العنوان:	أمن المعلومات .. مجالات الاختراق وآلية التعزيز
المصدر:	المجلة العربية للدراسات الأمنية
الناشر:	جامعة نايف العربية للعلوم الأمنية
المؤلف الرئيسي:	الطائي، محمد عبد حسين حسن
المجلد/العدد:	مج 20, ع 40
محكمة:	نعم
التاريخ الميلادي:	2005
الشهر:	أغسطس - رجب
الصفحات:	261 - 283
رقم MD:	354930
نوع المحتوى:	بحوث ومقالات
قواعد المعلومات:	EcoLink
مواضيع:	أمن المعلومات ، شبكات المعلومات ، تكنولوجيا المعلومات ، جرائم المعلومات ، تخزين و استرجاع المعلومات
رابط:	http://search.mandumah.com/Record/354930

أمن المعلومات ... مجالات الاختراق وآلية التعزيز

أ.د. محمد عبد حسين حسن الطائي(*)

التمهيـــد

واجهت واجهت المنظمات في السنوات الأخيرة تحديا كبيرا تمثل في الانتقال من شبكات المعلومات وهياكل النظم ذات الملكية الخاصة إلى شبكات المعلومات المفتوحة وهياكل النظم ذات الخدمات والزبائن المتنوعة والمتعددة . وعلى الرغم من أن هذه الشبكات زادت من كفاءة هذه المنظمات وعززت موقفها التنافسي في السوق إلا أنها بذات الوقت ـ وبسبب طبيعة البيئات المفتوحة التي تتسم بها ـ زادت من مخاطر أمن المعلومات ، إذ يؤكد المتخصصون في مجال نظم المعلومات على حقيقة جوهرية هي أن هذه الشبكات تعد سلاحا ذا حدين ، فمن جهة أسهمت في إحداث تغييرات جوهرية متسارعة ومطردة في أساليب وإجراءات العمل في المنظمات المختلفة عندما أصبحت عملية جمع البيانات من مصادرها المختلفة ومعالجتها وخزن المعلومات وتحديثها واسترجاعها وإيصالها إلى المستفيدين من خلال نظم المعلومات وشبكات الاتصالات المتطورة إحدى أهم السمات في عصرنا الحاضر «عصر ثورة المعلومات» ، ومن جهة أخرى سهلت هذه النظم والشبكات مهمة اختراق أمن المعلومات وسرقتها أو تحريفها وتشويهها أو إساءة استخدامها أو تسريبها خارج القنوات المخصصة لها أو المرخصة بتداولها والاستفادة منها (Jones,1993, 2) ، ذلك لأنه لا قيمة لهذه النظم وتلك الشبكات إلا إذا حصلت المشاركة بين المنظمة والمنظمات الأخرى ، وبناء عليه فالمنظمات ليست مطالبة بجعل معلوماتها متاحة خارج حدود نظمها وشبكاتها الخاصة فحسب و إنما السماح للآخرين بمراجعة أو تحديث معلوماتها في شبكاتها الداخلية أيضا ، الأمر الذي أتاح الفرصة لإسقاط حواجز الأمن المادية والإلكترونية المعتمدة من قبل المنظمات لحماية أمن معلوماتها .

(*) رئيس قسم إدارة الأعمال ونظم المعلومات الإدارية ، كلية الاقتصاد والعلوم الإدارية ، جامعة الزرقاء الأهلية .

مشكلة الدراسة

على الرغم من أن الرقابة القوية وفرت ضمانات جوهرية لحماية أمن المعلومات والحد من الوصول غير المرخص لها وكذلك التحريف والسرقة إلا أن التطورات الحديثة التي حصلت في نظم المعلومات وشبكات الاتصالات والتي تمت الإشارة إليها في المقدمة أعلاه قللت من فاعلية الرقابة التقليدية ، إذ وجدت هذه المنظمات أن سياساتها الأمنية المطبقة حاضرا بحاجة إلى التطوير أو أنها لم تعد ملائمة لمجاراة تلك التطورات بعد أن أصبحت سياساتها بخصوص أمن المعلومات لا تتناسب مع متطلبات نظمها وشبكاتها المتطورة بكفاءة وفاعلية . ففي المسح الذي تم إنجازه من قبل (Information Week Research) عن أمن المعلومات عام (١٩٩٩) والذي شمل (٢٧٠٠) من المختصين عالميا في هذا المجال اتضح الآتي (Palmer 2001, 14) :

١ ـ أشار (١٩٪) منهم إلى أنه لا توجد لديهم سياسة فاعلة لأمن المعلومات أولم تكن لديهم سياسة إطلاقا .

٢ ـ (٦٩٪) منهم مقتنع تماما بأن سياستهم الحاضرة لا تخدم بقوة أهداف منظماتهم .

٣ ـ يرى (٣١٪) منهم أن سياستهم الحاضرة عالية الفاعلية .

يضاف إلى ذلك أنه قد أظهر المسح أيضا أن هذه السياسات نادرا ما تتم مراجعتها وإعادة النظر فيها بصورة دورية للتحقق من ملاءمتها إذ اتضح الآتي :

٤ ـ (٤٠٪) منهم لم تكن لديهم برامج منتظمة لمراجعة سياساتهم الأمنية .

٥ ـ (١٥٪) منهم يقومون بالمراجعة لمرة واحدة فقط خلال السنة .

٦ ـ (٦٪) منهم لا يقوم بالمراجعة إطلاقا .

٧ ـ (١٠٪) منهم أنجز المراجعة لاكثر من مرة في السنة الواحدة .

٨ ـ (٢٤٪) منهم ينجز المراجعة بصورة مستمرة .

أهداف الدراسة وأهميتها

تسعى الدراسةالى تحقيق الأهداف الآتية :

١ ـ توضيح مفهوم أمن المعلومات وأهميته .

٢ ـ تحديد الأهداف الجوهرية التي تسعى المنظمة الى تحقيقيها من خلال أمن المعلومات .

٣ ـ بيان الجهات التي تخترق أمن المعلومات وأنواع المعلومات التي تثير الاهتمام لاختراق أمن المعلومات .

٤ ـ توضيح أهم المجالات التي يحصل فيها الاختراق .

٥ ـ بيان أنواع الخروقات الأمنية .

٦ ـ تقديم مقترح بالآلية الملائمة لتعزيز أمن المعلومات .

أما أهمية هذه الدراسة فيمكن تجسيدها من خلال الجوانب الآتية :

١ ـ يشير (Parker ,1997 : 15) إلى أنه على الرغم من أن العديد من المختصين لديهم خبرات وممارسات متباينة اعتمادا على الفرص المختلفة التي توفرها أعمالهم وبيئاتهم الثقافية وارتباط ذلك بالمشاكل والصعوبات المتعلقة بالمعلومات إلا أن هؤلاء المختصين لم تتوافر لديهم الفرصة والدافعية لإنجاز الدراسات عن أمن المعلومات بأنفسهم .

