الجمهورية العربية السورية
وزارة التعليم العالي
المعهد العالي لإدارة الأعمال

HIGHER INSTITUTE OF BUSINESS ADMINISTRATION

تقييم إمكانية الاستثمار في تطبيق نظام إدارة أمن المعلومات في قطاع الخدمات والاتصالات السورية

Evaluating the investment potential of implementing an Information Security Management System in Syrian services and communications sector

مشروع أعد لنيل درجة الماجستير في إدارة الأعمال

الإدارة التنفيذية

(MBA)

إعداد المهندس
عصام الفوال

إشراف الأستاذ الدكتور
طلال عبود

2020/2019

الإهداء:

إلى من يستحقون أسمى آيات الشكر والتقدير،

إلى أساتذتي الذين لا يتوانون عن تقديم كل ما لديهم من جهد ووقت ونصح وتوجية وإرشاد لبناء جيل واعٍ قادر على البحث العلمي وربط العلم بالعمل من خلال الاهتمام المستمر في البحوث.

إلى جميع الأهل والأحبة والزملاء،

إلى كل من ساندنى وأمدنى بالتشجيع،

أهدي هذا الجهد المتواضع.

كلمة شكر:

أتقدم بخالص الشكر والامتنان إلى استاذي القدير الأستاذ الدكتور طلال عبود على ما بذله من جهد متواصل، وما قدمه من توجيهات وإرشادات وما أبداه من صبر وتفهم كبيرين في سبيل إنجاز هذا العمل،

فله مني عظيم الشكر والإمتنان.

وأوجه شكري وتقديري إلى أساتذتي في المعهد العالي لإدارة الإعمال على الجهود الكبيرة وطريقة إيصال المعلومات التي كان لها عظيم الأثر في وصول البحث إلى هذه الصورة.

كما وأتقدم بجزيل الشكر والعرفان لكل من ساهم وساعد في إنجاز هذا البحث من جميع الأهل والأصدقاء.

ولشركة MTN سوريا إدارةً وموظفين.

سائلاً المولى عز وجل أن يجزي الجميع عني خير جزاء.

عصام الفوال

ملخص البحث:

هدف البحث هو تقييم إمكانية الاستثمار في تطبيق إدارة أمن المعلومات في قطاع الخدمات والاتصالات السورية حيث يعد وضع نظام إدارة أمن المعلومات وتطبيقها من الأولويات في الوقت الحاضر، وذلك كون هذا القطاع يعتمد بشكل أساسي على الحواسيب وتقانة المعلومات في تسيير أعمال المنشأة داخلياً وتقديم خدمات للمشتركين بميثاقية عالية.

إن إدراة أمن المعلومات في قطاع الخدمات والاتصالات السورية تتعرض للعديد من المخاطر والتهديدات وذلك لاعتمادها على الانترنت في توفير خدماتها. من جهة أخرى تتجلى الصعوبة في عدم القدرة على مواكبة التدابير الأمنية المضادة للاختراقات والتهديدات من خلال سرعة تطور الأساليب الحديثة المستخدمة في عمليات الاعتداءات على أمن المعلومات، وأيضاً ضعف التشريعات الموجودة على أرض الواقع سواء على المستوى الوطني أو الدولي مع وجود بطء ملحوظ في مدى كفاية التشريعات الموجودة للحد من عمليات التعدي على أمن المعلومات.

اختتم البحث بعدة توصيات عدة أهمها تشكيل فريق عمل يتبنى مستلزمات تطبيق إدارة نظام أمن المعلومات ويعمل على تلبية جميع متطلباتها ودعم استثمارها، ويقوم بالتركيز على دور العامل البشري كأحد أهم مهددات أمن المعلومات. بلإضافة إلى الدور الجوهري الذي يمكن أن يقوم به للحد من الهجمات والاعتداءات من خلال تدريبه المستمر لمواكبة التطورات في هذا المجال.

الكلمات المفتاحية: أمن المعلومات، إدارة أمن المعلومات، المعايير الدولية لأمن المعلومات، تشريعات أمن المعلومات.

Abstract:

The development of technology in the telecommunication and information technology fields plays an important part in the spread of information via internet. Attacks and risks are vulnerable to such environment where users need to be warned against these risks so to protect and save their information.

The aim of this research is to evaluate the investment of Information Security Management System for Telecommunication and Services sectors in Syria, where implementation of Information Security Management System is a priority, due to the sector's reliance on computers and Information Technology to run business and provide high reliability services to their subscribers.

The information security department in the Syrian services and communications sector is exposed to many risks and threats due to its reliance on the Internet in providing its services. On the other hand, the difficulty is manifested in the inability to cope with the security measures against breaches and threats through the rapid development of modern methods used in attacks on information security, and also the weakness of existing legislation on the ground, whether at the national or international level, with a marked slowdown in the adequacy of existing legislation to reduce information security infringement operations.

The research concluded with several recommendations, the most important of which is the formation of a working group that adopts requirements for implementing Information Security Management System and works to meet all of its requirements and support its investment, and focuses on the role of the human factor as one of the most important threats of Information Security and at the same time the essential role that it can play to reduce attacks and attacks through continuous training to keep abreast of developments in this field.

Keywords: Information Security, Information Security Management, International Standards for Information Security, Information security legislation .

الفهرس:

الفصل الأول

الإطار العام للبحث

1.1 مقدمة عامة:

إن العصر الذي نعيش فيه أصبح عصرا معلوماتياً بكل ما تحمله هذه الكلمة من معنى في ظل الثورة التكنولوجية الهائلة التي طرأت على المجتمع الدولي بصفة عامة والمجتمع السوري بصفة خاصة، فلقد أصبحت المعلومات هي الركيزة الأساسية التي يُعتمد عليها في كل مناحي الحياة ، وذلك في ظل التقنيات الحديثة ووسائلها المتعددة التي أُخترعت لتسهل أمور الحياة على الإنسان حتى أنها أصبحت تقوم ببعض وظائفه في العديد من المجالات ومن هنا تظهر الحاجة إلى وجود منهجية لبناء نظام إداري لأمن المعلومات يوفر الحماية المرجوّة للمعلومات على جميع مستوياتها وبجميع طرق حفظها أو تناقلها.

ونتيجة لانتشار شبكة الإنترنت فقد أشارت العديد من الدراسات الحديثة الى أن نسبة مستخدمي الإنترنت تتزايد باستمرار حيث وصل عدد مستخدمي الإنترنت على مستوى العالم في إحصاء 20/10/2020 إلى 4.66 مليار مستخدم (1) ، وعلى مستوى الشرق الأوسط بلغ العدد الكلي لمستخدمي الإنترنت إلى 183 مليون مستخدم وتحتل ايران المرتبة الأولى بعدد 58 مليون مستخدم للإنترنت (2). أما سوريا فبلغ عدد مستخدمي الإنترنت إلى 8.11 مليون مشترك في يناير 2020 مقارنة إلى 5.62 مليون مشترك في يناير 2017 (3).

ومع تزايد أعداد مستخدمي خدمات الإنترنت تتزايد الاستخدامات وبالتالي تتبادل المعلومات والبيانات بشتى أنواعها على مستوى العالم وتتنوع معها أهمية هذه المعلومات ودرجة سريتها وقيمتها الاقتصادية والمعنوية بين الدول والهيئات أو المؤسسات وكذلك الأفراد.

ومع توسع استخدام خدمات الإنترنت عالمياً بصورة عامة وانتشار استخدامه في سورية بصورة خاصة و ظهور التجارة الإلكترونية والحكومة الإلكترونية والإعتماد على خدمات الإنترنت في نواحي كثيرة ظهر الجانب السلبي لاستخدام الإنترنت وذلك بظهور أنماط جديدة من الجرائم المستحدثة على هذه الخدمة وهو ما يطلق عليه اسم الجرائم المعلوماتية وما تشمله من أعمال القرصنة والتجسس وانتهاك خصوصيات الغير وجرائم سرقة المعلومات.

لذلك كانت هناك حاجة ماسة إلى تعاون دولي للحد من تلك الجرائم الإلكترونية وحماية أمن المعلومات عن طريق تبادل الخبرات والتعاون على إيجاد وسائل قانونية وتقنية لمواجهة الأخطار التي تهدد أمن المعلومات مع الأخذ في عين الاعتبار الطبيعة المختلفة لبلدان العالم، واللغات الموجودة على شبكات الإنترنت.

2.1 مشكلة البحث:

بدأ التركيز على شبكات الإنترنت كتهديد أمني جديد بفعل الأحداث الدولية التي ظهرت نتيجة الانتهاكات التي تتم عبر خدمات الإنترنت وأبرزها أحداث 11 سبتمبر 2001 في الولايات المتحدة الأمريكية ثم في عام 2010 حين تم الهجوم الإلكتروني على برنامج إيران النووي عن طريق فيروس يسمى (ستاكسنت) ليمثل نقلة هامة بالتطور في مجال الأسلحة الإلكترونية، بالإضافة إلى الدور السياسي الذي لعبته مواقع التواصل الاجتماعي فيما يسمى بثورات الربيع العربي في بداية عام 2011 (4) ، بالإضافة إلى ما أعلنته شركة ياهوو Yahoo الشهيرة في عام 2016 إلى أن أكثر من بليون حساب على سيرفراتها جرت عليه عمليات قرصنة وسرقة بيانات للمستخدمين من أسماء وأرقام هواتف لشخصيات عامة وعالمية (5) أدت هذه الجرائم إلى خسائر مالية فادحة يتكبدها الإقتصاد العالمي سنويا بحسب تقرير أصدره مركز الدراسات الإستراتيجية بواشنطن بالتعاون مع شركة مكافي MacAfee لبرامج الأمن المعلوماتي لعام 2018 ، أن الإقتصاد العالمي يتكلف نحو 600 مليار دولار خسائر سنويا أي بما يعادل نحو 1 % من الدخل الإجمالي العالمي بسبب جرائم الإنترنت، مقارنة بحجم الخسائر لعام 2014 المقدرة بحوالي 500 مليار دولار أي بارتفاع وصلت نسبته إلى 0.8% (6).

أشار جرانت جروس (Grant Gross) في التعليق على التقرير السابق أنه بجانب الخسائر الاقتصادية فإنه هناك ما يقدر بنحو 80 مليون من عمليات المسح الإلكتروني للبحث عن الثغرات الموجودة في أجهزة مستخدمي شبكة الإنترنت يوميا، بالإضافة إلى 780 ألف عملية سرقة للحسابات الشخصية (7).

لذلك فقد تجسدت مشكلة الدراسة في رصد المخاطر التي تحيط بأمن المعلومات الرقمية والتدابير الأمنية التي يجب توافرها وما مدى إمكانية الاستثمار في تطبيق نظام إدارة أمن المعلومات في قطاع الخدمات والاتصالات السورية.

3.1 أهمية البحث:

تبرز أهمية البحث في تطبيق نظام إدارة أمن المعلومات بشكل خاص في أن أي معلومة قد تحمل اكتشاف جديد يفيد البشرية في مجال ما ، بالإضافة إلى أن أي معلومة أخرى تتعلق بالاقتصاد قد تكون سببا في إفلاس دول اقتصاديا وأخرى قد تساعد في بناء اقتصادها ، لذا فإن أهمية المعلومة تظهر في

ابتكارها وإحسان استخدامها ، وإذا ما أردنا تحديد الأهمية المادية للمعلومة نجد أن علماء أمن المعلومات انقسموا إلى اتجاهين لتحديد أهميتها (8):

الاتجاه التقليدي: الاتجاه الذي لا يرى في المعلومات أي قيمة مادية بل أنها ذات طبيعة معنوية لا تندرج تحت القيم المحمية ، إلا إذا كانت تنتمي إلى المصنفات الأدبية والفنية أو الصناعية.

الاتجاه الحديث: يرى أن للمعلومات قيمة مالية أشبه بالسلعة ، فهي نتاج ذهني ولكي تكون صالحة للتملك لا بد وأن يحوز مالكها على العناصر المكونة لها بطريقة شرعية في قالب يصلح للاطلاع عليها بغض النظر عن الوسيط الذي يتضمنها.

من هنا كان الاهتمام بهذا البحث لمعرفة الضوابط التي تحول دون انتهاك قيمة المعلومات والتدابير الأمنية المتوافرة لحمايتها وضمان وصولها بطريقة شرعية.

4.1 أهداف البحث:

في ضوء مشكلة وأهمية البحث ، فإن الباحث يسعى إلى تحقيق عدد من الأهداف التي يمكن إيجازها في النقاط التالية:

1. التعرف على مفهوم أمن المعلومات وعناصره.
2. التعرف على المخاطر التي تهدد أمن المعلومات.
3. التعرف على أساليب مواجهة الاعتداءات التي تواجه أمن المعلومات.
4. التعرف على متطلبات ومضمون نظام إدارة أمن المعلومات.
6. التعرف على أهم المعايير الدولية الخاصة بحماية أمن المعلومات.
7. التركيز على العامل البشري كأحد أهم مهددات أمن المعلومات.
8. تقييم إمكانية الاستثمار في تطبيق إدارة أمن المعلومات.

5.1 منهجية البحث:

اعتمدت الدراسة على على المنهج الوصفي التحليلي من خلال الرجوع الى المصادر ذات العلاقة ، وتحليل بياناتها وإجراء المقارنات اللازمة للخروج بنتائج حقيقية.

6.1 مصطلحات البحث:

1.6.1 أمن المعلومات Information Security:

هو العلم الذي يعُنى بحماية المعلومات من المخاطر التي قد تتعرّض لها. ويمكن تعريف أمن المعلومات بشكل مختصر بأنه: حمايــة المعلومات من الوصول غير المسموح به (9) ، ويكـون ذلـك من أجل ضمانة وسلامة المعلومات ، في هـذا السـياق نجـد أن مصـطلح أمـن المعلومـات هـو مصطلح عام يمكن أن ينطبق على أي شكل مـن أشـكال المعلومـات سـواء كانـت تقليديـة أو رقمية.

2.6.1 التشريعات Legislations:

هي مجموعة القواعد المكتوبة التي تنظم العلاقة القائمة بين الأطراف المعنية والداخلـة فيـه. ولـهذه القواعد القوة الجبرية اللازمة للتنفيذ والتقيـد بهـا ، والعقـاب في حالـة المخالفـة ، ولـكي تكون القواعد تشريعا فلابد وأن تكون مكتوبة استنادا إلى القاعدة التشريعية التي تقول بأنـه لا عقوبة إلا بنص (10).

3.6.1 المحتوى الرقمي Digital Content:

عبارة عن المواقع الإلكترونيـة المكتوبـة (المبنيـة والمرفوعـة) بإحـدى لغـات التكويـد الخاصـة بتحويل النص التناظري إلى نص رقمـي (11) ، والكيانـات الرقميـة التـي تعـد شـكل جديـد مـن أشكال أوعية المعلومات الرقمية ، تحتوي على ملف رقمي واحد أو أكثر من ملف من أشـكال الملفات الرقمية (12).

4.6.1 المصنفات الرقمية Digital Works:

هي الشكل الرقمي لمصنفات موجودة ومعدة سلفا دون تغيير أو تعديل في النسـخة الأصـلية للمصنف سابق الوجود ، كأن يـتم نقـل الـنص المكتـوب (مصـنف أدبي) أو الصـوت (مصـنف سمعي) ، أو الصوت والصورة معا (مصنف سمعي بصري) من الوسـيط التقليـدي الـذي كـان عليه إلى وسيط تقني رقمي متطور كالأقراص المدمجـة CD-ROM أو الأسـطوانات المدمجـة الرقمية DVD وهي الشكل الرقمي منذ البـدء لأي مصـنف ، بحيـث يكـون التثبيـت المـادي الأول للمصنف وعمل نسخ منه تم على وسط تقني متطور (13).

