأخطاء، حذف البيانات أو تشويهها مما قد يؤدي أيضا إلي فشل النظام وما يتعرض له من حوادث جمة.

وتتضح الحاجة لتواجد قواعد أمن المعلومات المرتبطة بتخصيص المخاطر والمسئولية القانونية عنها عند سرقة أو فقد اعتمادات إلكترونية محولة بين المؤسسات المصرفية أو المالية عبر الدود الدولية علي سبيل المثال. وقد تتضمن هذه التحويلات كميات نقدية كبيرة وهي مزاولات مالية شائعة جدا. وفي حالة عند كفاية قواعد تخصيص المخاطر والمسئولية القانونية حيال ذلك، يجب العمل علي تطويرها في نطاق سياسة الأمن لتحديد المسئوليات القانونية في حالات الاحتيال والغش والتحويلات السلكية واللاسلكية المتسمة بالإهمال وعدم الموثوقية منها.

(5) العقوبات والجزاءات:

تعتبر العقوبات والجزاءات Sanctions في استخدام نظم المعلومات وسائل مهمة لحماية اهتمامات الأطراف المتضمنة المعتمدة علي هذه النظم في توافر بياناته وسريتها وخصوصيتها في مواجهة أي هجمات تعرضها للضرر والإفشاء والإتلاف. ومن أمثلة هذه الهجمات التي تعطل نظم المعلومات الفيروساتViruses، أو الديدان Worms التي قد تؤدي إلي تبديل البيانات، الوصول غير القانوني، الاحتيال أو خداع الحاسب الآلي، إعادة استنساخ البرمجيات بأسلوب غير معتمد، الخ. وللتغلب علي هذه المخاطر قد تختار المؤسسات والمنظمات المختلفة تنوع من الطرق والأساليب للتعرف عليها ووصفها. ويوجد اتفاق دولي علي أساس المحور المطلوب للمجابهة الأخطار والأضرار التي ترتبط بأمن نظم المعلومات من خلال القوانين الجنائية والمدنية التي تسنها الجهات التشريعية في دول العالم. وينعكس ذلك بالطبع علي تطوير القوانين والتشريعات المرتبطة بحماية البيانات والحد من جرائم الحاسبات الآلية.

وفي نفس الوقت، يمكن التعرف علي كثير من العوامل التي قد تتفاقم نحو الأسوأ وتلك التي تقلل وتلطف من خطورة الأداء والتصرف المعين. وتحدد نيات الطرف المختص، نوع البيانات المتأثرة (كما في حالة بيانات الأمن القومي أو البيانات الطبية)، مدى الضرر الناجم، والمدى الذي يتعدى فيه الطرف المتضمن الاعتماد الممنوح له. وتتمثل العقوبات الإدارية المرتبطة بالانتهاكات أو الاعتداءات عل أمن المعلومات علي الغرامات التي قد تفرضها المنظمة أو الجهاز الإداري المختص التي تعتبرها كثير من الدول كافية إلي حد ما في مجال حماية البيانات. هذا إلي جانب، الأنواع الأخرى من العقوبات علي مقاييس الانضباط أو العقوبات المدنية المختلفة.

وفي هذا النطاق ممكن أن يمتد مدى التعاون العربي والدولي في الأمور المرتبطة بقانون العقوبات علي جرائم أمن المعلومات بحيث تتضمن المساعدة المشتركة وتبادل المعلومات وتسليم المتهمين وغيرها من مجالات التعاون لحماية المعلومات وتأمينها بين الدول.

(6) الكفاءة القضائية:

إضافة إلي كفاءة المحاكم القانونية المرتبطة بأمن المعلومات ونظمها، قد يرغب البعض إعطاء المنظمات أو الأجهزة الإدارية المعينة حقوقا لفرض العقوبات الإدارية.