٢ ـ ازدياد حاجة مد راء المنظمات لفهم و إدراك خطورة وأهمية هذا الموضوع ومن ثم السعي إلى الاستجابة السليمة من خلال تطوير السياسات والإجراءات التي تكفل حماية أمن معلوماتها . إذ حذر أحد التقارير من أن معلومات المنظمة تعد بمثابة «الذهب» في عصر ثورة المعلومات على النحو الذي يتوجب على الإدارات أن تدرك أهمية وكيفية حمايتها بأسلوب مشابه لحماية الجواهر الثمينة (Jones , 1993 : 2) .

٣ ـ شمولية الموضوع وعدم اقتصاره على منظمة دون أخرى، إذ أكد (Hill, 1995: 15)على أن جميع المنظمات تعتمد على المعلومات في تسيير أنشطتها

المختلفة، وعليه فإن مشكلات أمن المعلومات ستؤثر عليها جميعا دون استثناء.

٤ ـ يؤكد (Lukanen , 1992 : A4) أنه في الوقت الذي تزايد فيه الاهتمام بنظم المعلومات الحاسبية و أمنها وكذلك أمن المعلومات بشكل كبير في الوقت الذي ازدادت وتشعبت الدراسات في هذا المجال إلا أنه لا يوجد هناك مدخل شمولي ومهم يتناول أمن المعلومات في المنظمات .

مفهوم أمن المعلومات

يشير (Parker , 1997 : 14-15) إلى أننا بوصفنا متخصصين في أمن المعلومات فإنه يجب علينا تقديم تعريف ووصف عام لمصطلح » أمن المعلومات « لإداراتنا وزبائننا وصحفييها ونظرائنا في الحقول الأخرى بل لعائلنا أيضا . وأورد هذا الباحث تعريفات متعددة الأغراض بحيث يتناسب كل تعريف مع ما يعنيه بالنسبة لكل جهة ذات علاقة ، وفيما يأتي نعرض هذه التعريفات :

١ ـ هو المحافظة على المعلومات وسلامتها وسريتها وملكيتها والاستفادة منها .

٢ ـ هو المحافظة على المعلومات من تداخل استخدامها أو تخريبها أو استخدام معلومات مضللة أو تحريفها أو استبدالها أو سوء تفسيرها أو إلغاؤها أو سوء استخدامها أو الفشل في استخدامها أو الوصول إليها أو إظهارها أو مراقبتها أو نسخها أو سرقتها .

٣ ـ هو معالجة جميع الخروقات المذكورة في التعريف الثاني أعلاه قانونيا بشكل ناجح من قبل مالك هذه المعلومات بوصف هذه الخروقات انتهاكا لحقوق المالك .

٤ ـ هو الوظائف التي تهدف إلى حماية المعلومات والتي تشتمل على التجنب ، المنع ، الكشف ، الإعاقة ، التطفيف ، النقل ، التحويل ، الاسترجاع ، التصحيح والإقرار .

٥ ـ هو الإجراءات التي تحقق الحماية والتي يجب توجيهها من خلال الوفاء بالمعايير المحددة في إطار التشخيص السليم للسلبيات والتهديدات .

٦ ـ هو الحماية الدقيقة والتي غالبا ما تنجز من خلال صياغة ضوابط واضحة ومحددة بشكل سليم للمراقبة الأمنية وتطبيقها بفاعلية في إطار استخدام مجموعة من القواعد الرقابية كإرشادات .

في ضوء التعريفات السابقة يمكن تحديد أهم أبعاد مفهوم أمن المعلومات على النحو الأتي :

١ ـ تشير عملية صياغة الضوابط إلى ضرورة وجود الإستراتيجية الملائمة لأمن المعلومات في المنظمة ، ويجب أن تتناسب هذه الإستراتيجية مع طبيعة تكنولوجيا المعلومات ومع طبيعة تطبيقاتها في نظم المعلومات وفي شبكات الاتصالات المستخدمة في المنظمة ، كما يفترض تعديل هذه الإستراتيجية بما يتلاءم والتغييرات الحاصلة في هذه التكنولوجيا وفي تطبيقاتها . ويؤكد هنا (Palmer , 2001 : 15) على وجود الحاجة الماسة إلى إطار إستراتيجي عملي وشامل لأمن المعلومات يتصف بهيكلية وصياغة جيدتين وسهلتي الفهم والإدراك من قبل أعضاء المنظمة .

٢ ـ تحديد الجهة المسؤولة عن هذه الصياغة مع ضمان مشاركة جميع الأطراف ذات العلاقة ، ويرى (Parker : 1997 :17) أن الذين يسهمون في صياغة هذه الإستراتيجية ويتحملون مسئوليتها هم المالكون لها والمؤتمنون (القائمون عليها) والجهات التي تقدم الخدمات والمستفيدون منها إلى جانب الجهات المساندة الأخرى وهم المختصون في أمن المعلومات والمدققون ومنفذو القوانين وغيرهم من المساعدين . و لأجل تفعيل هذه المشاركة فإن الضرورة تقتضي جعل مسألة أمن المعلومات جزءا أساسيا من الوصف الوظيفي في المنظمة وأن تكون عاملا حاسما في الأداء والتقويم الوظيفيين وفي الترفيع ومنح المكافآت ، وبخلافه فإنه قد ينظر إلى هذه المسألة على أنها غير ضرورية أو معوقة للإنتاج وستطبق كمسألة جمالية فقط وليست ضرورية .

٣ ـ تتمثل الغايات الأساسية لأمن المعلومات في أية منظمة بالمحافظة على المعلومات من حيث : (Parker, 16-17 : 1997) .

أ ـ الإتاحة والمنفعة : تشير الإتاحة إلى امتلاك القدرة على الوصول إلى

المعلومات وإمكانية استخدامها بصورتها الحالية أينما كانت وكيفما تطلب الأمر ، بينما تشير المنفعة إلى حالة المعلومات التي تعد مفيدة أو متطابقة مع هدف محدد . ويحصل الاختراق في هذين الجانبين عند تخريب المعلومات أو اختلاطها بمعلومات أخرى - على النحو الذي يؤدي إلى تلوثها ـ أو رفضها أو تأخير و إطالة استخدامها أو سوء تفسيرها أو قلبها .

ب ـ تمامية المعلومات وواقعيتها : تتضمن التمامية الصفات الجوهرية الخاصة بكمال المعلومات وتماسكها وارتباطها بمجموعة القيم السائدة في المنظمة ، أما الواقعية فتعني الحالة المعبرة عن الصدق والأصالة في المعلومات وعمق تطابقها مع الحقيقة والواقع . ويحصل الاختراق للمعلومات في هذين الجانبين عند إدخال أو استخدام أو خلق معلومات كاذبة أو تحوير أو استبدال المعلومات أو سوء تفسيرها أو سوء استخدامها أو الفشل في استخدامها .