7.1 الدراسات السابقة:

1.7.1 المقدمة:

اهتمت العديد من الدراسات العربية والأجنبية بموضوع أمن المعلومات في بيئة الإنترنت والتشريعات المختصة بحمايته باعتباره موضوع ذا طبيعة خاصة جديرة بالاهتمام والبحث ، ومن أهم الدراسات التي تناولت هذا الموضوع ما يلي:

2.7.1 الدراسات العربية :

هدفت دراسة **إيهاب نور الدين** في عام 2018 (14) ، إلى قياس وتفسير أثر الإسناد الخارجي لمهام تكنولوجيا المعلومات على أمن وسرية المعلومات وذلك من خلال تحقيق عدة أهداف فرعية كان أهمها القيام بدراسة تحليلية لقياس وتفسير أثر هذا الأسناد والتعرف على مزاياه وعيوبه من خلال استخدام المنهج الاستقرائي عن طريق تصميم قائمة استقصاء وتوزيعها على المتخصصين في مجال تكنولوجيا المعلومات. واقتصرت الدراسة على بيان مدى تأثير الإسناد الخارجي لمهام تكنولوجيا المعلومات دون التطرق إلى دور هذا الإسناد على تقديم خدمات استشارية أخرى ، عن طريق عينه من داخل حدود البيئة المصرية تشتمل على مجموعتين: الأولى مكونة من المهندسين في مجال تكنولوجيا المعلومات ومجموعة أخرى خاصة بالمهندسين الذين يقدمون خدمة الإسناد الخارجي.

وخلصت الدراسة من خلال تحليل نتائج الاستقصاء على العينة المذكورة إلى أنه توجد علاقة ارتباط بين الإسناد الخارجي لمهام تكنولوجيا المعلومات وأمن وسرية المعلومات.

أما دراسة **عبد الوهاب ملياني** عام 2017 (15) ، سعت إلى تحليل ظاهرة الجرائم الواقعة على النظام المعلوماتي باعتباره البيئة التي تتم فيها كل الأعمال الخاصة بالمعلومات الإلكترونية من خلال القيام بدراسة تأصيلية لتلك الجرائم باعتبارها سببا أصيلا لصدور التشريعات الخاصة بحماية أمنها ، متبعا في ذلك المنهج الوصفي التاريخي والمنهج المقارن بالإضافة إلى المنهج الاستدلالي.

وقام الباحث بدراسة المعالجة التشريعية لأمن المعلومات الرقمية وتحديد طبيعة الجرائم التي ترتكب عليها وتحديد مدى استقلاليتها عن غيرها من الجرائم وما ينعكس بذلك على النصوص التشريعية في المجال الجنائي مع الوقوف على مدى توفيق المشرع في وضع استراتيجية لمواجهة تلك الجرائم على الجانبين الموضوعي والإجرائي.

توصلت الدراسة إلى العديد من النتائج أهمها ضرورة أن تتضمن مقومات استراتيجيات مواجهة جرائم الاعتداء ومحاربتها على الجوانب الجنائية الموضوعية والإجرائية تتماشى وطبيعة البيئة الرقمية حيث إنها لا تكفي وحدها لمواجهة الجرائم محل الدراسة ولابد من إيجاد

استراتيجيات مكملة على المستوى الفني والتقني والقضائي وضرورة التعاون القضائي الدولي في مسألة تسليم المجرمين.

سعى الباحث **معاذ أحمد عبد الرازق** في عام 2016 (16) ، إلى التعرف على المهددات التي تتعرض لها المعلومات ومحاولة التوصل إلى مقترحات تساهم في التصدي لها والأنظمة الكفيلة بالحد من تلك الظواهر السلبية بالإضافة إلى التعرف على وسائل حماية المعلومات والبيانات.

اتبع الباحث في تحقيق أهدافه من الدراسة المنهج الوصفي التحليلي وعمل مسح للمركز القومي للمعلومات عن طريق الاستبانة وإجراء المقابلات الشخصية والزيارات الميدانية والملاحظات ونتيجة لذلك توصل الباحث في نهاية الدراسة إلى عدد من النتائج أهمها استخدام أنظمة الحماية والمعايير العالمية لأمن المعلومات هي من أنسب الطرق التي يمكن اتباعها للحد من المخاطر التي تهدد أمن المعلومات، أوصت الدراسة بإنشاء وحدة تهتم بأمن المعلومات في كافة مرافق الدولة وضرورة التوعية وعمل تدريبات دورية للمستخدمين على أحدث الأنظمة والتقنيات المستخدمة في مجالات أمن المعلومات.

أما الباحثة **منال بنت حمدان** في عام 2016 (17) ، قد سعت إلى الكشف عن ممارسات أمن المعلومات المتبعة في المكتبة الرئيسية بجامعة السلطان قابوس للوقوف على مدى توافقها مع المعيار الدولي لأمن المعلومات (ISO/IEC 27002) من أجل معرفة نقاط الضعف والقوة التي قد تؤدي إلى تحسين الممارسات الأمنية بالمكتبة الرئيسية بدولة عمان.

اعتمدت الباحثة في دراستها على منهج دراسة الحالة من خلال استخدام عدة أساليب مثل الزيارات الميدانية والمقابلات الشخصية واستخدام أداة لجمع البيانات لفئة العاملين في الأقسام المسؤولة عن ممارسات أمن المعلومات بجامعة السلطان قابوس استهدفت منهم رؤساء الأقسام ومن ينوب عنهم في كل قسم.

وخلصت الدراسة إلى أن أغلب ممارسات أمن المعلومات بالمكتبة تتوافق مع ممارسات المعيار الدولي لأمن المعلومات (ISO/IEC 27002)، ونتيجة لهذه النتيجة فقد وضعت الباحثة عدة توصيات أهمها ضرورة تدريب وتوعية المستفيدين من المكتبات وتطوير سياسات أمن المعلومات بالمكتبات مستندة على المعيار الدولي لأمن المعلومات، مع ضرورة توفير التدابير المادية اللازمة مثل النسخ الاحتياطي وتوفير مصادر بديلة للطاقة.

3.7.1 الدراسات الأجنبية:

هدفت الباحثة **Venessa Burton** في دراستها عام 2018 (18) ، إلى التعرف على التحديات التي يواجها مدراء أمن المعلومات في بيئة الإنترنت المتخصصين في حماية المعلومات التجارية ومحاولة معرفة مدى كفاية حماية الملكية الفكرية من الانتهاكات التي يرتكبها مجرمي الإنترنت ، وتأثير ذلك على مسؤولي الأمن المعلوماتي ، وقامت الباحثة بدراسة قدرة هؤلاء المديرين على تطبيق قوانين حماية الملكية الفكرية على حماية أصول منشآت الأمن المعلوماتي ودراسة المخاطر التي تتعرض لها وذلك من خلال التعرف على الاستراتيجيات التي يتم استخدامها في تطبيق الحماية القانونية وآلية حمايتها ضد الإرهاب الإلكتروني.

استندت الباحثة في تحقيق أهدافها على البحث النوعي من خلال إجراء المقابلة الشخصية لعشرة مديرين من المتخصصين في مجال أمن المعلومات ولهم سنوات خبره في هذا المجال لا تقل عن 15 سنة من التعامل مع الشبكات والبنية التحتية لأمن المعلومات وفي مدينة واشنطن بالولايات المتحدة الأمريكية.

وخلصت الدراسة إلى أن القوانين المتبعة في حماية أمن المعلومات في بيئة الإنترنت تبطئ من عمل المديرين في أمن المعلومات نظرا لعدم مواكبتها للجرائم الحديثة لذلك فهي ليست فعاله بالشكل الكافي، كما أن القوانين تفتقر إلى آلية واضحة للتطبيق نظرا لتشعب وتنوع الجرائم الإلكترونية، لذلك أوصت الباحثة أنه لابد من توحيد القوانين التي تتصدى لهذه الجرائم بالإضافة إلى وضع سياسة استراتيجيات لأمن المعلومات تكون كافية لتنظيم ممارسات الأمن والحماية.

تناولت دراسة **Ibrahim Ghafir** في عام 2018 (19) ، الجانب المعرفي لدى العاملين والمستخدمين لأمن المعلومات في بيئة الإنترنت على وجه الخصوص ، وما يترتب على الوعي الأمني لديهم من مخاطر تتمثل في إمكانية حدوث جرائم الاحتيال والجرائم التي تتم باستخدام الهندسة الاجتماعية عندما يتم تسجيل دخول المستخدم للوصول إلى المواقع الإلكترونية ، والتدابير التي يمكن تنفيذها لحماية البيانات الشخصية والتجارية من الخسارة المحتملة.

وتوصلت الدراسة إلى تطوير برنامج تدريبي لزيادة الوعي الأمني لمساعدة الشركات والعاملين فيها لمعرفة المخاطر الإلكترونية المحتملة لحماية أنفسهم والمكان الذي يعملون فيه ، ويوفر أيضا البرنامج التدريبي التحديثات المستمرة لأهم الجرائم التي تتم في البيئة الرقمية مع التدريب على التدابير الأمنية للتصدي لهذه الجرائم ، مع إمكانية إصدار شهادات عند النجاح في جميع الوحدات المكونة للبرنامج التدريبي.

أما الباحث **Michele Zoerb** فقد قام بدراسة عام 2017 (20) ، تهدف إلى وضع إطـار عام لمفهوم أمن المعلومات في بيئة الإنترنت نظـرا لملاحظتـه وجـود تفـاوت بـين مفهـوم أمـن المعلومات وسياسات أمن المعلومات والضـوابط الداخليـة لمـنظمات أمـن المعلومـات ، وهـذا التفاوت في التعريف والمفهوم يخلق فجوه في العديد من المنظمات التي تتعامـل مـع بـرامج الأمن المعلوماتي ، ويعرضها لكثير من المخاطر وخلق نقاط الضعف ، وتسعى هذه الدراسـة إلى بناء فهم واضح للقضاء على التفاوت في تعاريف برامج أمن المعلومات واقتراح تعريف واطار عام يمكن استخدامه في المعايير الخاصة بصناعة وتطوير برامج أمن المعلومات.

اتبع الباحث أسلوب قائمة المراجعة للوصل إلى الهدف مـن الدراسـة وتوصـل إلى أن عناصر أي برنـامج أمن معلومات لمنظمة ما يشتمل عـلى ثلاثـة عنـاصر أساسية وهـي : إطـار الامتثال الإداري ، البيئة التقنية وأدواتها ، والسياسات والمعايير المتبعة داخل المنظمة ، فضلا عن أنه وضع تعريفا لبرنامج أمن المعلومات بأنه برنامج يهدف إلى حماية أصول المنظمة والأعمال الإلكترونية الموجودة لذلك فهو برنامج يركـز عـلى الـنظم المعمـول بهـا والمخـزون المعلومـاتي نفسه لأن الهدف الأساسي من البرنـامج هو حمايـة مقومـات المنظمـة والعمـل عـلى اسـتدامة الأعمال نفسها لأن العمليات التي تجرى داخل المنظمة والمستفيدين منهـا والعـاملين يمثلـون مجموعة العملاء الذين يخدمهم برنـامج أمن المعلومات.

هدفت دراسة الباحث **Rolf H. Weber** التي قـام بهـا عـام 2016 (21) إلى التعـرف على التدابير التشريعية التي تقوم على حمايـة أمـن المعلومـات في بيئـة الإنترنـت مـن خـلال إنترنت الأشياء ويناقش اللوائح الدولية المطبقة في هذا المجال مـع محاولـة الخروج بحلـول بديلة لمعالجة القضايا الأمنية الناشئة عن المخاطر التي تهدد أمن المعلومات.

وفي هذا الصدد تناول الباحث اتفاقية بودابيست لمكافحة جرائم تقنيات المعلومات المبرمة في عام 2001 ودخلت حيـز التنفيـذ عـام 2004 ، وأيضـا تنـاول تشريـع الإتحـاد الأوربي بشأن مكافحة جرائم أمن المعلومات في بيئة الإنترنت عام 2015 ، للوقوف على أهم النصـوص القانونية والأفعال التي تعتبر بمثابة جرائم إلكترونية من وجهة نظر المشرع.

وخلصـت الدراسـة إلى أن سرعـة التغيـير والتطـور التكنولـوجي وتطـور أسـاليب المهاجمين يتطلب ضرورة وجود أساليب جديدة لحماية المعلومات في بيئة الإنترنت إذ أن كل جهاز حاسب آلي متصل بالإنترنت يقع تحت تهديد هذه الجرائم مـع وجـود ثغـرات عديـدة تسهل هذه الهجمات ، ويتطلب

ذلك تعزيز الأمن المعلوماتي في بيئة الإنترنت بشكل عاجل وأيضا المرونة المبتكرة بما يكفي للتصدي لهذه الهجمات ، وأشاد الباحث بجهود الإتحاد الأوروبي في التدابير التشريعية وإن كانت على الأقل على الورق كما ذكر الباحث إلى أنها تلعب دورا هاما في الممارسة العملية لتعزيز أمن المعلومات بشكل عام.

في ضوء الدراسات العربية والأجنبية السابق ذكرها يمكن تلخيص النقاط التالية:

1. الإسناد الخارجي لضمان حماية أمن المعلومات.
2. توافق معايير أمن المعلومات بنسب متفاوتة في مكتبة السلطان قابوس.
3. تطبيق التدابير المضادة لحماية أمن المعلومات في الشركات الصغيرة المتواجدة في بيئة الانترنت.
4. الاهتمام بدور العامل البشري في مجال أمن المعلومات كأحد أهم مهددات أمن المعلومات الرقمية.
5. ضبط مصطلحات أمن المعلومات للتوافق مع معايير الأمن المتبع داخل منشآت أمن المعلومات.
6. تطبيق معايير أمن المعلومات في مجال أمن انترنت الأشياء من خلال القوانين الأوروبية الخاصة بمكافحة جرائم تقنيات المعلومات.

الفصل الثاني

الإطار النظري للبحث

1.2 مقدمة عامة:

1.1.2 عناصر أمن المعلومات:

يعتمد أمن المعلومات على ثلاثة عناصر أساسية لابد أن يتم توافرها في المعلومات التي تستوجب الحماية، وهي:

أ. السرية **Confidentiality**
ب. سلامة المعلومات وتكاملها **Integrity**
ت. وتوافر المعلومات **Availability**

تعرف باسم مثلث CIA أو CIA Triangle ، ويمكن تناولها على النحو التالي (22):

1- السرية Confidentiality: وهي القدرة على الحفاظ على سرية المعلومات عن طريق منع الدخول غير المصرح للمعلومات سواء كانت محفوظة على وسيط مادي أو يتم إرسالها عبر وسائل الاتصالات، والتأكد عدم الإفصاح عنها بالإضافة إلى عدم السماح بالاطلاع عليها إلا من خلال الأشخاص المصرح لهم بذلك.

2- سلامة المعلومات وتكامل المحتوى Integrity: التأكد من المحافظة على محتوى المعلومات وسلامته من العبث أو التعديل أو الإفساد وذلك عن طريق منع الوصول إلى هذا المحتوى عن طريق التدخل غير المشروع.