وقد تفرض وتخلق خاصية تدفق البيانات والمعلومات بين حدود الدول من جهة وحركة المنتهكين من جهة أخرى مشكلات كبيرة لمحاكمة جرائم الحاسبات والمعلومات. وعلي ذلك يجب

توافر قواعد منسجمة خارج نطاق القوانين والتشريعات القومية. وخلال أو أثناء تطوير هذه القواعد يجب أن تقوم كل دولة بمراجعة مدي ملاءمة تشريعاتها وقوانينها المحلية حتى يمكن التعامل مع الهجمات والأخطار عبر الحدود. كما أنه في حالة الدول التي قد تعترف التعاليم والمذهب المتواجدة بها علي إمكانية حدوث أحد عناصر الجرائم المعلوماتية من جهة، أولا تعترف كليا بهذه الجرائم من جهة أخرى، تبزغ الصعوبات لتطبيق قوانين جناية الحاسبات أو الجرائم المعلوماتية. وفي هذه الدول، يصبح من الضروري إدخال قواعد قانونية خاصة. علي سبيل المثال، أحدث وسن في المملكة المتحدة قانون سوء استخدام الحاسب Computer Misuse عام 1999 عندما يحث التطفل أو الاختراق في المملكة المتحدة أو أن التداخل البيني يؤثر علي استخدام الحاسبات فيها.

وعندما اقتراف مواطن جريمة كمبيوترية في ولاية أو دولة أخرى، قد تظهر مشكلات عند اكتشاف الجريمة وتواجد مرتكبها في دولة المنشأ. وكثير من الدول لا تسلم مواطنيها للمحاكمة علي الجرائم المعلوماتية لدولة أخرى. وفي هذه الحالات، يجب امتداد قواعد تسليم الخارجين علي القانون أو إمكانية نقل وقائع محاكماتهم إلي الدول المقترف بها الجريمة المعلوماتية. وسوف يسهم ذلك في تسهيل اتفاقات المساعدة المشتركة بين الدول والتعاون الإقليمي والدولي ونقل وقائع محاكمات الجرائم المعلوماتية في الأمور التي تخص أمن نظم المعلومات.

(7) الأدلة والبراهين:

أمن نظم المعلومات التي تحسن تعزيز دقة البيانات والمعلومات وتكاملها وتوافرها، تزداد قدراتها واعتمادها علي رصيدها من البيانات والمعلومات، مما قد يساعد إدخال واستخدام هذه المعلومات الموثوق منها كأدلة وبراهين موثقة في الوقائع الإدارية والقانونية. وفي إطار قواعد الأدلة والبراهين الواضحة في القانون المدني والقانون الجنائي وفي الوقائع الإدارية تصبح نظم المعلومات أكثر أمنا وتقدم تنبؤات أكثر أمنا ودقة للأفعال والتصرفات المتضمنة. وعلي الرغم من ذلك، قد تعرض السجلات الإلكترونية الحالية بعض المشكلات لقوانين الأدلة المتواجدة بالفعل.

2-7 التعليم والتدريب علي أمن المعلومات:

تتمثل المهمة الأولي في أمن المعلومات زيادة الوعي بالأمن لكل مستويات المجتمع المعاصر، في الأجهزة الحكومية والمنظمات والمؤسسات العامة والخاصة وكل الأفراد المستخدمين والمتعاملين مع نظم المعلومات، والتعرف علي أهمية وأهداف أمن المعلومات

والمزاولات الأحسن لإجراءات الأمن. ويتضمن دعم الوعي بأمن المعلومات التعرف علي المخاطر الكامنة وتطوير التوافق الاجتماعي لاستخدام نظم المعلومات بطريقة ملائمة.

ومن الضروري عند بناء الوعي بأمن المعلومات تعاون كل الأطراف المعنية والتزام الإدارة المختصة وعلي وجه الخصوص الإدارة العليا بذلك. كما يجب أن تتضمن برامج التعليم والتدريب علي موضوعات التوعية بأمن المعلومات التي توجه لفئات المستخدمين ورجال الإدارة علي كافة مستوياتهم الإدارية وأخصائيي الصيانة ومديري نظم المعلومات (مديري البرمجيات، مديري التشغيل، مديري الشبكات) ومديري تطوير البرمجيات والنظم، والمديرين المكلفين بأمن نظم المعلومات ومراجعي نظم المعلومات الداخليين أو الخارجيين المستقلين.