جـ ـ السرية والحيازة . تشير السرية إلى الصفة الخارجية التي تمنح للمعلومات والتي تنطوي على التكتم والخصوصية وذلك من خلال تحديد الضوابط والتعليمات التي تحدد الجهات المسموح لها بالاطلاع عليها ، أما الحيازة فتعني امتلاك المعلومات والتحكم بها في ظل ظروف معينة . ويحصل الاختراق في السرية في إمكانية الوصول الى المعلومات والكشف عنها أو مراقبتها ، أما اختراق أمن الحيازة فيأتي من الحصول على نسخ من المعلومات أو التخلي عن رقابتها او الائتمان عليها .

٤ ـ تتعدد الجهات التي تخترق أمن المعلومات إلى الحد الذي قد يتعذر معه أحيانا الكشف عن الجهة الحقيقية التي تقف وراء هذا الاختراق ، ويشير الى هذه الحقيقة الباحث (Hill , 1995 : 15) بقوله إن هؤلاء الذين لم يعتادوا على حجم المشكلات الملازمة لامن المعلومات قد لا يمتلكون فكرة واضحة عن تلك الجهات التي تخترق أمن المعلومات ، وهذه الجهات يمكن تعدادها على النحو الآتي :

الأفراد العاملون في مهام الاستلام والتسليم ، المحققون ، الزائرون بهدف الاطلاع ، المستشارون ، عملاء وجواسيس المنافسين ، الأفراد العاملون

حاضرا (المبرمجون ، موظفو البريد ، موظفو أمن المعلومات، البوابون) ، زوجات الأفراد العاملين وأقرباؤهم، الأفراد الساخطون الذين انتهت علاقتهم بالمنظمة وطردوا من العمل .

٥ ـ تتباين الجوانب التي تثير الاهتمام لاختراق أمن المعلومات بتباين طبيعة المعلومات التي تكون عرضة للاختراق ، ففي المستشفيات ينصب الاهتمام على سجلات المرضى ، وفي مجال التسويق تكون إستراتيجيات التسويق هي المهمة ، وتستحوذ الأسرار الصناعية في العمليات الصناعية والإنتاجية على الاهتمام الأكبر . ويرى (Hill , 1995 : 15-16) أن أهم الموارد المنظماتية التي تثير الاهتمام لسرقة المعلومات هي :

قوائم الزبائن ، المعلومات المستنسخة ، مراسلات المدير التنفيذي ، بيانات البحث والتطوير ، مشاريع الموازنة ، البيانات المالية ، الصفقات القانونية ، سجلات الأفراد، الخطط التسويقية .

٦ ـ كما تتعدد أنواع الخروقات لأمن المعلومات (كما سنأتي إلى تفاصيلها في المحور القادم) تبعا لخمسة أسس جوهرية هي :

أ ـ طرق اختراق أمن المعلومات : فالمعلومات يمكن أن تفقد بأربعة طرق رئيسة هي السرقة المتعمدة من قبل وكلاء غير مرخصين يعملون خارج المنظمة ، السرقة أو التخريب من قبل الأفراد العاملين السابقين والحاليين الساخطين على إدارة المنظمة والكشف العرضي من قبل الأفراد العاملين المؤتمنين على استخدام هذه المعلومات في أداء وظائفهم ، وأخيرا تدمير المعلومات من خلال استخدام الفيروسات .

ب ـ مجالات اختراق أمن المعلومات : وتتمثل هذه المجالات بالملفات الورقية ، أجهزة الفاكس ، الهاتف الخلوي ، الثرثرة ، التجسس ، انتحال الصفة وقواعد المعلومات الحاسوبية .

جـ ـ طبيعة عرض المعلومات : وتشمل المعلومات المطبوعة والمسموعة والمقروءة والمسجلة إلكترونيا .

د ـ الطرق المستخدمة في معالجتها ، تحديثها ، استرجاعها ، توصيلها إلى المستفيدين ، استخدامها ، الرقابة عليها .

هـ ـ مصادر المعلومات : وتشمل جميع المصادر التي يمكن أن تولد هذه المعلومات ومنها القوى الكهربائية والماء ، الحاسبات ، الأبنية والفضاءات والتسهيلات الأخرى، شبكات الاتصالات ، الأفراد العاملون ، الأجهزة والمعدات ، السلع والخدمات ، المخازن ، رؤوس الأموال ، السيارات ووسائط النقل .

ـ طرق اختراق أمن المعلومات

على الرغم من اختلاف الباحثين المختصين في مجال أمنية المعلومات بخصوص الطرق التي يمكن من خلالها اختراق أمن المعلومات (عمار ، ١٩٩٠) (منيب ، ١٩٩٠) (قشقوش، ١٩٩٢) (الشوا ، ١٩٩٤) (Ewing 1992) (Hill, 1995) (Tanzer , 1993) (Parker, 1997) لا أنه وكما أسلفنا فإن هناك أربع طرق مهمة يحصل بوساطتها الاختراق لأمن المعلومات وفيما يأتي توضيح لهذه الطرق :

١ ـ التجسس التنافسي (الصناعي) : ويتمثل في الاطلاع غير المخول به على المعلومات ، فالتهديد الخطير الذي يواجه أمن المعلومات هو الدخول (الوصول) غير المرخص إليها من قبل شخص ما ويعرف مثل هؤلاء الأشخاص عادة بمصطلح «المأجورين» (Hackers) وقد أحست منظمات كثيرة بوجودهم ، ويعزى السبب في ظهور مثل هذه الشريحة إلى زيادة حدة المنافسة بين المنظمات ، قصر دورة حياة المنتجات ، انخفاض هامش الربح ، انخفاض ولاء العاملين ، ويأخذ هذا التجسس أشكالا عدة أهمها (Abernathy,1991:77)

أ ـ التقاط المعلومات التي تظهر على الشاشة المرتبطة بالحاسب من خلال الاطلاع عليها وهو ما يصطلح عليه بالالتقاط الذهني .

ب ـ التقاط المعلومات من خلال التصنت المجرد عليها بين الحاسب والمحطات الطرفية بوساطة خطوط تحويلية أو مرسلات صغيرة أو استخدام الهوائيات في حالة البث عبر الأقمار الصناعية .

جـ ـ التقاط المعلومات مباشرة من الخطوط الهاتفية عن طريق وضع مركز تصنت أو مكبرات صوت صغيرة .

د ـ التقاط المعلومات من خلال الإشعاعات الصادرة من الحاسب والأجهزة الملحقة به وفك رموز هذه الإشعاعات لتحويلها إلى اللغة الأصلية .

هـ ـ التفتيش الدقيق في نفايات الشركات بحثا عن المعلومات .