3- توافر المعلومات وإتاحتها Availability: ضمان توافر المعلومات والقدرة على تقديمها وإتاحتها في الوقت المناسب من خلال الأشخاص المصرح لهم بذلك، والتأكد من أن هؤلاء الأشخاص لن يتم منعهم من استخدام المعلومات أو الدخول إليها.

يمكن توضيح عناصر أمن المعلومات المعروفة باسم مثلث CIA وهي أحد أهم العناصر الأساسية لأي نظام معلوماتي وفقا للمعايير الدولية المختصة بسياسات أمن وإدارة المعلومات، من خلال الشكل التالي:

شكل (1)

عناصر أمن المعلومات مثلث CIA

2.1.2 المخاطر التي تهدد أمن المعلومات:

بالرغم من أهمية أمن المعلومات وأهمية محتوياتها لدى مؤسسات المعلومات إلا أنها لا زالت تتعرض للكثير من المخاطر الأمنية التي تتعرض لها وتناولت العديد من الدراسات أنواع المخاطر التي تهدد أمن المعلومات وتعددت معها تصنيفات هذه المخاطر، فقد تكون ناتجة عن تهديدات طبيعية مثل الكوارث والزلازل أو من خلال العاملين أو مستخدمين النظام أنفسهم بمؤسسات المعلومات سواء كانت بنية القصد أو من غير قصد.

فقد أشارت الدراسات أن 80 % من الهجمات الناجحة على المعلومات تنشأ عن عوامل التهديد الخارجي ولكن تكون من جانب العاملين على النظام وذلك عن طريق ما يسمى بالاصطياد Phishing والخداع لأحد المسؤولين عن نظام أمن المعلومات من الداخل أو عن طريق تحميل برامج ضارة مما يتيح للمهاجمين الوصول إلى النظام (23).

من خلال الاطلاع على أدبيات الموضوع التي تتناول مخاطر أمن المعلومات والتصنيفات المختلفة لها، يمكن وضع تصنيف للمخاطر التي يتعرض لها أمن المعلومات إلى ثلاثة تصنيفات مختلفة وهي :مخاطر مادية (فيزيائية) ومخاطر إلكترونية معلوماتية، ومخاطر داخلية، وفيما يلي نتناول تصنيفات مخاطر أمن المعلومات على النحو التالي:

1- المخاطر المادية Physical Threats:

هي المخاطر الناجمة عن الوصول المادي لمكونات نظام أمن المعلومات أو تلف في الموارد المتاحة لأمن المعلومات وتشمل الضرر الذي تسببه الطبيعة من كوارث طبيعية محتملة على المنشأة المعلوماتية أو السرقة أو الحريق وغيره من الحوادث الطارئة، مما يتسبب في ضرر دائم للبيانات التي تحويها هذه المنشأة، ويمكن تقسيم المخاطر المادية إلى قسمين رئيسيين:

أ- المخاطر الطبيعية Natural Threats:

تتكون الأخطار الطبيعية من الكوارث الطبيعية مثل الفيضانات والعواصف والأعاصير والزلازل الأرضية والبراكين، ويمكن التغلب على هذه الكوارث الطبيعية والتنبؤ بها قبل حدوثها بفضل التطور التكنولوجي الحديث أو من خلال التخطيط في اختيار موقع المنشأة المعلوماتية قبل الشروع في بنائها (24).

تعد هذه الأخطار تهديدا على شبكات المعلومات وبنيتها التحتية لأنها تقع دون سابق إنذار لذلك يجب الاحتياط دائما وعمل نسخة احتياطية Backup بشكل منتظم لمحتويات الشبكة تحفظ هذه النسخة في أماكن بعيدة عن المقر الرئيسي للشبكة الأم حتى يمكن استرجاع هذه المعلومات في حالة حدوث واحدة من تلك الكوارث الطبيعية المحتملة (25).

ب- المخاطر البيئية الطارئة Environmental threats:

تحدث هذه المخاطر من خلال اختراق مقاييس الأمن الطبيعية نتيجة سوء الاستخدام للمكونات المادية لنظام أمن المعلومات مثل أجهزة التكييف أو بسبب الغبار والأتربة وغيرها من العوامل التي تؤثر على أماكن تخزين المعلومات من الإهمال المباشر في الأماكن المخصصة لها أو غير المباشر من خلال نقاط الربط الجوهرية خارج نظام أمن المعلومات إما في إمدادات الكهرباء أو قنوات الاتصال عن بعد (26) ، ويمكن أن يؤدي إلى تعطل العمل وتوقفه لفترات طويلة مما يؤثر على أمن وسلامة المعلومات.

2- المخاطر الداخلية Internal Threats:

هناك العديد من المخاطر التي يكون مصدرها من داخل نظام أمن المعلومات نفسه بواسطة العامل البشري مثل العاملين أو بواسطة قصور في النظام أو اختراق للبنية التحتية له من برمجيات وأجهزة

تتمثل في المكونات المادية للنظام، ويمكن تقسيم المخاطر الداخلية لأمن المعلومات إلى الأقسام الآتية:

أ- المخاطر البشرية Humans Threats:

أشارت الدراسات أن 80 % من الهجمات الناجحة على المعلومات تنشأ عن عوامل التهديد الخارجي ولكن تكون من جانب العاملين على النظام وذلك عن طريق ما يسمى بالاصطياد Phishing والخداع لأحد المسؤولين عن نظام أمن المعلومات من الداخل أو عن طريق تحميل برامج ضارة مما يتيح للمهاجمين الوصول إلى النظام (27).

ويقصد بالمخاطر البشرية أنها "الأخطاء التي يمكن أن تحدث أثناء تصميم التجهيزات أو نظم المعلومات، أو من خلال عمليات البرمجة أو الاختبار أو التجميع للبيانات أو أثناء إدخالها إلى النظام أو في عمليات تحديد الصلاحيات الخاصة بالمستخدمين، وتشكل هذه الأخطاء الغالبية العظمى للمشاكل المتعلقة بأمن وسلامة المعلومات" (28) عادة ما يتألف الأمن البشري في أي منشأة معلوماتية من ضرورة ضمان أن يكون الأشخاص المصرح لهم بالاتصال بالنظام جديرين بالثقة ومسؤولين بشكل يضمن عدم تعرضهم للضغوط التي يمكن أن تقع عليهم من خارج نظام أمن المعلومات، ويشمل نظام أمن المعلومات بالنسبة للعنصر البشري بشكل عام الفئات التالية (29):

1. المستخدمين: هم المستفيدين من المعلومات الموجودة في المنشأة المعلوماتية.
2. مشغلي الخدمات المعلوماتية: هم الأشخاص الذين يديرون نظام أمن المعلومات.
3. المبرمجين: هم المسؤولين عن برمجيات الحاسوب والأساليب التقنية المتعلقة بأمن المعلومات.
4. الزائرين :تضم هذه الفئة أولئك الأشخاص الذين لهم حق الاطلاع فقط على المعلومات دون التدخل فيها.
5. مهندسي المعلومات :هم المنوط لهم بتشغيل التطبيقات المعلوماتية وإصلاح الأخطار الواردة عليها، كما أنهم من يقومون بالمتابعة الدورية لنظام أمن المعلومات.

ب- المخاطر التقنية Technical Threats:

يغلب على هذه المخاطر الطابع الفني وتتم نتيجة تهديدات ناجمة عن القصور والثغرات الموجودة في مختلفة أنظمة أمن المعلومات، دون أي تدخل بشري أو أي تهديدات طبيعية أو بيئية ومن هذه التهديدات ما يلي:

1. تهديدات عيوب التصميم: تشمل عيوب التصميم في الأجهزة والبرامج والشبكات وأدوات الربط والتخزين، أو أي مكون آخر من المكونات المادية لأنظمة المعلومات.
2. تهديدات تشتت المعلومات: إذا كانت معلومات المنشأة مشتتة وتم تخزينها في أماكن كثير ومتفرقة يتم التعامل معها من خلال شبكات متعددة.
3. خلل في المعدات: أن تكون هذه الأعطال بسبب قدمها وعدم متابعة عمليات تجديدها وتحديثها أو بسبب الاستعمال الخاطئ.
4. أخطاء البرمجيات: قد تحتوي البرمجيات المستخدمة في أمن المعلومات على العديد من الأخطاء الأمر الذي ينعكس بالتالي على دقة المخرجات وصحة المعالجة التي يقوم بها النظام، ويتم ذلك عن طريق استخدام برامج غير أصلية أو نسخ مقلدة منها بطريقة غير شرعية.
5. أخطاء البيانات: يتعلق بأخطاء بإدخال البيانات في نظام أمن المعلومات بحيث يتم إدخال بيانات غير صحيحة مما ينعكس على دقة المعلومات المستخرجة في عمليات الاسترجاع (30).

3- المخاطر الإلكترونية Electronic Threats:

تقع المخاطر الإلكترونية في الغالب من خارج النظام من قبل أشخاص ليس لهم علاقة به أو صلاحيات الدخول، وتكون هذه الاعتداءات عباره عن قرصنة المعلومات واختراق الضوابط الرقابية والأمنية للنظام بهدف الحصول على معلومات لها طالع السرية، حيث تكمن خطورة تلك المخاطر في عدم معرفة من قام بالاختراق وماهي حدود قدرته في التخريب بالإضافة إلى عدم معرفة الهدف من وراء هذه الاختراقات (31).

منذ وقت قريب كانت المخاطر الإلكترونية تتعلق بتقنيات الحاسب الآلي ونظم المعلومات وما يتعلق بالمعالجة الآلية للمعلومات، حيث كانت تدور هذه المخاطر حول التلاعب في البيانات المدخلة للحاسب الآلي والاعتداءات التي تقع على المخرجات وسرقة البيانات عن طريق الاختراق، ويمكن تصنيف جرائم الحاسب الآلي إلى ثلاثة أنواع (32):

- الجريمة المحوسبة: وتكون الجريمة عبارة عن سوء استخدام أجهزة الحاسب الآلي بشكل غير قانوني، يؤدي إلى ارتكاب جريمة يعاقب عليها قوانين جرائم الحاسب الآلي.
- سوء الاستخدام لجهاز الحاسب الآلي: يكون سوء الاستخدام بشكل مقصود للتسبب في التخريب للأجهزة والتلاعب بالمعلومات.
- الجرائم المتعلقة بالحاسب الآلي :التي يكون فيها الحاسب الآلي نفسه أداة لتنفيذ الجريمة.

ويمكن أن تتم الجرائم الخاصة بالحاسب الآلي من العاملين داخل المنشأة المعلوماتية الذين لديهم صلاحيات التعامل مع النظام، حيث أشارت الدراسات إلى أن الخسائر الناتجة عن جرائم الحاسب الآلي ومنها دراسة أجرتها دائرة المحاسبة العامة وشركة أوركاند Orkand للاستشارات، أن حجم الخسائر المتعلقة بجرائم الحاسب الآلي تقدر بحدود 1.5 مليون دولار لشركات المصارف المحسوبة في الولايات المتحدة الأمريكية، ومن ناحية أخرى يقدر المركز الوطني لبيانات جرائم الحاسب الآلي في لوس أنجلوس بنحو 70 % من جرائم الكمبيوتر تزداد بصورة واضحة (33)، مما يجعلها تشكل تحديا خطيرا يواجه الإدارات العليا بشكل عام وإدارة نظم المعلومات بشكل خاص.

الجدير بالذكر أن ظهور الجريمة الإلكترونية أو السيبرانية كان نتيجة التطور التكنولوجي في نظام الاتصالات وخدمات الإنترنت، ويمكننا تصنيف الجرائم التي تتم عن طريق استخدام تكنولوجيا المعلومات من خلال الحاسب الآلي إلى الأقسام الآتية (34):

أ- جرائم نشر المعلومات السرية.
ب- جرائم التزوير الإلكترونية.
ت- جرائم ترويج الإشاعات.
ث- جرائم تقنية المعلومات.

3.1.2 أشكال المخاطر التي تهدد أمن المعلومات:

تعددت أشكال ونماذج المخاطر التي تهدد أمن المعلومات فمنها ما يتعلق بالمخاطر الناتجة عن الجرائم الخاصة بالاعتداء على محتوى الحاسب الآلي سواء في مكوناته المادية أو المكونات المعنوية وقواعد البيانات أو المعلومات التي تكون ضمن محتويات الحاسب الآلي، أو الجرائم المتعلقة بمحتويات الشبكة العالمية التي تستخدم من خلال الحاسب الآلي وتكون وسيلة للربط بين الحواسب الآلية وما

ينتج عن ذلك من الجرائم السيبرانية، وفيما يلي نتناول بإيجاز قدر الإمكان لأهم نماذج هذه المخاطر في ضوء تصنيفات المخاطر التي تهدد أمن المعلومات السالفة الذكر وذلك على النحو التالي:

1. هجوم تعطيل الخدمة Denial Of Services (DOS):

يتم هجوم تعطيل الخدمة عن طريق إرسال عدد هائل من طلبات الاتصال أو أوامر بروتوكولات الشبكات مثل أمر Ping إلى الجهاز الضحية من أجل إغراقه في معالجة هذه الطلبات مما يحمل الحاسب الآلي أكثر من طاقته حتى يتوقف عن الاستجابة، ومن ثم عدم قدرته على القيام بمهامه، وقد تصل درجة الإغراق Flooding إلى تعطيل الهدف نهائيا والخروج من الخدمة.

يستهدف هجوم تعطيل الخدمة عبر خدمات الإنترنت ثلاثة أنواع مختلفة وهم: المستخدم وجهاز الحاسب الآلي المضيف للخدمة بالإضافة إلى شبكة الاتصال، حيث يبدأ هجوم تعطيل الخدمة باستخدام أدوات ترسل عبر الإنترنت مثل تعرف باسم Trin00,Tribe Flood Network, Stacheldraht وهي أدوات خاصة بإغراق الحاسب الآلي بالأوامر المتتالية حتى يقف عن الاستجابة ومن ثم يمكن استغلال الثغرات في وقت توقف الحاسب الآلي للوصول غير المصرح به للبيانات واستخدام بعض الأساليب لإتلاف البيانات وتعطيل الخدمة ومنع المستخدمين الشرعيين من الوصول إليها (35).

2. الهندسة الاجتماعية Social Engineering:

أشار ساجار رالكار Sagar Rahalkar إلى أن الهندسة الاجتماعية هي الفن الخادع في التواصل مع الناس من أجل الحصول على معلومات هامه تأخذ الشكل السري، ومعظم الناس لا يعلمون مدى قيمة المعلومات التي يمتلكونها، فنجد المهاجمين يقومون باستخدام العديد من الحيل المختلفة لإقناع الضحية بتقديم هذه المعلومات عن طريق الادعاء بأنه مسؤول معترف به كما هو الحال في سرقات أرقام بطاقات الائتمان فيدعي هنا المهاجم بأنه مسؤول بنك من البنوك الشهيرة ثم يسأل الضحية عن رقم الائتمان الخاص به أو رقم التعريف الشخصي الخاص به (36).

ومن خلال هجمات الهندسة الاجتماعية يستخدم المهاجمون مجموعة من التكتيكات المتنوعة لإنجاز أهدافهم، ويمكن أن تكون حيله بسيطة مثل اكتساب ثقة الضحية عبر الهاتف للحصول على معلومات سرية لإعداد الطعم لشخص ما للوصول إلى موقع الويب المخترق من خلال ما يسمى بالاصطياد الإلكتروني (37).