علي سبيل المثال، يجب تدريب المراجعين المؤهلين مهنيا علي فحص وتدقيق وتقويم نظام المعلومات، كما يجب أن يمتلك هؤلاء المراجعين معرفة متعمقة عن تخطيط وتطوير وتشغيل نظم المعلومات، بالإضافة إلي امتلاك الخبرة الفعلية في أداء مراجعات نظام المعلومات.

ومن المهم أيضا تقديم نوعية بأمن المعلومات ونظمها للمسئولين عن تعزيز القانون وخاصة لرجال الشرطة، المحققين، القضاة، رجال النيابة العامة، الخ.

وبذلك تهدف برام ج التعليم والتدريب دعم التوعية الضرورية بأهداف نظم المعلومات، والأداء الأخلاقي في استخدامها، وتطبيق إجراءات ومزاولات أحسن للأمن.

3-7 تقوية الأمن وإصلاحه وتبادل المعلومات والتعاون:

(1) تقوية الأمن وإصلاحه:

يجب تواجد أساليب أمن ملائمة ممكن الوصول إليها كمقدمة لصيانة وتقوية الحقوق المرتبطة بأمن نظم المعلومات وإصلاح أي انتهاكات لهذه الحقوق. ويتضمن ذلك الوصول إلي المحاكم المختصة وتوفير أساليب التحري الملائمة للسلطات المختصة. وتتضمن اختراقات أمن نظم المعلومات فشل أدائها، تعمد إفسادها، سرقة بياناتها، انتهاك خصوصيتها، إفشاء سريتها، الخ.

وتوجد حاجة ملحة لبرامج تعليم واتصال وتعاون أحسن، ومشاركة معلومات بين إدارات وأجهزة تنفيذ القانون، مشغلي قنوات الاتصالات، مقدمي الخدمة، والبنوك علي كافة المستويات الوطنية والإقليمية والدولية. وفي هذا الصدد، يجب تعاون سلطات تنفيذ وتقوية وتنقيح القانون مع كافة الأطراف المعنية بأمن المعلومات لتسهيل الاستخبارات والتحري في الدول الأخرى.

وفي هذا لإطار يجب:

- تقديم وسائل أمن ملائمة يمكن الوصول إليها لتقوية وصيانة الحقوق النابعة من تنفيذ توجيهات ومعايير الأمن.
- تقديم المساعدة والدعم الفوري فيما يتصل بالأمور الإجرائية والاستخباراتية المرتبطة بانتهاكات أمن نظم المعلومات

(2) تبادل المعلومات:

تتبادل الحكومات ووحدات القطاع العام والقطاع الخاص المعلومات فيما بينها، وتنشئ إجراءات لتسهيل وتبادل المعلومات المرتبة بتوجهات ومعايير الأمن وتعمل علي تنفيذها. وكجزء من الجهود المبذولة حيال تبادل المعلومات تنشر المقاييس والمزاولات والإجراءات التي تنشأ لمراقبة توجيهات أمن المعلومات. وعلي ذلك يجب القيام بالتالي:

- تبسيط تبادل المعلومات المختصة بتوجيهات ومعايير الأمن والعمل علي تنفيذها.
- نشر المقاييس والمزاولات والإجراءات التي تنشئ لمراعاة أمن المعلومات.

(3) التعاون:

يجب أن تطور الحكومات والقطاع العام والقطاع الخاص مقاييس ومزاولات وإجراءات أمن سهلة ومتوافقة مع تلك المطورة من قبل الأطراف الأخرى التي تذعن وتستجيب للتوجيهات والمعايير. كما يجب أن يراعي في تطوير هذه المقاييس والمزاولات تجنب أي تعارض وصعوبات في التطبيق. وبذلك يصبح التعاون الأساس الذي تطور به القوانين والإجراءات المطبقة علي كافة المستويات المحلية والوطنية والإقليمية والدولية.