و ـ الدخول إلى النظم الحاسبية للمنظمة باعتماد ذرائع مختلفة مثل الادعاء بأنه باحث أكاديمي أو محلل شركات أو أخصائي معلومات أو مشتر يرغب بكسب ثقة الأفراد العاملين .

٢ ـ سوء استخدام المعلومات . ويشير إلى الحالة التي تسخر وتوظف فيها المعلومات لتحقيق أهداف غير مشروعة أو في مجالات غير مسموح بها لتحقيق مصالحه الشخصية أو مصالح جهات أخرى حتى في الحالات التي يحق للمستفيد في الوصول إلى هذه المعلومات ، ويحصل هذا الاختراق بسبب استغلال أحد الأفراد من قبل الشركات المنافسة من أجل المال أو الرغبة في التجسس أو بسبب طرد الفرد العامل ومن ثم قيامه بعرض معلوماته وكشف أسرار المنظمة وإستراتيجيتها ، وتأخذ هذه الطريقة صيغا عدة هي :

أ ـ سرقة المعلومات المخزونة في ذاكرة الحاسب أو في الأقراص والأشرطة من خلال استنساخها .

ب ـ زرع برنامج فرعي معروف لدى الفرد في البرنامج يتم إخفاؤه بسرية تامة ومهارة لتحقيق أغراض غير مشروعة .

جـ ـ التعديل في برامج الحاسب أثناء تصميم البرنامج أو تنفيذه أو تحديثه وصيانته .

د ـ استخدام الحاسب والمعلومات المخزونة فيه لارتكاب الخروقات وتنفيذها ومتابعة التنفيذ من خلال تصميم برنامج يخصص لهذا الغرض .

هـ ـ إجراء تحويلات وهمية للنقود من خلال مستحقات مصطنعة .

و ـ دفع مستحقات لشركات وهمية وتغذية الحاسب بقوائم دفع وهمية .

ز ـ استبدال رقم حساب بآخر أو إحلال بطاقة بأخرى أو مضاعفة الرواتب .

حـ ـ طبع قوائم حسابات غير حقيقية واستغلال ثقة الزبائن بالحاسب .

٣ـ الإهمال : وهو يمثل الطريقة الأكثر شيوعا لاختراق المعلومات ويعزى السبب في ذلك إلى إهمال الأفراد العاملين وتهاونهم أو ضعف إدراكهم لأهمية الاحتفاظ بسرية المعلومات والعواقب الوخيمة المترتبة لاختراق أمن المعلومات . إلى جانب عدم معرفتهم المعلومات التي تحتاج إلى الحماية ومن يمتلك الدافع إلى سرقة هذه المعلومات من داخل المنظمة وخارجها وكيف يمكن كشفه وإيقافه في الوقت المناسب(Marine,1990: 24) . (Wood&Banks,1993:51)

٤ـ تدمير المعلومات من خلال استخدام الفيروسات التي شغلت المتخصصين في السنوات الأخيرة بسبب اتساع مخاطرها وسهولة انتشارها والأضرار الكبيرة المترتبة عليها والتي تشتمل على مهاجمة البيانات والمعلومات والبرامج وإتلافها وحذفها وتعديلها جذريا من خلال تشويهها وتحريفها وإدخال معلومات غير صحيحة ، حذف الملفات و إعادة تسميتها وتغيير تواريخ الملفات المخزونة ، فضلا عن إيقاف الحاسب عن العمل او إبطاء تشغيله وتقليص السعة التخزينية . وتجدر الإشارة هنا الى صعوبة حصر وتعداد جميع أنواع الفيروسات المستخدمة حاليا في اختراق أمن المعلومات وذلك لتعددها وتنوعها وتزايد انتشارها باطراد فضلا عن تطور صيغها وأشكالها باستمرار .

ـ مجالات اختراق أمن المعلومات

تعد مجالات اختراق أمن المعلومات من أكثر الموضوعات مثارا للجدل والاهتمام من قبل المختصين في نظم المعلومات الإدارية بسبب كونها الأساس في توفير الفرص الملائمة لحدوث الاختراق، من هنا تقتضي الضرورة البحث في بعض الجوانب التفصيلية لهذه المجالات وعلى النحو الآتي : (Parker,1993:10-14)

١ ـ الملفات الورقية . على الرغم من استخدام النظم الحاسوبية إلا أن الملفات الورقية لازالت تستحوذ على النسبة الأكبر من الملفات المستخدمة في أغلب المنظمات، وأهم الفرص المتاحة في هذا المجال هي :

أ- عدم تصنيف الملفات على النحو الذي يمكن معه معرفة مدى سرية المعلومات التي تنطوي عليها ومن ثم حفظ هذه الملفات بشكل منفصل في مواقع أمينة أو في خزانات مقفلة .

ب- الاستعمال الواسع النطاق لأجهزة النسخ واستنساخ ما هو أكثر من النسخ المقررة سواء أكانت المعلومات حساسة أم لا . أو محاولة بعض الأفراد نسخ صور من الوثائق الحساسة والاحتفاظ بها لأنفسهم ، أو نسيان النسخة الأصلية في الجهاز .

جـ- رمي النسخ الرديئة الطبع التي تحتوي على معلومات حساسة دون إتلافها بشكل ملائم.

د- فشل إدارة المنظمة في التعامل مع البحوث الداخلية التي تنشرها المنظمة أو في جرائد أخبارها الداخلية او المجلات أو غيرها من النشرات التي تنشرها والتي قد تضم معلومات حساسة مثل إعلان الشروع بطرح منتج جديد أو نتائج البحوث التسويقية أو تفاصيل عن الأفراد العاملين في المناصب الحساسة .

هـ- ضعف التعامل مع المعلومات التي انتفت الحاجة لها ، إذ يتم في الأغلب التخلص منها من خلال رميها في سلة النفايات وهو أسلوب غير سليم ، فقد تستغل هذه النفايات من قبل الأفراد الذين يتعاملون بها مثل الفراشين أو غيرهم لدوافع شخصية كما قد يندفع من يريد الحصول على المعلومات إلى البحث وبشكل قانوني وبقرار من المحكمة إلى هذه النفايات باعتبارها نفايات مهملة في مركز تجميع النفايات.

و- اللجوء إلى طريقة بيع الأجهزة المنتهية والقديمة (Printouts)من الحواسيب التي قد تضم معلومات سرية يتوجب عدم الاطلاع عليها .

٢- وباء أجهزة الفاكس : لقد ازداد استخدام هذه الأجهزة منذ منتصف الثمانينيات وبشكل كبير بسبب المزايا العديدة التي تتصف بها والمتمثلة بالسرعة والسهولة العاليتين في نقل البيانات والمعلومات إلى جانب انخفاض التكلفة . ومع هذه المزايا فإن هذه الأجهزة تتيح الفرص لاختراق أمن المعلومات ومن أهمها :

أ ـ وضع هذه الأجهزة في مواقع عامة دون أية قيود تمنع الوصول إليها ، بحيث يمكن لأي فرد عابر أن يضع لاقطة ناقلة أو البقاء أمام الجهاز والتقاط ما يسجله وخاصة في حالة ضعف الرقابة على هذه الأجهزة .