3. الاصطياد الإلكتروني Phishing:

يعتبر الأسلوب النموذجي للجمع بين جرائم خداع الهندسة الاجتماعية وتكنولوجيا الشبكات، الذي يتم عن طريق عمل موقع إلكتروني مزيف لموقع إلكتروني قائم بالفعل بهدف خداع المستخدمين، ويكون ذلك عادة من خلال الرسائل غير المرغوب فيها عن طريق البريد الإلكتروني ورسائل الهاتف المحمول بالإضافة إلى الإعلانات الكاذبة التي تظهر بشكل مفاجئ خلال تصفح محتويات المواقع الإلكترونية ومن خلالها سرقة حسابات البريد الإلكتروني أو أرقام الحسابات البنكية وغيرها من المعلومات الهامة (38).

ترجع تسميته بهذا الاسم إلى عام 1996 حيث كان قبلها يطلق عليه مصطلح الصيد قبل أن يتغير إلى الاصطياد الإلكتروني، كما أن أول حادثة تمت باستخدامه كان ضحيتها موقع أمريكا أون لاين America Online (AOL) في عام 1990، لأنه من أجل فتح حساب للحصول على خدمات الموقع يجب على المستخدم أن يكتب تفاصيل بطاقته الائتمانية كاملة ثم قام المهاجمون بعمل موقع مزيف مماثل للموقع الأصلي، من خلاله تمت سرقة ملايين البيانات البنكية الخاصة بالمشتركين في موقع أمريكا أون لاين (39).

يتم خداع المستخدمين عن طريق الرسائل المزيفة السالف ذكرها التي تحتوي على روابط لمواقع إلكترونية مزيفه تشابه الموقع الإلكتروني الأصلي، وبالتالي يقوم المستخدم بالدخول على تلك المواقع وملئ البيانات التي تعود على كتابتها عند تصفحه للموقع الأصلي مثل معلومات حسابه البنكي أو معلومات خاصة بمواقع أخرى هامه وبذلك يقع المستخدم ضحية لجرائم الاصطياد الإلكتروني، لإن الموقع المزيف يكون متماثل من حيث الواجهة الرئيسية للموقع الأصلي مثل ألوان التصميم والأشكال ويمكن أن يختلف الموقع المزيف عن الأصلي بفرق بسيط كحرف زائد أو ناقص عن عنوان الموقع الأصلي ونتيجة لهذا التشابه فلا يستطيع المستخدم العادي أن يفرق بين الموقع الأصلي والمزيف(40).

4. البرمجيات الضارة Malware:

تعد البرمجيات الضارة من أعظم الاعتداءات التي تتعرض لها أنظمة المعلومات التي تصيب أجهزة الحاسب الآلي والهاتف المحمول في حالة اتصاله بخدمة الإنترنت، وتشير البرمجيات الضارة على وجه العموم إلى برنامج أو كود يمكن زرعه سرا في جهاز الضحية بدون إذن منه

بغرض إحداث الضرر فيه أو تعطيله أو القيام بأي إجراء غير مشروع على المعلومات التي يحتويها جهاز الضحية(41).

أما بالنسبة لأنواع البرامج الضارة فقد قسمها أستاذ أمن المعلومات مارتينيز توريس Martinez Torres إلى ثلاثة فئات رئيسية من حيث الاعتماد على كيفية انتشارها عبر شبكات الإنترنت وهي الفيروسات وأحصنة طروادة والديدان (42) ، وهي على النحو التالي:

أ- الفيروسات Viruses:

بدأ ظهور الفيروسات في السبعينات من القرن الميلادي الماضي، وكانت درجة خطورتها بسيطة في البداية ليست على مستوى الخطورة الموجودة في الوقت الحاضر، ثم أصبحت أكثر خطرا وانتشارا عن السابق نظرا لتزايد استخدام الحاسب الآلي وانتشار خدمات الإنترنت، لذلك تعد أكبر فئات البرامج الضارة من حيث تعدد أشكالها وأنواعها.

وأشار فيرناندو جورجيل Fernando Georgel إلى أن الفيروسات عبارة عن البرامج التي يمكن أن تصيب برامج أخرى عن طريق تغييرها أو بنسخها مره أخرى بداخل برامج الحاسب، وتمر دورة حياة الفيروسات بعدة مراحل حتى تتمكن من إلحاق الضرر بجهاز الحاسب الآلي، وهم أربعة مراحل نتناولهم على النحو التالي (43):

1. مرحلة الخمول: عندما يكون الفيروس خاملا في انتظار تنشيطه من قبل المستخدم.
2. مرحلة الانتشار: تحدث عندما يقوم الفيروس بإنشاء نسخة من نفسه وإدراجها في برنامج معين من البرامج المحفوظة على جهاز الحاسب الآلي.
3. مرحلة التفجير: يقوم فيها الفيروس بالتحرك في تنفيذ وظائفه المطلوبة منه.
4. مرحلة التنفيذ: يقوم الفيروس بالبدء في التصرف على النحو المطلوب منه في تدمير البرامج أو تسريب المعلومات وإتلافها.

ب- أحصنة طروادة Trojans Horses:

تعد أحصنة طروادة من البرمجيات الضارة التي تظهر في شكل برامج مشروعة ولكنها تخفي في داخلها برامج ضارة حتى يقوم الضحية بتثبيتها على جهازه أو تشغيله ثم يتمكن المخترق من الوصول عن طريقها إلى جهاز الضحية، لذلك أطلق على هذه البرمجيات إسم أحصنة طروادة نسبة

إلى القصة اليونانية المشهورة التي قام الإغريق بالتسلل داخل حصان خشبي ضخم مخبئ بداخلة الجنود حتى يتثنى لهم الدخول إلى أراضي العدو كتمويه لاكتساب الحرب (44).

وفي حالة ما إذا قام المستخدم للجهاز الضحية بتشغيل البرامج التي تحتوي على أحصنة طروادة يتم حينها تنشيط البرامج الضارة المخبأة بداخلها وتعمل على ممارسة عملها الذي صممت خصيصا للقيام به وغالبا ما يكون الغرض منها هو التجسس، حيث تسمح هذه البرمجيات بالتحكم في الجهاز الضحية أثناء الاتصال بخدمة الإنترنت وتصفح محتوياته فضلا عن تنفيذ الأوامر المتعلقة به (45).

ج- الديدان Worms:

على عكس الفيروسات التي تتطلب من الضحية اتخاذ بعض الخطوات للتعرض للفيروسات مثل نسخه من مصدر آخر مصاب أو تنشيطه بالخطأ، فإن الديدان لها القدرة على الانتشار بشكل سريع عبر الإنترنت ويكون الهدف منها عادة نفس الأهداف الخاصة بالفئتين السابقتين وهو إحداث الضرر بأنظمة الكمبيوتر لتدمير المعلومات التي يحتويها، أو لجمع المعلومات الشخصية بدون علم صاحب جهاز الحاسب الآلي (46)، وعادة ما تنتشر ذاتيا عبر شبكة الإنترنت من خلال نقاط الضعف التي تتسبب في وجود الثغرات الأمنية الموجودة في نظام أمن المعلومات (47).

5. برمجيات التجسس Spyware:

تعتبر برامج التجسس نوع آخر من البرمجيات الخبيثة التي تتوافر فيها الأغراض غير الشرعية فهي تعمل على مراقبة كل ما يكتبه الضحية حتى أنه تسجل النقرات على لوحة المفاتيح وترسلها إلى المخترق وتقوم أيضا على أعمال خبيثة أخرى (48) . البرامج الضارة التي تقوم بتنفيذ مهامها بشكل مستقل عن طريق الاتصال بالشبكات الاجتماعية أو موقع ما على شبكة الإنترنت، وتقوم هذه البرامج بجمع معلومات حول ما يقوم به المستخدم من أنشطه سواء عبر الإنترنت أو في وضع عدم الاتصال بالإنترنت على الجهاز الخاص بالضحية وإرسال هذه المعلومات للمخترق فور اتصال الحاسب الآلي بالإنترنت (49)، ولبرامج التجسس أنواع عديده نذكر منها ما يلي:

أ. برامج التجسس البسيط ومتابعة نشاط المستخدم.
ب. برامج تسجيل نقرات لوحة المفاتيح Keyloggers.
ت. برامج الإعلانات Adware.
ث. النوافذ الفقاعية أو المنبثقة Popup.

6. البريد الإلكتروني غير المرغوب Spamming:

ويتم في هذا النوع من الهجمات استخدام البريد الإلكتروني كوسيلة لإغراقه بالرسائل الدعائية لمنتجات معينة مما يستهلك موارد الحاسب الآلي ويتطلب ذلك كثيرا من الوقت والمال مما يؤدي إلى خنق الشبكة والعمل على إبطائها في نقل البيانات وسرعة استجابة خدمة الإنترنت نفسها.

يرجع السبب لاختيار البريد الإلكتروني ليكون البيئة التي يتم من خلالها شن مثل هذا النوع من الهجمات إلى أن العلاقات الاجتماعية القائمة بين المستخدمين وخاصة في مواقع التواصل الاجتماعي تكون قائمة على الثقة الوهمية، مما يعني أنه من السهل إقناع المستخدم المستهدف بقراءة محتوى البيانات غير المرغوب فيها ويرجع ذلك إلى الإيهام بأنها رسائل آمنه ونتيجة لذلك يمكن أن تطور هذه الهجمات إلى جرائم الاصطياد الإلكتروني Phishing (50).

جدير بالذكر أن تلك الأنواع التي تم تناولها تعتبر أهم نماذج وأشكال المخاطر التي تتعرض لها أمن المعلومات في بيئة الإنترنت، بالإضافة إلى العديد من الأنواع الأخرى مثل مخاطر هجمات الانتحال Spoofing Attacks وهجمات اعتراض البيانات Sniffer Attacks وغيرها من المخاطر التي لا يتسع المجال لذكرها.

4.1.2 التدابير الأمنية لحماية أمن المعلومات:

من خلال تناول مخاطر أمن المعلومات السالف ذكرها كانت هناك حاجة ماسة لتوفير التدابير الأمنية الكافية لحماية أمن المعلومات من هذه المخاطر بالإضافة إلى إيجاد تقنيات مبتكرة تضمن شرعيتها وتأمينها من تلك المخاطر، ويمكن تقسيم التدابير الأمنية اللازمة لحماية أمن المعلومات إلى أربعة أقسام رئيسية وهي :التدابير التنظيمية، المادية، التقنية، بالإضافة إلى التدابير التشريعية لضمان توفير حماية أمن المعلومات، وفيما يلي تناول هذه التدابير على النحو التالي:

أولا: التدابير التنظيمية Organizational Measures:

تتعلق التدابير التنظيمية بالأنشطة الإدارية داخل مؤسسات أمن المعلومات، حيث تهدف هذه التدابير لبناء بيئة آمنة للمعلومات والحفاظ عليها من خلال مجموعة من الإجراءات الإدارية الأمنية المضادة ويتم اختيارها للتطبيق بشكل فعال داخل مؤسسات أمن المعلومات (51)، ويمكن تقسيم التدابير التنظيمية إلى قسمين هما :تدابير إدارية وأخرى شخصية خاصة بالعاملين في مؤسسات المعلومات، نتناولهما كما يلي :

أ- التدابير الإدارية:

يراد بالتدابير الإدارية سيطرة جهة الإدارة على إدارة نظم أمن المعلومات وقواعدها مثل التحكم بالبرمجيات الخارجية أو الأجنبية عن المنشأة، فضلا عما يتعلق بمسائل الإشراف والمتابعة على أنشطة المؤسسة في الرقابة على الاشتراكات الخارجية للمنشأة مع المؤسسات الأخرى ومسائل التحقيق في المخاطر التي تتعرض لها المنشأة (52).

ويمكن توفير التدابير الإدارية للازمة لحماية أمن المعلومات من خلال مجموعة من التعليمات والإرشادات مثل سياسات أمن المعلومات واستراتيجيات إدارة أمن المعلومات، حيث يتم اعتماد هذه السياسات لتحديد طرق استخدام المعلومات ومصادرها بشكل آمن وعمل الوثائق اللازمة لمراقبة التعامل مع المعلومات، كما يتم المراقبة على السلوكيات الغير مألوفة سواء من العاملين داخل المنشأة أو خارجها، ويجب توثيق هذه السياسات في وثائق مكتوبة وتعميمها على العاملين بالمنشأة لزيادة الوعي والاهتمام بأمن المعلومات (53).

ب- التدابير الشخصية:

تتعلق التدابير الشخصية بحماية المعلومات على مستوى الأفراد العاملين على نظام أمن المعلومات حيث يشكل الأفراد العاملون على النظام أحد أهم التهديدات القوية التي يمكن أن تؤثر على أمن وسلامة المعلومات، فقد يرتكب الفرد خطأ عند استخداما لنظام أو أثناء إعداد وتجهيز البرامج الخاصة بالمنشأة مما يقلل من فعاليتها كما يجب عدم إغفال أن أعظم التهديدات تأتي قد تأتي من العاملين على النظام(54).

ترتبط حماية العاملين في النظام بوسائل التعريف الخاصة بهم والتأهيل والتدريب للمتعاملين مع وسائل الأمن إلى جانب الوعي بمسائل الأمن ومخاطر الاعتداء على أمن المعلومات، لذا فإن أهم الإجراءات التي يمكن أن تساعد المنشآت المعلوماتية على اتخاذ التدابير اللازمة لحماية أمن المعلومات من التهديدات التي قد تحدث من العاملين لديها ما يلي (55):

1. تحديد كلمات مرور للعاملين على أن يراعى تحديد صلاحيات كل موظف بما يتناسب مع طبيعة عمله، وتكون قاصرة على نطاق عمله بالمنشأة فقط وليست صلاحيات دون حدود.

2. اختيار العاملين بعناية تامة مع ضرورة التأكد من أمـانتهم وإخلاصـهم ويظهـر ذلك من خلال قيام الإدارة بمراقبة سلوكياتهم عن بعد للتأكد من ذلك.
3. تدريب العاملين بشكل جيد تجنبا للعديـد مـن المشـكلات التـي قـد تواجههـا الشبكة.
4. التأكد من إزالة بيانات العاملين المنتهية مـدة خـدمتهم في المنشـأة مـن قائمـة مستخدمي النظام.

ثانيا: التدابير المادية Physical Measures:

يطلق مصـطلح التـدابير الماديـة علـى كافـة الوسـائل التـي تمنـع الوصـول إلى نظـم المعلومات وقواعدها مثل الأقفال والحواجز والغرف المحصنة وغيرها من الوسائل التي تقـوم على حماية الأجهـزة الحساسـة مـن العبـث أو التخريـب، ولتحقيـق المسـتوى المطلـوب مـن الحماية المادية لأمن المعلومات لابد من مراعاة عدة عوامل، منها ما يلي (56):

1. تخصيص غرف مغلقه لحماية أجهزة خادم الشبكة المركزيـة للمنشـأة أي بعيـدا عن غرف العاملين أو المستفيدين حتى لا يكون متاحا للجميع.
2. استخدام الكابلات المغلفة وذلك لتقليل الإشعاع الثانوي المنبثق من خلالها، مـع إمكانية إضافة أكثر من غلاف عليها لمنع هذا الإشعاع.
3. توفير وسائل مراقبة لموقع المنشأة من الداخل والخارج مثل الدوائر التلفزيونيـة المغلقة.
4. تأمين الأبواب والمنافذ وذلـك باسـتخدام أجهـزة الإنـذار الآليـة لتقـوم بتشـغيل أجراس التنبيه في حالة الدخول في غير ساعات العمل الرسمية.
5. تركيب الكابلات الخاصة بالشبكة عبر تمديدات عـبر الجـدران أو فـوق الأسـقف حتى لا تكون معرضه لوصول غير المختصين.