8- الخلاصة:

استعرض هذا العمل المرتبط بتوجهات أمن وشفافية المعلومات في ظل الحكومة الإلكترونية، أن التوسع الكبير في استخدام تطبيقات وخدمات نظم المعلومات الإلكترونية المحملة علي كافة أنواع شبكات المعلومات (الشبكات المحلية، شبكات الإنترانت، شبكات الإكسترانت، شبكة المجال العريض وشبكة الإنترنت) التي تعتمد بعضها علي بعض، وقابليتها للتعرض للإضرار المختلفة وحاجتها لبناء الثقة فيها، كل ذلك أدي إلي تعظيم موضوع أمن المعلومات

ونظمها في البيئات الرقمية. وفي هذا الصدد حدد مفهوم أمن المعلومات وطبقاته المختلفة، وإطار الأمن، ومكونات ومحاور الأمن مع التهديدات علي أمن نظم المعلومات والأضرار التي قد تنجم من قصور إجراءات الأمن، مع تعزيز أمن نظم المعلومات القائمة.

وناقش هذا العمل أيضا متطلبات أمن المعلومات المختلفة التي ترتبط بالأمن الطبيعي لأجهزتها وبرمجياتها وشبكاتها، وتوضيح عمليات التحقق من أمن المعلومات من حيث التعريف، الاعتماد، الإدارة والمراجعة لها، مع تنفهم طرق وأساليب استخدام نظم الأمن، وتطوير السياسة الموجهة وإجراءات المحاسبة والتنفيذ المحتاج إليها. كما عرضت الدراسة الحالية اعتبارات وأبعاد أمن المعلومات، حيث تتمثل الاعتبارات في عدم تواجد نظم أمن محققة بالكامل، والتوازن بين المخاطرة والتكلفة وبين الحاجة للأمن وعدم الرضى عن الوضع القائم. أما أبعاد أمن المعلومات وخاصة ما يرتبط منها بمعيار إدارة أمن المعلومات للمنظمة الدولية للتوحيد القياسي ISO 177799 فتشتمل علي سياسة الأمن، تنظيم الأمن، تصنيف الأصول ورقابتها، أمن الأفراد، الأمن الطبيعي والبيئي، الرقابة علي الوصول، تطوير النظم وصيانتها، إدارة استمرارية الأعمال والتوافق.

كما وضحت الدراسة توجيهات ومعايير أمن نظم المعلومات فيما يتعلق بالغرض العام منها ومجالها والمفاهيم الخاصة بها بالإضافة إلي تحد المبادئ العامة منها، وكيفية تنفيذ أمن المعلومات من حيث تطوير سياسة خاصة به تتسم بالانسجام مع المعايير وتروج للأطراف المعنية وتحدد المخاطر المختلفة والمسئولية القانونية وما يرتبط بها من عقوبات وجزاءات.

ويلاحظ أن هذا العمل يؤكد بناء الثقة والأمن في استخدام تكنولوجيا المعلومات والاتصال، ويحدد أن تعزيز إطار الطمأنينة المرتبط بأمن المعلومات وأمن الشبكات وصيانة الحقوق والسرية والخصوصية تعتبر شرطا مسبقا لبناء وتعزيز جهود إقامة الحكومة الإلكترونية وصولا لمجتمع المعلومات المستهدف.

من هذا المنطلق عملت الدراسة علي ترويج ثقافة مجتمعية للأمن تطور خطط وسياسات لها وتنفذ بالتعاون مع كل الأطراف المتضمنة في أمن المعلومات. وفي إطار التوعية المستمرة بثقافة الأمن والتدريب عليها يمكن تعزيز الأمن ذاته وضمان حماية البيانات وسريتها وخصوصيتها والعمل علي توافرها للأطراف المعتمدة فقط وسوف يؤدي ذلك بالطبع إلي احترام المواطنين

لبرامج ومشروعات الحكومة الإلكترونية والولوج بخطي ثابتة نحو مجتمع المعلومات ذات التوجه التنموي ورفع مستوي معيشة وحياة الفرد والمجتمع.