ب ـ الفرصة الأخرى تتمثل في الانتفاع من الخطوط الهاتفية التي يمكن أخذ خط منها بكل سهولة ومن ثم الوصول غير المرخص إلى معلوماتها . وكما أشار أحد الخبراء فإن بعض الحكومات تدخل روتينيا إلى كل الاتصالات الأجنبية القادمة وعندما تكتشف وجود بعض المعلومات المفيدة لشركاتها الموردة المحلية فإنها غالبا ما تزود هذه الشركات بهذه المعلومات .

٣ ـ الهاتف النقال : ازداد استخدام هذا الجهاز في السنوات القليلة الماضية بشكل مثير وخاصة من قبل رجال الأعمال لمزاياه الكثيرة المعروفة . إلا أن هذا الاستخدام يحمل في طياته فرصة خطيرة للاختراق من قبل المهتمين بالمعلومات المتدفقة عبر هذه الهواتف(Menkus,1993:60) . إذ إن المعلومات السرية التي تنطوي عليها مكالماتهم ومناقشاتهم عبره وأية معلومات خاصة بهم معرضة لاسترقاق السمع من قبل الأفراد الآخرين . فقد يلتقط أصحاب الهواتف الأخرى المكالمة أو يمكن التقاطها من خلال ما يسمى (Scanners) الخاصة بأجهزة الراديو عند ضبطها على التردد المناسب . يضاف إلى ذلك فإن العديد من أجهزة التلفاز ذات نظام (UHF) المصنوعة قبل عام ١٩٨٢ قادرة على التقاط الترددات المستخدمة في الهواتف النقالة ولا يعرف كم هو عدد أجهزة التلفاز الموجودة تحت الاستخدام حاليا .

٤ ـ الثرثرة : تعد الثرثرة من المجالات المهمة التي تتيح الفرص المناسبة لاختراق أمن المعلومات وبخاصة في حالتين قد لا يأبه بهما الكثير من الأفراد العاملين وهما :

أ ـ المناقشات التي تجري في أوقات الراحة وتناول الطعام والشراب حول أعمال المنظمة والتي قد تكون منفذا لتسريب المعلومات إلى أفراد جالسين بالقرب منهم وينصتون لمناقشاتهم في الوقت الذي تتعذر معرفة هوية هؤلاء الأفراد المنصتين إذ قد يكونون على اتصال مع المنافسين ومن ثم تستغل هذه المعلومات للإضرار بالمنظمة .

ب- إغفال بعض الأفراد لأهمية السكوت وعدم الخوض في موضوعات قد تكشف بعض المعلومات الحساسة عن المنظمة وخاصة من قبل ممثليها في المحافل الرسمية أثناء السفر وحضور المؤتمرات والندوات واللقاءات الصحفية .

٥ - التجسس وانتحال الصفة : ينطوي هذا المجال على فرص عدة متنوعة في أشكالها وفي أساليب استغلالها وهي فرص تتصف بشكل عام بكونها توفر الاطمئنان في نفوس الأفراد العاملين في المنظمة للتحدث وبكل سهولة عن المنظمة وتقديم المعلومات عنها ، ومن نماذج هذه الأساليب نذكر :

أ- القيام بجولات سياحية استطلاعية لمشاهدة المعدات وعمليات الإنتاج .

ب- الادعاء بطلب الوظيفة والرغبة في التعيين في المنظمة ومن ثم ضرورة معرفة الكثير عن المنظمة من خلال المقابلات وإجراءات التعيين .

جـ- الادعاء بأنهم باحثون أكاديميون أو محللون صناعيون أو استشاريون أو طلبة وذلك من أجل الحصول على معلومات محددة عن المنظمة وأنشطتها والأفراد العاملين فيها .

د- الادعاء بأنهم من كوادر الخدمات والتعيين في المنظمة كعمال للصيانة أو فراشين لجمع المعلومات من داخل المنظمة .

٦ - الملفات الإلكترونية : كما هو الحال بالنسبة للملفات الورقية فإن الهدف الأساسي من أمن المعلومات للملفات الإلكترونية يتمثل في كيفية توفير الحماية للمعلومات التي تنطوي عليها هذه الملفات ، وهي المسألة التي باتت الشغل الشاغل للمعنيين بها بسبب الفرص الكثيرة والسهلة التي يتيحها هذا المجال والتي يمكن الإشارة إلى بعض منها وهي :

أ - إساءة استخدام كلمة السر وتشتمل على : (Chebium,1991:32)

- إشراك الأفراد الآخرين في كلمات السر ومن ثم انتقالها إلى جهات أخرى تسعى إلى استغلالها .

- استخدام كلمات السر التي تحمل دلالات معينة في حياتهم اليومية مثل أسماء العائلة أو تواريخ الميلاد .

ـ الاستمرار مدة طويلة دون تغيير لكلمات السر .

ـ الاحتفاظ بنسخة مكتوبة من كلمات السر على المكاتب وبالقرب من أجهزة الحاسب .

ب ـ ترك المحطات الطرفية (Terminals) مفتوحة ، إذ يلغي الحاجة إلى كلمة السر ويفتح المجال للوصول إلى المعلومات بكل سهولة .

جـ ـ ترك أجهزة الحاسب المحمولة (Laptop) مفتوحة في غرف الفنادق أو على مقاعد الطائرات والقطارات ومترو الأنفاق بشكل يسمح لمشاهدة ما يظهر على شاشاتها أو بوضع قرص مرن فيها واستنساخ المعلومات عليه(Menkus,1993:57) .

د ـ ترك حافظات الأقراص مفتوحة وخاصة تلك التي تضم معلومات حساسة الأمر الذي لا يتيح الفرص للاطلاع عليها أو سرقتها فحسب وإنما تعرضها إلى التلف بسبب تلاعب وعبث بعض الأفراد العاملين في محاولة لاستخدامها . ونفس الخطورة تكون قائمة عند غلق هذه الحافظات ولكن مع ترك المفتاح معلقا عليها .

هـ ـ استخدام الدبابيس والمغناطيس والكلابات المعدنية على الأقراص المرنة مما قد يسبب تلفا لجزء كبير من المعلومات التي تتعذر قراءتها أو استرجاعها .

و ـ كما تسبب بقايا الأكل والشرب حول المكان مخاطر مماثلة .