فضلا عن أن هناك طرق أخرى وأدوات تساعد المنشـأة عـلى تحقيـق الأمـن المادي وحمايته من التهديدات وهذه الطرق تتداخل مـع التـدابير التقنيـة لأمـن المعلومـات ولكـن سنتناول فقط ما يتعلق بالأمن المادي لأمن المعلومات، من هذه التدابير نذكر ما يلي:

1. التحكم في الوصول Access Control:

يعتبر التحكم في الوصول من التدابير المادية الهامـة والحساسـة في أمـن المعلومـات، فجميع أنظمة أمن المعلومات تحتاج أن تعمل في بيئة آمنة بعيدة عن أيدي غير المتخصصـين حتى لا يؤثر ذلك على كفاءتها مثل العبث والتخريب أو الأعطـال بسـبب العوامـل الطبيعيـة المختلفة مثل الحرائق والزلازل أو انقطاع التيار الكهربائي.

تبين أن التحكم بالوصول بالنسبة للتدابير المادية ينقسم إلى شقين :الشق المادي ويتعلق بالتدابير المادية مثل الحواجز الفيزيائية المادية لحماية الموارد المادية والمنشآت، والشق التقني الخاص بتصاريح الدخول الخاصة بالعاملين في المنشأة مثل كلمات السر وبطاقات الدخول الممغنطة بالإضافة إلى القياسات الحيوية Biometrics للتحكم بالوصول لخدمات المنشأة، فيما يلي سنتناول الشق المادي:

أ- الحواجز الفيزيائية Physical Barriers:

تتعلق الحواجز الفيزيائية بالوسائل التي تساهم في منع الوصول إلى الموارد الحيوية في منشأة المعلومات من أجهزة وشبكات وغيرها ولتطبيق ذلك لابد من توافر التدابير الآتية (57):

1. وضع ما يسمى بحواجز محيط المنشأة Perimeter الذي يتعلق بحماية محيط المنشأة الخارجي مثل الجدران الخارجية وصافرات الإنذار.
2. وضع حواجز أمام مدخل مراكز الأجهزة وإقفالها منعا لتعرضها لبرامج التجسس وغيرها.
3. التحكم من خارج المنشأة عن طريق البوابات المغلقة وسجلات الدخول وأجهزة المراقبة.

ب- الكاميرات ونظم المراقبة:

تساعد الكاميرات ونظم تحقيق الهوية للموظفين والمترددين على المنشأة من حفظ الأمن المادي لأمن المعلومات وذلك من خلال مراقبة الدخول والخروج من وإلى المنشأة وتحديد هوية المصرح لهم بالتواجد في المكان الذي يوجد فيه الحاسب الآلي، وتساعد كاميرات المراقبة على رصد أي نشاط من جانب أفراد غير مصرح لهم بالتواجد في أمكان وجود الأجهزة الحساسة، وأيضا تعد دليلا في حالة ارتكاب أي تهديدات على أمن المعلومات (58).

2. نظم الإنذار المبكر:

تستخدم كنوع من التدابير اللازمة لحفظ أمن محيط المنشأة بالإضافة إلى حماية الموارد التقنية والمادية الموجودة بها، وتستخدم هذه النظم العديد من الأجهزة الحساسة الخاصة بالإنذار المبكر Sensors لرصد أعمال السرقة والحريق والعديد من الكوارث الطبيعية مثل الزلازل البراكين وغيرها وتستخدم أجهزة أخرى لرصد المواد المشعة والسامة للحفاظ على الأمن المادي للأجهزة (59).

ثالثا: التدابير التقنية Technical Measures:

هناك العديد من التدابير التقنية التي تهدف إلى حماية أمن المعلومات من المخاطر الداخلية والخارجية والعمل على الحد منها، سنتناول أهم هذه الوسائل على النحو التالي:

1. برامج مكافحة للفيروسات Antivirus Software:

هي البرمجيات التي تستخدم لإكتشاف وإزالة كافة أنواع البرمجيات الضارة والخبيثة والعمل على محوها تماما من النظام لما لهذه البرمجيات من تهديدات قد تؤثر على أمن المعلومات التي تضمها المنشأة (60).

وعملت العديد من شركات الحماية على تطوير برامج مضادة للأنواع الحديثة من الفيروسات التي تنتشر في البيئة الإلكترونية ومن أمثلتها MacAfee, Kaspersky, Norton, Avira, Avast وغيرها من الشركات ،ولكي تكون برامج مكافحة الفيروسات قادرة على القيام بعملها بشكل متكافئ وفعال لابد من تمتعها بعدد من السمات الواجب توافرها، نذكر منها ما يلي (61):

1. أن يكون مدمج بداخلها جدار ناري Firewall للتصدي لأي محاولات لاختراق بنية نظام أمن المعلومات، ويقوم بالتحديث التلقائي لنفسه للتعرف على الأنواع الحديثة من البرمجيات الضارة.
2. أن تتمكن هذه البرامج من فحص البريد الإلكتروني للمستخدمين بشكل مستمر والعمل على كشف أي تهديدات يمكن أن تحدث مثل جرائم الانتحال وغيرها.
3. أن يكون ذو استهلاك قليل لموارد الحاسب الآلي الموجود فيه حتى لا يتسبب في بطء الحاسب الآلي وتوقفه عن العمل في حالة القيام بعمليات البحث عن الفيروسات.

2. برامج الجدران النارية Firewalls:

تعمل هذه الفئة من البرامج على تأمين المنافذ Ports الموجودة في الحاسب الآلي التي من خلالها تتمكن التطبيقات من على الحصول على خدمات الإنترنت، وفي كثير من الأحيان لا يعلم المستخدم بالمنافذ المفتوحة على النظام مما يسمح بنسيان تأمين هذه المنافذ وحمايتها، فتعمل برامج الجدران النارية كمصفاة تمنع وصول البرمجيات الضارة إلى الأجهزة عن طريق هذه المنافذ المفتوحة (62).

وتقوم الجدران النارية على حماية أجهزة الحاسب الآلي أو شبكة تربط العديد من الأجهزة من الاختراقات من طرف جهة ثالثة، حيث يقوم بتصفية حزم البيانات المتبادلة مع الشبكة، وتنقسم الجدران النارية إلى نوعان وهما:

ج. **الجدران البرمجية:** يستخدم هذا النوع على الحاسبات الآلية المستقلة أو المرتبطة بشبكات الإنترنت أو على الخوادم ومن أبرز أنواع هذه الجدران Norton, Kaspersky.

ح. **الجدران المادية:** وتسمى أحيانا بالعلب السوداء حيث تستخدم على الأجهزة الخادمة التي تقوم على تزويد الأجهزة الأخرى بخدمات الإنترنت وهي أكثر أمنا من الجدران النارية البرمجية ومن أمثلتها SOHO WatchGuard (63).

3. التشفير Encryption:

يعتبر التشفير هو العلم المستخدم لحفظ أمن وسرية المعلومات، فلا يمكن معرفة فحوى المعلومات المرسلة من قبل أي شخص آخر غير الشخص المرسلة إليه تلك المعلومات ويكون مالكا لمفتاح فك تشفيرها مع ملاحظة أنه في حالة وصول تلك المعلومات إلى أشخاص آخرين فإنهم لا يستطيعون الاستفادة منها أو حتى فهم معناها (64)، وينقسم إلى نوعان أساسيان وهما كالتالي (65):

1. التشفير المتماثل Symmetric Encryption:

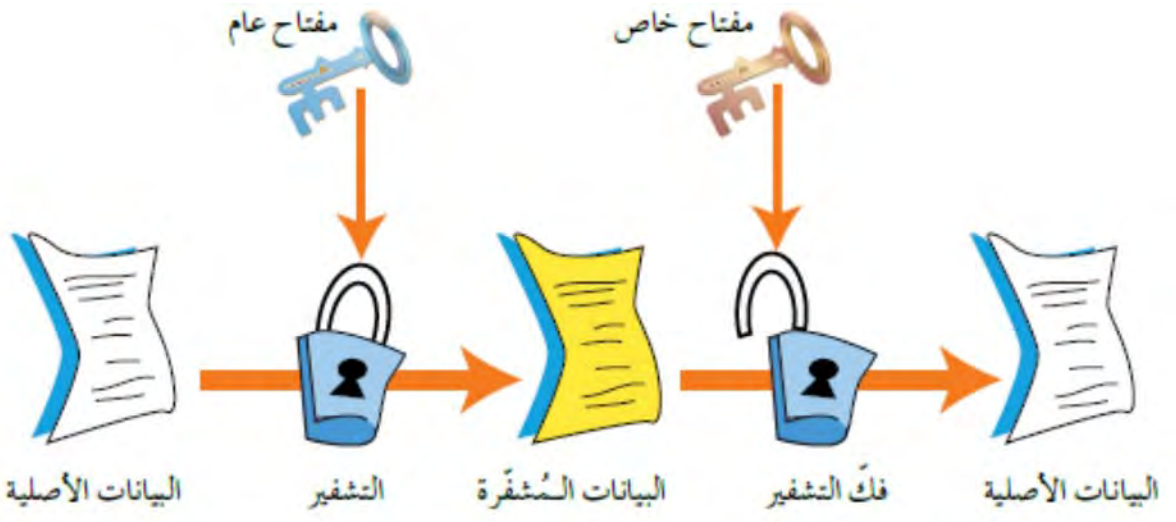
شكل (2)

التشفير المتماثل Symmetric Encryption (66)

يسمى أحيانا بالتشفير المتناظر أو باسم تكنولوجيا تشفير المفتاح الخاص، ويستخدم في هذا النوع من التشفير مفتاح واحد للتشفير وفك الشفرة وبذلك فإنه يكون معلوما بين مرسل المعلومات والمستفيد منها، ويرسل مفتاح فك التشفير بوسيلة أخرى بعيدا عن المعلومات المرسلة، ويوضح الشكل (2) طريقة عمل التشفير المتماثل.

2. التشفير غير المتماثل Asymmetric Cryptography:

يستخدم في هذا النوع مفتاحان لكل مستخدم للمعلومات يكون إحداهما معروفا من قبل المستخدمين الآخرين في حالة الرغبة في إرسال معلومات مشفرة إلى شخص آخر على علم بالمفتاح الأول، ولفك التشفير يستخدم مفتاح خاص لا يعرفه سوى مستقبل المعلومات نفسه، ويمكن توضيح طريقة عمل التشفير غير المتماثل من خلال الشكل التالي.



شكل (3)

التشفير غير المتماثل Asymmetric Encryption (67)

أتى التشفير الغير متماثل لإصلاح عيوب ومشاكل النوع السابق من التشفير حيث كانت تواجه مشكلة التوزيع غير الآمن للمفاتيح المستخدمة في التشفير المتماثل، فيتم استخدام مفتاحان إثنين تربط بينهما علاقة ما لزيادة الأمان والتعقيد في محاولة فك تشفير المعلومات المشفرة باستخدام التشفير الغير متماثل.

4. أنظمة كشف الاختراق Intrusion Prevention System:

تعمل هذه الأنظمة على منع التسلل ورصد المحاولات المتكررة للاستغلال حتى إذا لم يتم إصلاح نقاط الضعف التي يجري استغلالها، ويمكن لهذه الأنظمة أن تقدم إشعارات فورية لهذه المحاولات وأن تمنع هجمات مستهدفة معينة وقت حدوثها .حيث إن نقاط الضعف في نظم أمن المعلومات تكون المصدر الأول لعمليات التسلل، وعادة تكون هذه النقاط التي تمثل ثغرات داخل النظام موجودة نتيجة لسوء الاستخدام من قبل العاملين على النظام (68).

تختلف أنظمة كشف الاختراق عن برامج الجدران النارية في أنها تقوم في فحص حركة المرور للمعلومات من وإلى المستخدمين للكشف عن الهجمات المتوقعة عكس برامج الجدران النارية التي تفرض قواعد صارمة على حركة المرور وإغلاق المنافذ التي يمكن استغلالها في عمليات الاختراق فيقوم بفحص المعلومات المتداولة واتخاذ قرار السماح بمرور هذه المعلومات أو منعها في حالة الشك في أنها محاولات لاختراق النظام، لذلك فإن برامج كشف الاختراق أقل نضجا من الجدران النارية ولكنها أكثر تعقيدا في طريقة العمل (69).

5. التحكم بالوصول Access Control:

سبق وأن تناولنا التحكم بالوصول في التدابير المادية ولكن من الناحية المادية الخاصة بحماية أمن موارد المنشأة وما يتعلق بأمن المحيط من حيث المنشآت المادية والأجهزة الإلكترونية التي تحتويها هذه المنشأة، وهنا نتناول تدابير التحكم في الوصول من الجانب التقني وما يتعلق بالوسائل التكنولوجية الحديثة لفرض الحماية على أمن المعلومات ، وتتخذ المنشأة العديد من الوسائل التقنية لتحقيق الخطوات السابق ذكرها مثل بطاقات الهوية وكلمات السر والبطاقات الذكية ووسائل التعريف البيولوجية أو ما يسمى بالقياسات الحيوية، وسنتناول أهم هذه الوسائل في النقاط التالية :

أ- كلمات السر Passwords:

يمكن لكلمات السر أن تكون عبارة عن كلمة أو جملة تستخدم للدخول إلى النظام والمصادقة عند الدخول مثل سؤال :ماذا تعرف؟ (70)، أو أي طريقة لكتابة كلمات السر ولكن بشرط أن تكون معقدة وغير قابلة للتخمين، ويجب اتخاذ عدد من الخطوات عند إعداد كلمات المرور نذكر منها ما يلي :(71)

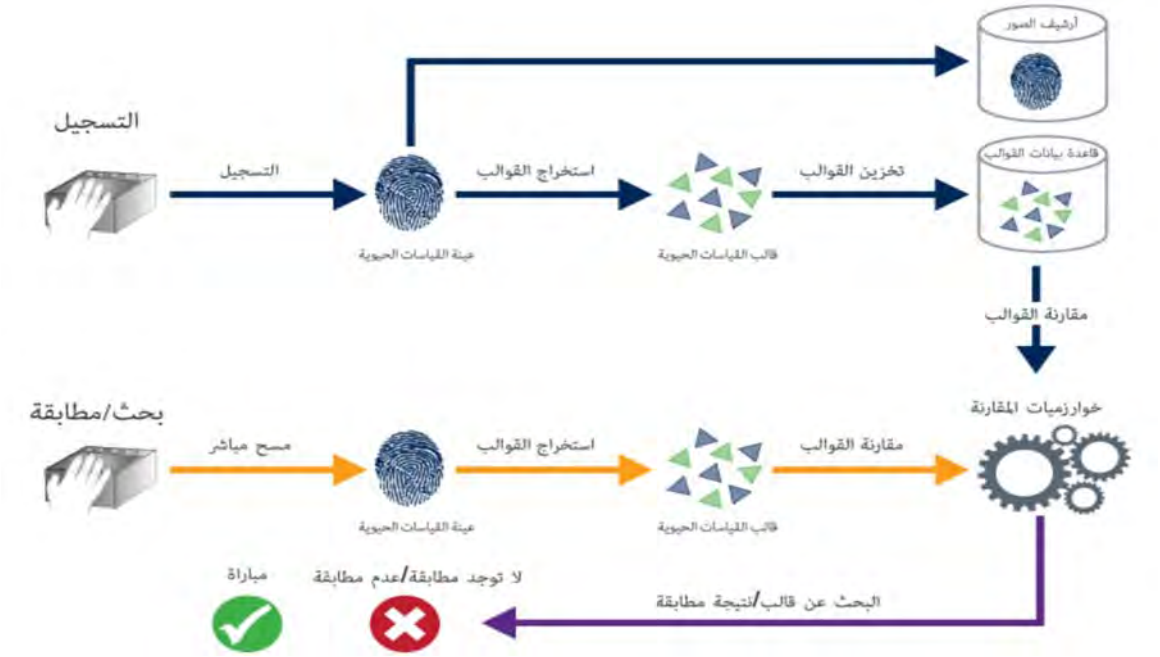
أ. لا تضمن بيانات شخصية مثل تاريخ الميلاد وغيره.
ب. أن تكون صعبة وغير قابلة للتخمين وتكون خليط بين الحروف والرموز والأرقام.
ت. عدم إطلاع الغير عليها بأي شكل، مع ضرورة أن يتم تغييرها بشكل دوري.