وعلي هذا النهج، دعت الدراسة الحكومات ووحدات القاع العام والقطاع الخاص وكل الأطراف المعنية بأمن نظم المعلومات إلي اتخاذ الخطوات اللازمة لحماية أمن وشفافية النظم طبقا لمبادئ توجيهات ومعايير الأمن التي طورتها المنظمات الدولية المختصة، وعلي ذلك استنتجت الدراسة النتائج التالية:

- إقامة أطر سياسية وتنظيمية وقانونية لمواجهة الأمور المتعلقة بمخاطر الأمن كالقرصنة وإدارة أسماء النطاق وحماية المواطنين وتوسيع هذه الحماية في البيئة الرقمية.
- تطوير سياسة أمن المعلومات وتشجيع تطبيقها وتطويعها لبرامج وسجلات الحكومة الإلكترونية.
- تدعيم الخبرة والمزاولة الأحسن لأمن نظم المعلومات من خلال تطوير التوجيهات والمعايير الفنية علي نطاق واسع والاستعانة بما هو مطور عالميا.
- تنظيم حملات عامة لنشر الوعي تهدف إلي تحسين معرفة الجمهور وتفهمهم بأهمية أمن المعلومات وحقوق الملكية الفكرية وحماية البرمجيات.
- في مجالات البرمجيات والتجارة الإلكترونية وأنشطة التجارة المرتبطة بها ولأعمال والحكومة الإلكترونية، توجد حاجة ملحة لتعزيز المبادرات التي تضمن التوازن العادل بين حقوق الملكية الفكرية ومصالح مستخدمي المعلومات.
- تحديد وتخصيص المخاطر والمسئولية القانونية المتصلة بفشل أمن المعلومات، وما يرتبط بها من جزاءات وعقوبات إدارية وجنائية ترتبط بسوء الاستخدام أو تعمد الضرر.
- إصدار القوانين والتشريعات التي تحدد صحة العقود والوثائق المنشأة والمنفذة من قبل نظم المعلومات، وكفاية المحاكم التشريعية في تطبيق قواعد الأمن، وتسليم المتهمين في جرائم أمن المعلومات، وأساليب الحصول علي البراهين والأدلة والموافقة عليها في

  قواعد وبنود القانون المدني والقانون الجنائي، الخ.

وعلي الرغم من تعقد موضوع أمن وشفافية المعلومات، إلا أنه يمكن توفير بعض الأفعال المنطقية التي تساعد في تقليل مشكلات ومخاطر الأمن التي تتسبب في عدم أمن النظم. وفي هذا الصدد يمكن التوصية بالتالي:

- إدراك مشكلة أمن المعلومات وضرورة العمل علي حماية وتأمين نظم المعلومات وشبكات نقلها.
- استنباط استراتيجيات وسياسات أمن ملائمة.
- نقد بعض إجراءات علاج قصور أمن المعلومات البسيطة والتي تنفذ مرحليا.
- البحث عن مساعدات مهني وتعاون من كافة الأطراف المحلية والوطنية والإقليمية والدولية في مجالات أمن المعلومات.
- تطبيق التوجيهات والمعايير الدولية والمزاولات الأحسن في أمن المعلومات.
- ضرورة تعريف الفجوات الخاصة بأمن المعلومات المتواجدة في التشريعات والقوانين الوطنية والعمل علي تلافيها.
- حث الأمم المتحدة علي سن وإصدار قانون عن أمن المعلومات في الفضاء الخارجي Cyber-Space.

المراجع: References

1. Gelbstein, Eduardo and Kamal, Ahmed. Information Insecurity: A Survival Guide to the Uncharted Territories of Cyber-Threats and Cyber Security. (New York, UNICT Task Forth and UNITAR).
2. IEEE 8012.10 Standard for Interoperable Local Network Security (SILS).
3. IETF. IPSEC Working Group.
4. IETF. SAAG (Security Area Advisory Group).
5. INTOSAI. EPP Audit Committee (International Organization for Supreme Audit Institutions). Information System Security Review

Methodology: A Guide for Reviewing Information System Security in Government Organizations [October 1995].

6. ISO 13353: A Five Part Set of Guidelines for the Management of Information Security.
7. ISO 15408: Common Criteria for Information Security Evaluation [http://www.commoncriteria.org]
8. ISO 177799: Code of Practice for Management of Information Security.
9. ITU Recommendation X.273; Open Systems Interconnection, Network Layer Security Protocol.
10. ITU Recommendation X.509: Authentication Framework (relates to Digital certificate and Public Key Encryption).