ـ آلية تعزيز أمن المعلومات

يقود العرض السابق لطرق ومجالات الخروقات الأمنية إلى التفكير الجدي بتعزيز أمن المعلومات من خلال اعتماد الآلية الملائمة التي تكفل تحقيق هذا الهدف ، وقد اختلف المتخصصون في هذا المجال حول طبيعة هذه الآلية وأبعادها إلى الحد الذي يتعذر معه الحديث عن أساليب معيارية موحدة يمكن اعتمادها من قبل مختلف المنظمات بغض النظر عن طبيعة أنشطتها وحجمها وأهدافها وفلسفة إداراتها وطبيعة تكنولوجيا المعلومات المعتمدة من قبلها(Shapira,1993:37) . ومع ذلك فإنه يمكن

الاسترشاد بهذه الآراء لبلورة بعض المقترحات التي تشكل الإطار لآلية تعزيز أمن المعلومات في المنظمات المختلفة ، ولأجل تسهيل مهمة تحديد أبعاد هذه الآلية فقد ارتأينا تصنيفها من خلال الاتجاهات الآتية :

الاتجاه الأول : صياغة الإستراتيجية الأمنية .

يسهم وجود الإستراتيجية الملائمة لأمن المعلومات في توفير المناخ السليم لتحقيق الأمن وتعزيزه وذلك من خلال الجوانب آلاتية(Almer, 2001 : 13) :

أ- إعداد الحلول الأمنية التكتيكية في ضوء صلتها بأهداف المنظمة .

ب- تشخيص قيمة موجودات وموارد المنظمة المعلوماتية .

جـ- ترتيب أسبقيات المنظمة من أنشطة وبرامج أمن المعلومات .

د- تشخيص نقاط القوة ونقاط الضعف في البرامج الحالية المعتمدة لأمن المعلومات .

هـ- تسهيل مهمة تطوير وتحسين سياسات المنظمة الحالية لأمن المعلومات .

و- تعزيز الاتصالات بين أعضاء فرق أمن المعلومات والإدارة التنفيذية وتوفر فهما مشتركا لتطبيق الإستراتيجية على نحو فاعل .

ويقترح (الطائي ، ٢٠٠٠ : ٢٩٤-٣٠٨) إطارا عاما لهذه الإستراتيجية وفق الأبعاد آلاتية :

- صياغة الرؤية الإستراتيجية لنظام الحماية الأمنية والتي تحدد الوضع الحالي لنظام الحماية وما يجب أن يكون عليه هذا النظام مستقبلا .

- تحديد القواعد الأساسية لنظام الحماية والتي يمكن الاسترشاد بها وهذه القواعد هي قاعدة قبول الحماية وقاعدة النقاط الحرجة وقاعدة المسؤولية القانونية .

- تحديد أساليب الحماية الأمنية الإدارية والتي تشتمل على حماية مركز الحاسب والتحكم بالدخول إلى هذا المركز وحماية الأقراص والأشرطة والبرامج والتجهيزات والحماية من الحريق .

- تحديد أساليب الحماية الأمنية التشغيلية والتي تضم حماية المدخلات وحماية

عمليات المعالجة وحماية المخرجات وحماية قاعدة المعلومات .

الاتجاه الثاني : التشريع والقانون .

ويقع ضمن اهتمامات وصلاحيات رجال القانون وذلك من خلال إصدار التشريعات والقوانين التي تحد من الخروقات الأمنية على النحو الذي يلحق الضرر بالمنظمات . إذ تعد جريمة سرقة المعلومات جريمة العصر بحق بعد أن انتشرت وتوسعت وتعددت طرقها وفنونها مع التوسع الكبير في استخدام الحاسب وملحقاته في تطبيقات نظم المعلومات الإدارية على النحو الذي أثارت قلق المشرعين القانونيين، ويشير هنا أحد الخبراء في مجال القانون إلى أن سرقة المعلومات أصبحت أسرع الجرائم انتشارا في عصرنا الراهن مع تطور المجتمع وتحوله إلى مجتمع تكنولوجي في أغلب مناحيه، ومما يزيد الأمر تعقيدا أن القانون يمضي متخلفا عن هذه التطورات التكنولوجية بخطوات كبيرة ، فالقانون لا يعامل المعلومات كسلعة ذات قيمة كبيرة فضلا عن أن القانون في الكثير من الدول لا يعاقب على هذا النوع من الجرائم كما لا يتيح الفرصة أمام الجهات القضائية بملاحقة هؤلاء المجرمين قانونيا (الطائي ، ٢٠٠٠ : ٣٠٩) . ولقد كان هذا الموضوع مثار مناقشات حادة اشتركت فيها الوكالات الحكومية القانونية الأمريكية حول التوصل إلى الإجراءات القانونية التي تحد من حالات الخروقات وتسهم في كشف الأدلة التي تساعد السلطات القضائية على إصدار العقوبات الرادعة وتطبيق تلك الإجراءات .

الاتجاه الثالث : الأفراد العاملون في المنظمة .

على الرغم من عدم كمال إجراءات أمن الحاسب والمعتمدة حاضرا من قبل أغلب المنظمات إلا أن هذه الإجراءات فاعلة بما فيه الكفاية في حماية المعلومات المخزونة على الحاسب ، ولكن يبقى الأفراد المستخدمون العامل الأساسي في أمن المعلومات وليس الحاسب ، إلى الحد الذي يمكن القول معه إنه لا قيمة لأي نظام أمني مهما كانت التكنولوجيات المستخدمة فيه متطورة في حالة فشل مستخدمي هذا النظام في اتباع الإجراءات الملائمة لتنفيذه . بناء عليه فإن الالتزام ببرنامج أمني فاعل

للمعلومات يجب أن يبدأ من العاملين في المنظمة وفي مقدمتهم الإدارة العليا نزولا إلى المستويات الأخرى (Richards-Carpenter,1993,:21) . ويعد الوعي بأهمية وخطورة أمن المعلومات الأساس في تحقيق مثل هذا الالتزام إلى جانب إدراك أهمية دورهم في حماية المعلومات ومن ثم معرفة أهمية تحمل مسوؤلية ذلك حتى في مجالات الحياة اليومية الاعتيادية والتعامل مع هذه المعلومات بطريقة مقبولة ، فالإدراك والمعرفة يمثلان نصف المعركة حيث إنه بمجرد أن يصبح الأفراد مدركين لأهمية قيمة المعلومات عندها تصبح مهمة تطبيق الإجراءات الخاصة بالنظام الأمني سهلة وممكنة (Wood & Banks ,1993 :52) . ويجمل (الطائي ، ٢٠٠٠ : ٣٠٠ ـ ٣٠١) أهم هذه الإجراءات بالآتي :

- التحري الدقيق عن الأفراد العاملين الذين سيشغلون مناصب معينة في إدارة وتشغيل وحدة نظام المعلومات الإدارية قبل الإقدام على اختيارهم وتعيينهم وتثبيتهم في وظائفهم .
- فصل المهام عن بعضها البعض وخاصة تلك التي تسهل وتشجع على اختراق أمن المعلومات ، ومنع العاملين من استخدام أكثر من طريقة واحدة لتغذية الحاسب .
- الاهتمام بالأفراد العاملين ورفع روحهم المعنوية من خلال توفير الأجواء الملائمة والاهتمام بمشاكلهم وسماع آرائهم ومقترحاتهم وتعزيز المكافآت الممنوحة لهم .
- الإجراء القانوني الذي يتمثل في وجود مادة قانونية تنص على معاقبة الأفراد الذين يسهلون مهمة اختراق أمن المعلومات في إطار مسئوليتهم القانونية .