ب- البطاقات الذكية Smart Cards:

تستخدم البطاقات الذكية كتقنية من تقنيات التحكم بالوصول حيث يختزن فيها معلومات عن المستخدم مثل أسمه وبياناته الشخصية وكلمة المرور الخاصة به على شريط ممغنط يستخدم عند رغبة الشخص في الدخول إلى نظام المعلومات واستخدام مواردها وذلك بتمرير البطاقة من خلال ماسح رقمي يعمل على ترجمة البيانات المختزنة عليها ومقارنتها ببيانات الشخص على النظام، ويسمح له بالمرور عند تطابق هذه البيانات بين البطاقة والنظام (72).

ج- تقنيات القياسات الحيوية Biometrics:

تهدف تقنيات القياسات الحيوية في التدابير المتعلقة بالتحكم بالوصول إلى تحديد هوية المستخدم والتحقق منها استنادا على بعض الخصائص البيولوجية التي لا يمكن تكرارها بين شخص وآخر مثل الوجه والأذن وقزحية العين وبصمات الأصابع، والحمض النووي أو الخصائص السلوكية للإنسان مثل الصوت وطريقة المشي والتوقيع (73) ، ويوضح الشكل التالي عملية حفظ عينات من الخصائص البيولوجية للمستخدم والمصادقة عليها من قبل النظام للسماح له بالدخول عند الحاجة:



شكل (4)

طريقة عمل نظم القياسات الحيوية Biometric systems (74)

يوضح هذا الشكل استخدام طريقتين للتحقق من هوية المستخدم : الأولى تسمى طريقة التسجيل، يتم فيها أخذ عينة من أحد الخصائص البيولوجية مثل تفاصيل الوجه و قزحية العين وبصمات أحد الأصابع عن طريق مسح بيولوجي لهذه الخصائص وتخزينها في ملف خاص بالمستخدم مدمج بالنظام. وعند محاولة الشخص الدخول إلى النظام تتم الطريقة الثانية وهي مرحلة المطابقة والتحقق من الهوية حيث تتم مقارنة الخصائص البيولوجية لهذا الشخص كما في الشكل الموضح وعند المطابقة يسمح له بالدخول إلى شبكة النظام.

6. التخزين الاحتياطي Backup:

يقصد بالتخزين الاحتياطي مجموعة الإجراءات والمعلومات والبرامج التي يجب توفيرها في أماكن مخصصة خارج المقر الرئيسي للمنشأة وذلك للرجوع إليها في حالة حدوث ما يمنع استخدام النظام الأساسي المعمول به داخل المنشأة، سواء كان ذلك بسبب عرضي أو متعمد ونظرا لارتفاع تكاليف تأسيس نظام تخزين متكامل هناك بعض الخيارات التي يمكن للمنشأة أن تتخذها في عمل نظام تخزين احتياطي لمحتوياتها منها ما يلي (75):

أ- نظام احتياطي متكامل :

يكون هذا النظام ذات تكلفة عالية لما يتطلبه من إجراءات وتجهيزات كبيرة تماثل النظام الأساسي المستخدم في المنشأة من حيث الأجهزة والإيدي العاملة والمتخصصين.

ب- مركز فرعي لنظام التخزين :

في هذا الخيار يكون للمنشأة أحد الفروع الذي يتم اعتباره مركزا احتياطيا للنظام الأساسي بحيث يزود ببعض أجهزة التخزين ويتم ربطه بالشبكة الأم واستخدامه كبديل في حالة حدوث أي أخطار تعترض النظام الأساسي.

ج- الاتفاق المتبادل :

يتم الاتفاق بين منشأتان بحيث يكون لديهما تماثل في نفس الأنظمة المستخدمة بحيث يتم اعتبار أحدهما مركز تخزين احتياطي للأخر في حالة تعرض أحدهما لأي حدث طارئ والعكس مع المنشأة الأخرى، ويعد هذا الخيار أقلهم تكلفة وتوفيرا للجهد المبزول في إنشاء مركز تخزين احتياطي.

7. التوقيع الرقمي Digital Signature:

يعتبر التوقيع الرقمي تأشيرة على الوثيقة باستخدام ما يسمى بالمفتاح الخاص الذي يكون لدى المرسل للمعلومات فقط فهو ليس التوقيع التقليدي، حيث تحول المعلومات إلى صورة رقمية مشفرة وتتكون المعلومات النهائية التي تكون جاهزة بعدها للإرسال من دالة رقمية خاصة بالمعلومات ودالة أخرى خاصة بالتوقيع بواسطة المفتاح الخاص وباندماجهما معا ينشأن التوقيع الرقمي ويقوم مستلم المعلومات باستخدام المفتاح العام الذي بحوزته بفك شفرة المعلومات المرسلة (76) ، وهناك نوعان للتوقيع وهما كالتالي (77):

أ- التوقيع المفتاحي Key-Based signature:

يقوم هذا النوع بتزويد الوثيقة الإلكترونية بتوقيع مميز يحدد خلاله الشخص الذي قام بالتوقيع ووقت التوقيع ومعلومات هامة عن صاحب التوقيع، حيث يتم تسجيل التوقيع الرقمي بشكل رسمي عند جهات خاصة تعرف باسم Certification Authority وهو طرف محايد مهمته التأكيد من صحة ملكية التوقيع الرقمي.

ب- التوقيع البيومتري Biometrics Signature :

هو عبارة عن تحديد نمط معين لحركة يد الشخص الذي يقوم بالتوقيع وذلك من خلال توصيل القلم الإلكتروني المستخدم في التوقيع بجهاز حاسب آلي يقوم الشخص باستخدامه للتوقيع ومن خلال الصلة بين القلم والحاسب الآلي يقوم بتسجيل حركة اليد عند التوقيع، حيث إن حركة اليد أثناء التوقيع تختلف بين شخص وآخر وهي من السمات الشخصية التي لا تتكرر، ويتم تسجيل التوقيع البيومتري من خلال جهة محايدة كالتي تستخدم في التوقيع المفتاحي.

8. العلامات المائية Digital Watermarking:

تستخدم هذه العلامات في كثير من الأحيان كطريقة لضمان ملكية المحتوى وقد تكون العلامات عن نص مرئي أو شعار يحدد بوضوح المالك الحقيقي للمصنف وتكون هذه العلامات بتغطية جزء كبير من البيانات ويصعب إزالتها، وبعض هذه العلامات غير مرئية للعين البشرية ويمكن استرداد هذه البيانات بعد موافقة المالك للمصنف حتى يقوم بإزالة العلامات المائية من المصنف ويكون بعدها صالحا للاستخدام (78).

رابعا: التدابير التشريعية Legal Measures:

نتيجة لإساءة استخدام التقنيات التكنولوجية الحديثة باستخدام الحاسب الآلي وخدمات الإنترنت، بادرت العديد من الدول باتخاذ العديد من التدابير التشريعية ضد هذه المخاطر ،سنتناول فيما يلي أهم التدابير التشريعية التي تحمي أمن المعلومات على المستوى الدولي بالإضافة إلى أحدث التشريعات التي صدرت في الجمهورية العربية السورية بشأن حماية أمن المعلومات من المخاطر التي تستخدم تقنيات المعلومات وذلك على النحو التالي:

1. التدابير التشريعية الدولية:

تعد معاهدة الويبو بشأن حماية حق المؤلف 1996 ومعاهدة الويبو بشأن فناني الأداء والتسجيلات الصوتية 1996 ويطلق عليهما اتفاقيتي الإنترنت من أولى الجهود الدولية التي تناولت إشكالية حماية أمن المعلومات في بيئة الإنترنت لأنهما توفران الحماية لحقوق المؤلف والحقوق المجاورة في بيئة الإنترنت، حيث حرصت معاهدة الويبو بشأن حق المؤلف في المادة الرابعة على تأكيد أن برامج الحاسب الآلي تعتبر من المصنفات الأدبية، وأيضا في المادة الثامنة منها نصت على حماية المصنفات الرقمية التي تنشر على شبكة الإنترنت (79).

كما جاءت اتفاقية بودابست للجرائم الإلكترونية 2001 حيث اهتمت بجرائم الفضاء الإلكتروني ولا سيما الجرائم المرتكبة من خلال استخدام تكنولوجيا الاتصالات وخدمات الإنترنت مثل الجرائم المتعلقة بالمعاملات المالية غير المشروعة وانتهاك حقوق التأليف والنشر بالإضافة إلى تناولها للجرائم التي تنتهك كرامة الإنسان وخصوصيته (80).

وتضمنت اتفاقية بودابست العديد من صور الجرائم الإلكترونية بما في ذلك الجرائم المرتكبة ضد انتهاك العناصر الأساسية لأمن المعلومات وهي السرية وسلامة وتوافر البيانات، أي أن هذه الاتفاقية اهتمت بحماية أمن المعلومات وذلك عن طريق فرض الحماية على عناصرها أو ما يسمى بمثلث CIA.

فقد كانت أول التشريعات التي تستخدم مصطلح نظم الحساب الآلي Computer Systems ووضع تعريف مفصل له في نصوص الاتفاقية هو أي جهاز يقوم بالمعالجة التلقائية للبيانات أو مجموعة من الأجهزة المترابطة أو ذات صلة ببعضها البعض، وبهذا المفهوم فإن الاتفاقية قد شملت كل الأجهزة الرقمية بما فيها ما أطلق عليه فيما بعد بإنترنت الأشياء Internet of Things (IoT) (81).

بالإضـافة إلى اتفاقيـة بودابسـت فقـد أصـدر الإتحـاد الأوروبي تشريـع خـاص بـأمن الشـبكات والمعلومـات في عـام 2016 يسـمى بتوجيـه الاتحـاد الأوروبي لأمـن الشـبكات والمعلومـات Network and Information Security (NIS) Directive الـذي اهـتم بحماية عناصر أمن المعلومات CIA، ويعد أول تشريع على مستوى الإتحـاد الأوروبي بشـأن أمن الفضاء الرقمي الذي يحمل رقم 169 وتتمثل أهدافه في تحقيق الحد الأقصى من حمايـة البيئة الإلكترونية وتحديد العلاقة بين مزودي خدمات الإنترنت والمستخدمين وعلاقـتهما معـا بالأمن المعلوماتي على مستوى الإتحاد الأوروبي (82).

2. التدابير التشريعية الوطنية:

تم إحداث الهيئة الوطنية لخدمات الشبكة في سوريا بموجب القانون رقم /4/ تاريخ 2009/2/25، بهدف تنظيم وتنسيق وتسهيل العمل على الشبكة المعلوماتية.

وتعمل الهيئة بشكل أساسي على تنظيم خدمات التوقيع الإلكتروني، وإدارة أسماء النطاقات على الانترنت تحت النطاقين العلويين السوريين (sy., .سورية)، وتنظيم استخدام عناوين الإنترنت الرقمية (IPs) للشبكات الحاسوبية في سورية. وعلى كل مامن شأنه توفير بيئة تمكينية لتقديم خدمات إلكترونية متقدمة تساهم في نمو الاقتصاد الوطني.

ومن الأهداف العامة للهيئة الوطنية لخدمات الشبكة في سوريا ما يالي:

1. تنظيم نشاط خدمات التوقيع الإلكتروني وتسجيل أسماء النطاقات على الانترنت وغيرها من الأنشطة في مجال المعاملات الإلكترونية وخدمات الشبكة.
2. الإسهام في تطوير استخدام الخدمات الإلكترونية, ورفع كفاءة التعاملات التجارية والمالية على الشبكة.
3. الإسهام في الضبط والمراقبة لحالات الطوارئ على الشبكة.
4. المساهمة في رفع كفاءة تطبيق قواعد أمن وحماية الشبكات ومواقع الانترنت.
5. دعم البحوث والدراسات في مجال خدمات الشبكة وتشجيع الاستفادة من نتائجها.
6. نقل التكنولوجيا المتقدمة في مجال أمن المعلومات وتحقيق الاستفادة منها.
7. رعاية المصالح المشتركة للأنشطة المتعلقة بخدمات الشبكة.

ومن مهام الهيئة الوطنية لخدمات الشبكة في سوريا كل من ما يالي:

1. تحديد وضبط مواصفات المنظومات الخاصة بالتوقيع الإلكتروني، وتنظيم نشاطات تقديم خدماته ومنح التراخيص لمزاولة أعمال هده الخدمات.
2. إدارة النطاقات العلوية السورية (.sy و.سورية) على شبكة الإنترنت، وتحديد السياسات والقواعد الناظمة لتسجيل الأسماء تحت هذه النطاقات.
3. منح وإدارة التراخيص للمسجِّلين المخوّلين بتسجيل الأسماء تحت النطاقات العلوية السورية، والتحقق من التزامهم بالقواعد الناظمة لذلك.
4. وضع المواصفات والمعايير الخاصة بأمن وحماية الشبكات ومواقع الإنترنت، والإشراف على حسن الالتزام بها.
5. وضع المعايير الخاصة بمواجهة حالات الطوارئ على الإنترنت أو غيرها من الشبكات المعلوماتية والحاسوبية، والإشراف على حسن الالتزام بها، وتأليف فرق عمل للتصدي لهذه الحالات.
6. وضع النواظم والضوابط والمعايير الخاصة بعمل المواقع على الإنترنت أو غيرها من الشبكات المعلوماتية، والإشراف على حسن تطبيقها لدى أصحاب المواقع والجهات المستضيفة لها.
7. إدارة عمليات تخصيص عناوين الإنترنت في الجمهورية العربية السورية، والتنسيق مع السلطات الإقليمية والعالمية المختصة لأجل ذلك.
8. فض النزاعات بين المرخَّص لهم في مجالات عمل الهيئة عن طريق التحكيم، وفق القوانين والأنظمة النافذة.
9. التنسيق مع المنظمات الدولية المعنية بنشاطات الهيئة.
10. التدريب والتأهيل الاحترافي التخصصي في مجال تكنولوجيا المعلومات بشكل عام، وفي مجال أمن المعلومات وحماية الشبكات، ومراكز المعطيات بشكل خاص في القطاعين العام والخاص على حد سواء.