الاتجاه الرابع : الإجراءات الصحيحة في التعامل مع الملفات الورقية ومع أجهزة النسخ والفاكس والهاتف النقال والحاسب والمتطفلين . وذلك من خلال تجاوز العيوب والثغرات التي تشكل الفرص السانحة لاختراق أمن المعلومات في هذه المجالات وعلى النحو الآتي :

١ ـ الملفات الورقية . إن أمن المعلومات في الملفات الورقية يمكن تحقيقه بسهولة فيما إذا أدرك الأفراد المتعاملون معها- وخاصة تلك الملفات

المصنفة على أنها سرية ـ مدى الحاجة لأمن المعلومات . وهناك مجموعة من الإجراءات التي يمكن أن تضمن أمن هذه الملفات وهي (Leyzorek 1991 :24 - 27) :

أ ـ منع وصول الأفراد غير المرخصين إلى هذه الملفات والسعي إلى تصنيف الملفات إلى ملفات سرية وغير سرية وحفظ السرية منها في مواقع أمينة أو في خزانات مقفلة .

ب ـ عدم استنساخ أكثر من النسخ المقررة سواء أكانت المعلومات حساسة أم لا مع الحذر الشديد من استرداد النسخ الأصلية بعد الانتهاء من عملية النسخ .

جـ ـ عدم رمي النسخ رديئة الطبع والتي تحتوي على معلومات مهمة في سلة المهملات قبل تمزيقها بشكل مناسب من خلال استخدام مكائن خاصة معدة لهذا الغرض .

د ـ الحذر والانتباه عند اختيار من يطلع على بحوث المنظمة الداخلية ونشراتها وأخبارها الداخلية ، وإذا لم يكن هناك بد من نشر المعلومات فإنها يجب أن تنشر في إطار عام وليس تخصصي .

٢ ـ الفاكس : إن أفضل طريقة للتعامل مع أجهزة الفاكس تتمثل في الإجراءين الآتيين :

أ ـ الانتباه عند إرسال معلومات سرية إلى أجهزة الفاكس ذات الاستخدام العام وتجنب استخدام الفاكس في المراسلات التي تتصف بالسرية ، وإذا كان لابد من ذلك فإنه يجب على إدارات المنظمات اتخاذ المزيد من إجراءات الرقابة لمنع الوصول العام إلى أجهزة الفاكس وذلك بتكليف أفراد مهمتهم مراقبة الجهاز بشكل مستمر أو وضع أجهزة الفاكس في غرف مقفلة لا يدخلها إلا الأفراد المخولون .

ب ـ السعي إلى استخدام أجهزة خاصة لمنع حدوث المراقبة غير المرخصة لأجهزة الفاكس التابعة للمنظمة .

٣ ـ الهاتف النقال : يرى (Menkus , 1990 : 61) أن أفضل إجراء يمكن

اعتماده لتجاوز الخروقات الأمنية في الهاتف النقال هو تجنب مناقشة الأمور الهامة والامتناع عن التحدث بالمعلومات الحساسة التي قد يؤدي تسريبها أو إساءة استخدامها إلى إلحاق الضرر بالمنظمة .

٤ ـ التجسس : يمكن الحد من حالات التجسس أو التقليل من آثارها السلبية من خلال اعتماد الإجراءات آلاتية :

أ ـ عدم السماح بإجراء الجولات السياحية إلا في حالات الضرورة القصوى .

ب ـ حصر الزائرين الغرباء في منطقة محددة معروفة ومراقبتهم عن كثب طيلة الوقت .

جـ ـ تجنب إعطاء الكثير من المعلومات عن المنظمة لطالبي الوظائف .

د ـ تجنب التغافل عن كوادر الخدمات الخارجية مثل شركات التنظيف ومكاتب الصيانة وما شابهها .

هـ ـ تجنب إغفال الأفراد العاملين الساخطين أو الذين أنهيت خدماتهم .

٥ ـ الملفات الإلكترونية : لأجل تحقيق أمنية هذه الملفات ينصح أغلب المختصين باعتماد إجراءين على الأقل ويتم تعزيزهما بإجراءات إضافية أخرى وهما :

أ ـ استخدام كلمة السر بهدف الوصول إلى النظام ابتداء ، ومن ثم بعد الاستخدام ، فعلى الرغم من أن بعض الإجراءات المستندة إلى الحاسب تعطي اهتماما خاصا لكلمات السر إلا انه لا يزال العديد من المستخدمين لا يعيرون الاهتمام والجدية الكافية وقد يعدها البعض غير ملائم كإجراء أمني ، من هنا ولأجل تفعيل هذا الإجراء يجب على المستخدمين الالتزام ببعض القواعد الخاصة باستخدام كلمة السر ومن أهمها عدم إشراك الآخرين فيها حتى ولو كانوا موضع الثقة ، وتجنب وضع كلمات العبور ذات المعنى في الحياة اليومية ، والسعي إلى تغيير كلمة السر بشكل منتظم إلى جانب تجنب الاحتفاظ بنسخ مكتوبة منها على المكاتب بالقرب من الحاسب وأيضا تجنب تقليد كلمة السر على أرقام الهاتف .

ب ـ تدقيق ما تمت من عمليات لتسهيل مهمة كادر أمن المعلومات من متابعة أية تغييرات حصلت على المعلومات وتأشيرة أين ومتى تم إحداث هذه التغييرات .

أما الإجراءات الأمنية الأخرى فتتمثل في :

١ ـ استخدام الطرفيات التي يمكن إقفال لوحة مفاتيحها أو الاحتفاظ بها في غرف مقفلة لمنع الوصول إليها .

٢ ـ استخدام الحاسبات ذات الأقراص الصلبة ممكنة الاستبدال بحيث يمكن رفع القرص الصلب والاحتفاظ به في مكان مقفل وأمين .

٣ ـ تقليص كمية المعلومات الحساسة المخزونة على الحاسب إلى أدنى حد ممكن .

٤ ـ اتخاذ إجراءات التحوط تجاه سرقة الجهاز إما بالاحتفاظ به داخل الأمتعة بشكل يتعذر رؤيته أو حمله بطريقة يتعذر سرقته .