ويعتبر المرسوم التشريعي رقم 17 لعام 2012 - تطبيق أحكام قانون التواصل على الشبكة ومكافحة الجريمة المعلوماتية السوري من أحد التشريعات الوطنية في حماية جرائم تقنيات المعلومات وذلك لاشتماله على العديد من صور الجرائم التي تتم في بيئة الإنترنت والنص على العقوبات التي تقع على مرتكبي مثل هذه الجرائم وكذلك تحديد العلاقة التي تربط مزودي خدمات الإنترنت بالمستخدم لهذه الخدمة والتزامات كلا منهم حتى لا يقع تحت طائلة القانون.

تضمن القانون العديد من الصور للجرائم مثل الاعتداء على سلامة شبكات الإنترنت وتقنيات المعلومات وجرائم الدخول غير المشروع واعتراض البيانات بدون وجه حق، حيث نص في المادة 17 على عقوبة الحبس ثلاثة أشهر إلى سنتين والغرامة من مئة ألف إلى خمسمئة ألف ليرة سورية لكل من أعاق أو منع قصدا بأي وسيلة كانت الدخول إلى منظومة معلوماتية أو الشبكة أو عطلها أو أوقفها عن العمل أو أعاق أو منع قصدا باي وسيلة كانت الوصول إلى الخدمات أو البرامج أو المواقع الالكترونية أو مصادر البيانات أو المعلومات عليها (83).

بالإضافة إلى التأكيد على حماية عناصر أمن المعلومات CIA حيث نصت في المادة 18 /أ/ و /ب/ على العقوبة بالحبس من ثلاثة أشهر إلى سنتين والغرامة من مئة ألف إلى خمسمئة الف ليرة سورية كل من اعترض او التقط قصدا بوجه غير مشروع المعلومات المتداولة على منظومة معلوماتية أو الشبكة أو تنصت عليها و من شهر إلى ستة اشهر والغرامة من مئة ألف إلى خمسمئة الف ليرة سورية كل من استخدم الخداع للحصول على معلومات شخصية او سرية من المستخدمين على منظومة معلوماتية أو الشبكة يمكن استغلالها لأغراض إجرامية (84).

نشير إلى أن قوانين المعلوماتية والكمبيوتر والإنترنت السورية قد نصت على جرائم أخرى تهدد أمن المعلومات مثل جرائم الاعتداء على البريد الإلكتروني وجرائم الاعتداء على تصميم المواقع الإلكترونية وجرائم الاعتداء على الأنظمة المعلوماتية وتهديد سلامتها مع توقيع أقصى العقوبة على من قام بواحدة من تلك الجرائم سواء بالحبس أو بالغرامة المالية أو بإحدى العقوبتين.

5.1.2 المعايير الدولية لإدارة أمن المعلومات:

تعتبر المنظمة الدولية للتوحيد القياسي International Organization for Standardization (ISO) التي تعرف باسم منظمة الأيزو هي المنظمة التي تهتم بوضع المعايير الدولية لضبط أمن المعلومات بالمؤسسات والمنظمات، وهي منظمة تضم ممثلين من عدة منظمات قومية للمعايير وبالرغم من أنها منظمة غير حكومية إلا أن المعايير التي تقوم بوضعها تعتبر بمثابة قوانين واجبة التطبيق هذا ما يجعلها أكثر قوة من معظم المنظمات غير الحكومية (85) ، وتقع منظمة الأيزو في مدينة جنيف حيث تم تأسيسها عام 1946 وتضم أكثر من 145 بلد عضو منذ إنشاؤها، وبلغ عدد المعايير الدولية التي أصدرتها 19500 معيار (86) .

وترتكز المعايير الدولية على مجموعة من الإجراءات التي يقترح تطبيقها في مؤسسات المعلومات والاعتماد عليها، وأصدرت منظمة الأيزو العديد من المواصفات القاسية المتخصصة في

مجـال أمـن المعلومـات نـذكر منهـا معـايير ISO, MEHARI, ITIL, COBIT (87) ، وأهـم هـذه المعـايير التـي تسـمى بمواصـفات نظـم إدارة أمـن المعلومـات (ISO:27000)، وتتكون من ستة معايير فرعية، وهما كما يلي (88):

1. أيزو 27001: يشتمل على المعايير الخاصة بالاستمرار على تحسين الخدمات عن طريق وضع الأسس اللازمة لضبط ممارسات الأفراد في إدارة أمن المعلومات.
2. أيزو 27002: يعطي المبادئ والمعايير الخاصة بتنظيم وإدارة أمن المعلومات.
3. أيزو 27003: يوفر القواعد الخاصة بتنفيذ الإجراءات الإضافية الخاصة بأمن المعلومات.
4. أيزو 27004: يهتم توفير المقاييس الخاصة بقياس مدى فعالية تطبيق نظم إدارة أمن المعلومات من خلال مجموعة من الضوابط والمواصفات.
5. أيزو 27005: يوفر مجموعة من المقاييس الخاصة بإدارة المخاطر التي تهدد أمن المعلومات.
6. أيزو 27006: يقدم مبادئ وضوابط توجيهية للاعتماد بالمنظمات التي تقدم الشهادات الخاصة بالمصادقة على نظام إدارة أمن المعلومات .

نوضح فيما يلي أهم هذه المعايير وأكثرها تطبيقا في إدارة نظم أمن المعلومات وهما معياري الأيزو 27001 و27002 وذلك على النحو التالي:

1. المعيار الدولي لأمن المعلومات ISO 27001:

صدر هذا المعيار في عام 2005 وهو عبارة عن مجموعة من الإرشادات والإجراءات المتبعة لتطوير وتشغيل ومراقبة ومراجعة وتحسين نظام أمن المعلومات الموثق داخل المنظمة بهدف تحقيق الإدارة الفعالة والمستمرة للمخاطر التي تتعرض لها أمن المعلومات مع توفير الحماية المناسبة لها، وضمان وضع إطار رقابي حازم من خلال إنشاء نظام لإدارة المعلومات والالتزام بالمتطلبات التي يحققها (89).

يهدف هذا المعيار إلى تحديد الاحتياجات اللازمة لإقامة وتنفيذ وتشغيل واستراض وصيانة وتحسين نظام إدارة أمن المعلومات داخل المنظمات وعادة ما يصلح للتطبيق على جميع أنواع المنظمات بما في ذلك المنظمات ذات النشاط التجاري أو الأنظمة الحكومية بفروعها المختلفة، حيث يعتمد هذا المعيار على نموذج يعرف بدائرة ديمنج أو نموذج التحسين المستمر للأداء

Plan-Do-Check-Act (PDCA) الذي يتكون من أربعة مراحل متتالية تمثل أحد أهم آليات إدارة الأعمال وتطوير الجودة بالمؤسسات وهي (90):

خ. مرحلة التخطيط **Plan**: تأسيس نظام لإدارة أمن المعلومات.

د. مرحلة التنفيذ **Do**: تنفيذ الخطط وتشغيلها.

ذ. مرحلة التحقق **Check**: مراجعة النظام بعد تنفيذه وتشغيله.

ر. مرحلة العمل **Act**: صيانة وتحسين أداء وكفاءة النظام.

2. المعيار الدولي لأمن المعلومات ISO 27002:

يطلق على هذا المعيار " قواعد ممارسة إدارة أمن المعلومات " وهو أول معيار يصدر عن سلسلة معايير إدارة أمن المعلومات (أيزو 27000) الصادرة عن المنظمة الدولية للتوحيد القياسي، ويهدف هذا المعيار إلى توفير القواعد والمواصفات التي تضبط منهجية إدارة أمن المعلومات من خلال الاسترشاد بأفضل الممارسات الأمنية التي من شأنها أن تساعد في الوصول إلى الحد الأدنى لأمن المعلومات (91).

وصدر هذا المعيار في عام 2013 لمواكبة التطورات في أمن المعلومات وتكنولوجيا الاتصالات فهو يوفر إرشادات حول الممارسات الواجب إتباعها في اختيار وتنفيذ وإدارة أمن المعلومات حيث تم إعداده وتصميمة ليتم استخدامه كمرجع لمعرفة الإرشادات والإجراءات الواجب إتباعها لإدارة نظم أمن المعلومات إلى جانب المواصفات والخطوات الإرشادية الواردة بمعيار الأيزو 27001:2013 . (92)

الفصل الثالث

الإطار العملي للبحث

1.3 مقدمة عامة:

بعد الدراسة النظرية لنظام إدارة أمن المعلومات من حيث ماهيته، وطرق تطبيقه، والتعرف على عناصره، كان من الضروري استكمال العمل من خلال دراسة الواقع التطبيقي.

سيتم في هذا الفصل عرض أمثلة على بعض الاختراقات الأمنية من الفترة ما بين 2013 و 2019 و عرض ثلاثة عناصر أساسية تشمل أنواع الهجمات الإلكترونية التي يتعرض لها قطاع الخدمات والإتصالات بمافيها هجمات على خادم نظام أسماء النطاقات و هجمات طلب الفدية و هجمات حجب الخدمة وأخيراً هجمات الإحتيال على شركات الإتصالات ومن ثم الانتقال الى العنصر الثاني للحديث عن إحتماليات وقوع هذه الهجمات على قطاع الخدمات والإتصالات، كما تم التطرق في نهاية البحث على تكلفة وخسائر قطاع الخدمات والإتصالات من هذه الهجمات الإلكترونية. كما سيتم عرض أهم نتائج دراسة تكلفة خرق البيانات السنوي لعام 2020 الصادر من معهد بونيمون وأمن آي بي أم في الولايات المتحدة الأمريكية.

ونظرًا لمحدودية توافر البيانات و المعلومات، ووجود ممارسات عدة معيقة للحصول على بيانات ذات صلة في الجمهورية العربية السورية، لم يكن من الممكن تنفيذ دراسات أو إحصائيات رقمية توضح واقع تطبيق إدارة أمن المعلومات على قطاع الخدمات والإتصالات في سورية.

أمثلة على بعض الاختراقات الأمنية من الفترة ما بين 2013 و 2019 (93):

- **Equifax** - في عام 2017، تسببت إحدى الثغرات في تطبيق موقع إلكتروني في فقدان الشركة للبيانات الشخصية لعدد 145 مليون أمريكي. وشملت تلك البيانات أسماءهم وأرقام ضمانهم الاجتماعي وأرقام رخص القيادة. وقد تمت الهجمات على مدى ثلاثة أشهر من مايو إلى يوليو، ولكن لم يتم الإعلان عن الاختراق الأمني قبل شهر سبتمبر.
- **Yahoo** - تم اختراق 3 مليارات حساب من حسابات المستخدمين في عام 2013 بعد محاولة تصيّد احتيالي منحت المخترقين إمكانية الوصول إلى الشبكة.
- شهد موقع **eBay** اختراقًا كبيرًا في عام 2014. على الرغم من أن معلومات البطاقات الائتمانية لمستخدمي **PayPal** لم تتعرض للخطر، إلا أن العديد من كلمات مرور العملاء قد تعرضت للاختراق. ثم تصرفت الشركة بسرعة وأرسلت رسالة عبر البريد الإلكتروني إلى مستخدميها وطلبت منهم تغيير كلمات مرورهم من أجل الحفاظ على أمانهم.

- تعرض موقع المواعدة **Ashley Madison**، الذي روّج لنفسه بين المتزوجين الذين يرغبون في المواعدة الغرامية، للاختراق في عام 2015. حيث سرّب المخترقون عددًا كبيرًا من بيانات العملاء عبر الإنترنت. ثم بدأ المبتزون في استهداف العملاء الذين تم تسريب أسمائهم؛ وربطت تقارير غير مؤكدة بين عدد من حالات الانتحار والتعرض لاختراق البيانات.
- شهد موقع **Facebook** عيوبًا برمجية داخلية أدت إلى فقد البيانات الشخصية لعدد 29 مليون مستخدم في عام 2018. وقد كان هذا اختراقًا أمنيًا محرجًا بشكل خاص لأن الحسابات المخترقة تضمنت حساب الرئيس التنفيذي للشركة مارك زوكربيرج.
- أعلنت فنادق **Marriott** عن تعرضها لاختراق أمني واختراق للبيانات أثر على ما يصل إلى 500 مليون سجل للعملاء في عام 2018. وبالرغم من أن اختراق نظام حجوزات النزلاء حدث في عام 2016، لم يتم اكتشاف الاختراق إلا بعد مرور عامين.
- كشفت شركة **Avast** التشيكية عن تعرضها لاختراق أمني في عام 2019 عندما تمكن أحد المخترقين من اختراق بيانات اعتماد شبكة VPN لأحد الموظفين. لم يشكل هذا الاختراق تهديدًا لبيانات العميل، بل كان يهدف إلى إدخال البرامج الضارة في منتجات Avast.

1.1.3 أنواع الهجمات الإلكترونية:

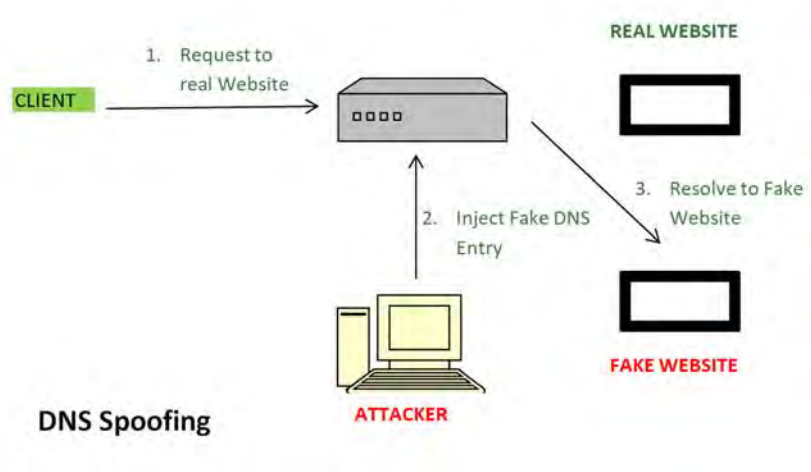
وهناك العديد من الهجمات الإلكترونية التي يتعرض لها قطاع الخدمات والإتصالات على مدار الساعة ولقد تم إختيار أخطر وأهم اربعة أنواع من هذه الهجمات وهي على النحو التالي:

هجمات على خادم نظام أسماء النطاقات - DNS-attacks:

تمثّل إفساد خادم نظام أسماء النطاقات (DNS) أو تزويره أحد أنواع الهجوم الإلكتروني الذي يعمل على استغلال ثغرات النظام في خادم أسماء المجالات لتحويل حركة المرور عن الخوادم الشرعية وتوجيهها نحو خوادم مزيفة.

يتم العثور غالبًا على التعليمات البرمجية الخاصة بإفساد ذاكرة التخزين المؤقت لخادم أسماء النطاقات (DNS) في عناوين المواقع المرسَلة عبر رسائل البريد الإلكتروني العشوائية. تحاول رسائل البريد الإلكتروني هذه إرغام المستخدمين على النقر فوق عنوان الموقع المتوفر، مما يؤدي بدوره إلى إصابة الحاسوب. ويمكن أيضًا لإعلانات الشعارات والصور، الموجودة في كل من رسائل البريد الإلكتروني ومواقع الويب غير الموثوق فيها، توجيه المستخدمين إلى هذه التعليمات البرمجية. وبمجرد إفسادها،

سيقوم حاسوب المستخدم بنقله إلى مواقع الويب المزيّفة التي تم تزويرها لتبدو مثل مواقع ويب حقيقية، مما يُعرّضه لمخاطر مثل برامج التجسس أو مسجلات لوحة المفاتيح أو الفيروسات المتنقلة.