٥ ـ استخدام برامج السرية (Encryption Programs) وهي الخوارزميات التي تمزج وتجانس محتويات مجاميع المعلومات وتناغم الملفات أو تعالج الملفات والبريد الإلكتروني وتغلق الحاسب أمام محاولات خرق سرية المعلومات ، إذ تعمل هذه البرامج باستخدام مفتاح خاص لمجانسة الخصائص في الملف أو الشبكة مما يتيح خليطا من المعلومات غير المفهومة إلا من قبل الأفراد المتلقين المقصودين والمخولين بالاطلاع عليها .

الاتجاه الخامس : مواجهة الفيروسات .

تستخدم المنظمات في الوقت الحاضر العديد من الإجراءات العملية التي تسهم في الكشف عن الفيروسات بسرعة ومعالجتها وتطهير ذاكرة الحاسب والتخلص من الأقراص والأشرطة الملوثة بالفيروس وهذه الإجراءات بحاجة إلى تحسين وتفعيل مستمرين بسبب خطورة هذه الفيروسات وبسبب الأهداف التي يسعى إلى تحقيقها المتعاملون معها ، من هنا فإن الخطوة الأفضل هي الوقاية من الفيروس وممارسة إجراءات الحماية التي تتضمن الآتي :(Roy, Jin & Roy ,1991 :18)

١ ـ إيجاد نسخ إضافية للبرمجيات والملفات المستخدمة والتي قد تتعرض للإصابة بالفيروس .
٢ ـ تأمين مواقع بعيدة لتخزين النسخ الاحتياطية عن مواقع الأجهزة الحالية .
٣ ـ منع استخدام الأقراص والأشرطة من خارج المنظمة وخاصة المجهولة منها إلا بعد التأكد من خلوها من الفيروسات وأيضا التحقق من مصدرها الأصلي .
٤ ـ اعتماد رموز خاصة بالبرمجيات المستخدمة في النظام على النحو الذي يتعذر معه الاستفادة منها حتى في حالة نسخها مع التشديد على تجنب استخدام كلمات سر النظم الشائعة ، إذ إن لبعض الفيروسات قدرة الوصول إلى النظام من خلال المحاولات مع كلمات السر لحين الوصول إلى الكلمة المطلوبة .
٥ ـ مراقبة الحاسب باستمرار للتأكد من عدم وجود فيروس مختبئ مع التأكيد على استخدام مضادات الفيروس .
٦ ـ حصر مسوؤلية أمن أجهزة ومواقع الحاسب وملحقاته بجهة محددة .

الاتجاه السادس : إنشاء وحدات أمن المعلومات .

يرى (Parker , 1997 :15) ضرورة استحداث ثلاث وحدات تنظيمية تتولى مسوؤلية توفير أمن المعلومات وهذه الوحدات هي :

١ ـ وحدة المعايير والسياسة والتي ترفع تقاريرها إلى الإدارة العليا وقد تنجز هذه الوحدة أيضا عمليات تقويم ومراجعة الوضع الأمني للوحدات المنظمية الفرعية وترفع التقارير بشأن الخروقات الأمنية التي يتم الكشف عنها .
٢ ـ وحدات متخصصة «واحدة أو أكثر » تقام في التشكيلات المنظمية الفرعية لغرض تقديم المقترحات بشان التطوير المستمر للإجراءات الرقابية المعتمدة وتشغيلها وصيانتها .
٣ ـ شبكة من الكادر الذي يعمل بدوام جزئي أو كامل وبصفة منسقين أمنيين في كل تشكيل منظمي فرعي وتختص هذه الشبكة برقابة الوضع الأمني داخل هذه التشكيلات وكذلك إيصال المعلومات الأمنية إلى العاملين في مجال المعلومات في تلك التشكيلات المنظمية .

المراجـــع

أولاً: المراجع باللغة العربية

أسامة عبد الله قايد، « الحماية الجنائية للحياة الخاصة وبنوك المعلومات »، دار النهضة العربية، (١٩٩٤).

ماجد عمار، «المسؤولية القانونية الناشئة عن استخدام فيروس الكومبيوتر»، بحث مقدم إلى المؤتمر العلمي لنظم وتكنولوجيا المعلومات، القاهرة، (١٩٩٠).

محمد سامي الشوا، «ثورة المعلومات وانعكاساتها على قانون العقوبات»، دار النهضة العربية، (١٩٩٤).

محمد عبد حسين الطائي، « نظام المعلومات الإدارية»، دار الكتاب للطباعة والنشر، جامعة الموصل، (٢٠٠٠).

هدى قشقوش، «جرائم الحاسب الإلكتروني»، دار النهضة العربية، (١٩٩٢).

ثانياً: المراجع باللغة الأجنبية

Belden Menkus,"Celluar Telephone Use Can be Dangerous ", Modern Office Technology ,35 (August ,1990).

Belden Menkus ,"Laptop Security ", The Internal Auditor ,50 ,(February,1993).

Carolann Marine, "The Spy Who Loves You ", Record Management Quarterly , 24)April1990(.

Baruch Shapira,"Ten Tips to Enhance Data Security " , Journal of Systems Management ,44 ,(June ,1993) .

Charles Cresson Wood &William W. Banks,Jr ," Human Error: An Overlooked But Significant Information Security Ploblem,"Computers & Security,12 ,(February,1993) .

Colin Richards-Carpenter ,"Keeping A system Safe & Secure ",Personnel Management ,(March ,1993) .

David C. Jones ,"Computer Advances Create New Data Theft Exposures", National Under Writer ,97,(June 14,1993) .

Donn B. Parker ,"A comprehensive List Of Threats To Information ", Information System Security,2ii,(Sumer,1993) .

Donn B. Parker,"Information Security In A nutshell ", Information System Security, 6,)Spring1997).

Joe Abernathy, "Former Hackers Offer Services in Computer Security", Houston Texas Chronicle,23,(June, 1991) .

Lance J. Ewing , "Keeping the Lid on Secrets ", Risk Management , 39,)November1992).

Lisa B. Hill," Information Security: An Overview & Resource Guide For Information Managers ",Record Management Quarterly ,29,)Jan1995) .

Malcolm E. Palmer, "Information Security Policy Framework" ,Information System Security ,10,)May-Jun2001).

Marc Tanzer," Keeping Spies Out of Your Company" , Personnel Journal , 72,)May1993) .

Michael Ley Zorek, "A missing Feature in Some Records Management Systems", Records Management Quarterly,(January,1991) .

Patricia Graham Roy ,W.J. Kenny Jih & Ashok Roy,"Computer Viruses :An Overview for Records Managers", Record Management Quarterly, 25,(April,1991) .

Rajn Chebiun,"Computer Crimes: Passwords,Split Duties Safeguard Against Sabotage",Tallahassee Florida Democrat,6,(March,1991).