شكل (5)

وهجمات DNS Cache Poisoning واحد من الهجمات المتكررة ويسمى كذلك DNS Spoofing ، حيث يُجبر المستخدم على الانتقال لموقع مزيف احتيالي شبيه بالموقع الأصلي بقصد تحويل حركة المرور والحصول على بيانات الاعتماد للمستخدمين كما هو موضح بالشكل رقم (5).

هجمات طلب الفدية - Ransomware:

هجمات طلب الفدية هي نوع من البرمجيات الخبيثة المصممة لمنع الضحايا من الوصول إلى الملفات، وبتشفير بيانات الضحية ما لم يدفع لها فدية لفك تشفيرها، على الرغم من عدم وجود ضمان باستعادة الوصول لهذه الملفات.

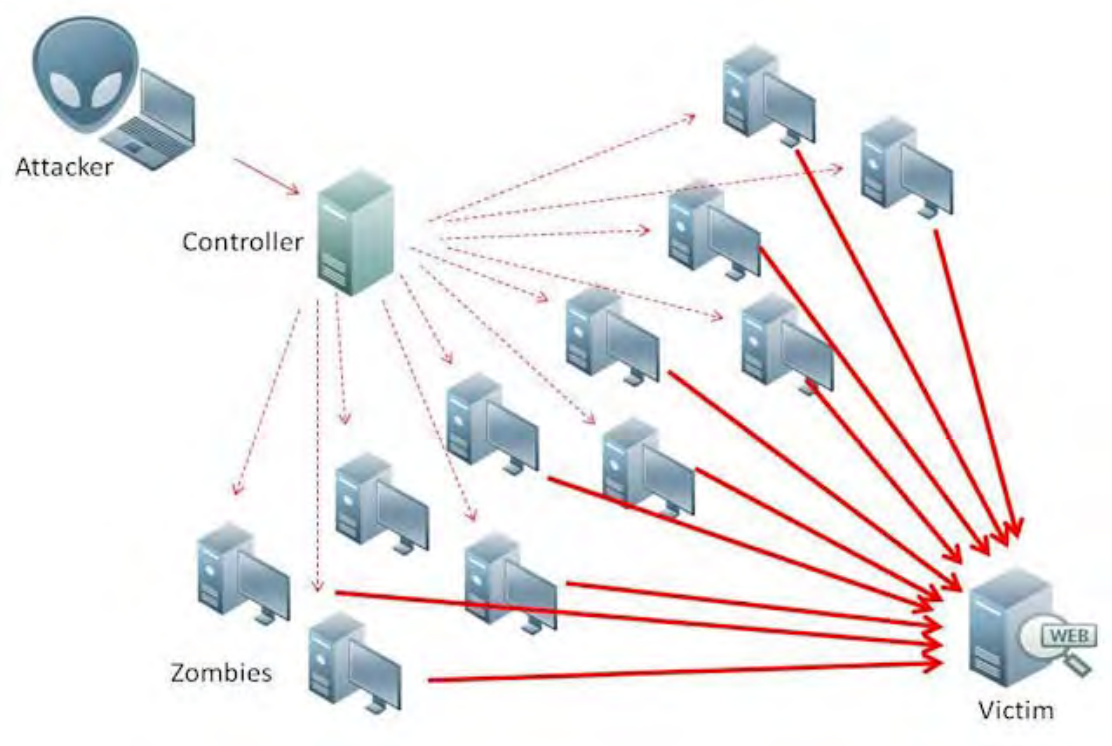
شكل (6)

الجدير بالذكر أن هذا النوع من الهجمات يتزايد باستمرار، حيث ويضح التقرير السنوي للجرائم الإلكترونية لعام 2019 الذي أصدرته شركة (Cybersecurity Ventures)، بأن الشركات التجارية وقعت ضحية لهجوم الفدية كل 14 ثانية في عام 2019، وستقع كل 11 ثانية بحلول عام 2021.

هجمات حجب الخدمة - DDoS:

يعمل هجوم حجب الخدمة (DDoS) على تعطيل مواقع الويب عن طريق غمر نظام أو خادم أو شبكة بطلبات وصول بشكل أكبر مما يمكنها التعامل معه.

وتخدم هجمات DDoS عادةً أحد الغرضين: حيث إنها قد تكون عمل انتقامي ضد شركة، أو عملية إلهاء تسمح للقراصنة باختراق النظام بينما يركز مسؤولي أمن المعلومات على استعادة الموقع.



شكل (7)

وكما يوضح الشكل (7) هي هجمات تتم عن طريق إغراق المواقع بسيل من البيانات غير اللازمة يتم إرسالها عن طريق أجهزة مصابة ببرامج (DDOS Attacks) تعمل على نشر هذ الهجمات بحيث يتحكم فيها القراصنة والعابثين الإلكترونيين لمهاجمة الشبكة (الإنترنت) عن بعد بإرسال تلك البيانات إلى المواقع بشكل كثيف مما يسبب بطء الخدمات أو زحاماً مرورياً بهذه المواقع ويسبب صعوبة

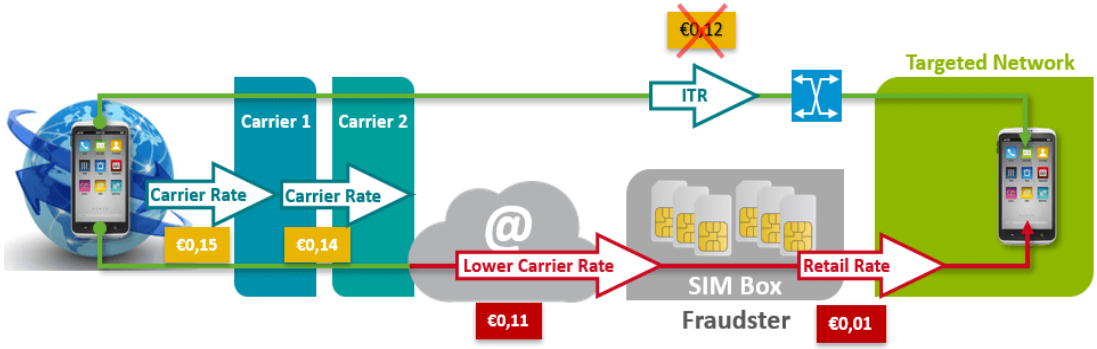
وصول المستخدمين لها نظراً لهذا الزحام وخصوصاً أنه يبدو، وباعتراف الكثير من خبراء الأمن على الشبكة، وكأنه لا يوجد علاج في الوقت الحالي لهذا الأسلوب في الهجوم على مواقع الشبكة (الإنترنت) ، وعلى هذا الأساس فإن هذا النوع من الهجمات يُدعى في بعض الأوساط "بإيدز الإنترنت".

هجمات الإحتيال على شركات الإتصالات - Telecom fraud:

من أحد أهم أنواع هجمات الإحتيال على شركات الإتصالات هو صندوق الSIM (SIM Boxing) حيث يتم إعادة التوجيه غير القانوني للمكالمات الصوتية الدولية من قبل كيانات غير مصرح لها باستخدام أجهزة بوابة GSM وبطاقات SIM محلية لإنهائها كمكالمات دولية.

كل عام ، يعاني المشغلون حول العالم من خسائر فادحة بسبب صناديق SIM أو بوابات GSM التي تتجاوز الاتصالات البينية الرسمية ، مما يتسبب في خسارة الملايين من دقائق البيع بالجملة.
حيث لا تقتصر المشكلة على الخسائر المالية المباشرة فقط. كل مكالمة يتم تجاوزها تقوض جودة الخدمة والخبرة. في الوقت الحاضر ، تعد فرص عدم رد المشتركين على المكالمات الهاتفية عندما لا يتم التعرف على CLI (هوية الخط المتصل) الوارد عالية.

وتعد نسبة الرد على الاستيلاء (قياس جودة الشبكة ومعدلات نجاح المكالمات) (Answer-Seizure ASR - Ratio) لمكالمات صندوق SIM أقل من المكالمات العادية. إذا تلقيت مكالمة مع CLI (هوية الخط المتصل) غير صحيح ، فلن تعرف بالطبع من اتصل بك ، وبالتالي لا يمكنك معاودة الاتصال به.



شكل (8)

بالإضافة الى أن جودة الصوت في مكالمات صندوق SIM رديئة للغاية ، ووقت إعداد المكالمة أطول ومعدل نجاح المكالمة أقل بكثير. ناهيك عن أن خصوصية اتصالاتك ستنتقل عبر أيدي المحتالين / مشغلي أجهزة SIM.

2.1.3 إحتماليات وقوع الهجمات:

لقد أصبحت الهجمات الإلكترونية بديلاً عن الحروب التقليديّة وغالباً تكون القطاعات المستهدفة هي القطاعات و المجالات الحاوية على معلومات مهمة و قيمة للغاية ، على سبيل المثال لا الحصر قطاع الخدمات والإتصالات ، فقد زادت في الآونة الأخيرة عدد الهجمات الكترونية على قطاع الخدمات و الاتصالات دولياً بصفة عامة و في الجمهورية العربية السورية بصفة خاصة و ذلك لاحتوائها على معلومات حساسة للغاية مثل البيانات الشخصية للمشتركين بالإضافة لأماكن تواجدهم مما يسهل إمكانية مراقبتهم و نقل هذه المعلومات لجهات خارجية ، وبالرغم من كل الإجراءات الأمنية المكثفة ، لا توجد هناك حماية من الهجمات الإلكترونية بنسبة 100%.

إن احتمالية حدوث هجمات على خوادم نظم أسماء النطاقات - DNS-Attacks حسب التقرير المذكور في الدراسة EfficientIP تصل إلى 43% من شركات الاتصالات خلال فترة 12 شهر الماضية مع ملاحظة أنه 81% تطلب أكثر من ثلاثة أيام لتطبيق إجراءات حماية هذه القطاعات بعد إدراك الهجوم(93).

أما هجمات طلب الفدية ، فقد كشفت إحدى الجهات المتخصصة في مكافحة الهجمات الإلكترونية، بأن نسبة ارتفاع هجمات طلب الفدية على الشرق الأوسط خلال العام 2018 بلغت 378%.

وبحسب الدراسة الحديثة التي أجرتها شبكة كاسبرسكي الأمنية بعنوان "أمن تقنية المعلومات: نفقاتٌ على مركز التكلفة أم استثمار استراتيجي" أن حادث اختراق واحد للبيانات يمكن أن يكبّد الشركات في منطقة الشرق الأوسط وتركيا وإفريقيا خسائر بحوالي مليون دولار. وتفيد الدراسة بأن الشركات الإقليمية أصبحت الآن تولي الإنفاق على أمن تقنية المعلومات اهتماماً أكبر، ومن المتوقع أن تُخصّص ما يصل إلى 27% من موازنات تقنية المعلومات لهذا الجانب الحيوي(94).

أما فيما يتعلق بهجمات حجب الخدمة (DDoS) ، وهو هجوم إلكتروني يمنع المستخدمين من الدخول إلى النظام لفترة من الزمن ، فقد ازدادت احتمالية هجمات حجب الخدمة (DDoS) لمنع مواقع لجهات مهمة و كبيرة من الدخول إليها من قبل العملاء والشركاء والمستخدمين لساعات أو أيام، مما أدى إلى خسائر مالية كبيرة، والإضرار بسمعتها، بالإضافة إلى خسائر أخرى.

فوفقاً لدراسة أجرتها جريدة (الخليج) الاماراتية فقد ارتفع في الربع الثاني من عام 2019 إجمالي عدد هجمات حجب الخدمة الموزعة (DDoS) بنسبة 18%، مقارنة بالفترة نفسها من عام 2018.

وأظهرت الهجمات التي تستهدف مستوى التطبيقات و من ضمنها تطبيقات الاتصالات، والتي يصعب تنظيمها والحماية منها، نمواً ملحوظاً، فارتفع مقدارها بنحو الثلث (32%)، مقارنة بالربع الثاني من 2018. ونتيجة لذلك، فإنها تشكّل الآن ما يقرب من نصف (46%) جميع الهجمات التي تمنعها خدمة (كاسبرسكي) للحماية من هجمات حجب الخدمة (Kaspersky DDoS Protection) (95).

وأخيراً هجمات الإحتيال على شركات الإتصالات، إن هذا النوع من الهجمات مستمر وتصل نسبة تعرض قطاع الإتصالات لهذا النوع من الهجمات وخصوصاً في منطقة الشرق الأوسط وأفريقيا الى نسبة عالية بسبب التطور المستمر في تكنولوجيا المعلومات وعدم مواكبة قطاعي الخدمات و الإتصالات بنفس سرعة تطور المعلومات.

3.1.3 تكلفة وخسائر الهجمات:

تسببت الهجمات الإلكترونية وعمليات القرصنة التي اجتاحت العديد من دول العالم في أن يقفز حجم الإنفاق على أمن المعلومات إلى نحو 96.3 مليار دولار خلال العام الماضي فقط بزيادة بلغت نسبتها نحو 8% عن حجم الإنفاق خلال العام قبل الماضي.

وتشير التقارير إلى أن متوسط تكلفة خرق البيانات الواحد في عام 2020 يتجاوز 150 مليون دولار، ومع زيادة مستوى الاتصال بين المزيد من عناصر البنية التحتية للأعمال، فإنه من المتوقع أن تكلف الجرائم الإلكترونية الشركات أكثر من 2 تريليون دولار خلال عام 2019 (96).

هجمات على خادم نظام أسماء النطاقات - DNS-A ttacks:

استنادًا إلى دراسة استقصائية أجرتها شركة TechRepublic شملت 900 مهنة تقنية عبر أمريكا الشمالية وأوروبا وآسيا والمحيط الهادئ ، وجد "تقرير تهديدات DNS العالمية لعام 2020" أن 79٪ من المنظمات تعرضت لهجمات DNS في عام 2019 ، بانخفاض طفيف عن 82٪ في 2018.

كان متوسط الهجمات على المنظمات في العم الماضي 9.5 هجمات ، مما أدى إلى متوسط تكلفة حوالي 924،000 دولار لكل هجوم (97).

وذكر Nick Ismail في دراسة بعنوان "تكافح شركات الاتصالات للتخفيف من تهديدات الهجمات الإلكترونية" أن بشكل عام ، تستغرق شركات الاتصالات وقتًا طويلاً للتخفيف من أي هجوم ؛ تتطلب متوسط ثلاثة موظفين ليقضوا بشكل جماعي أكثر من 17 ساعة لكل هجوم. ووجد التقرير أن متوسط

التكلفة لكل هجوم DNS آخذ في الارتفاع لقطاع الاتصالات. في العام الماضي ، كلف هجوم DNS واحد مؤسسة اتصالات 622،100 دولار. يُظهر البحث هذا العام أن شركات الاتصالات تخسر في المتوسط 886،560 دولارًا من كل هجوم DNS ، بزيادة قدرها 42٪ في 12 شهرًا فقط (98).

هجمات طلب الفدية - Ransomware:

تتفاقم مشكلة هجمات طلب الفدية Ransomware أكثر وأكثر، حيث تجاوزت المبالغ المدفوعة من قبل الشركات والأفراد أكثر من 25 مليون دولار على مدى العامين الماضيين في محاولة لاستعادة البيانات الحاسوبية الخاصة بهم مرة أخرى من المتسللين الذين عملوا على تشفيرها، وذلك وفقاً لبحث جديد أعدته شركة غوغل حول هذه الظاهرة، وتستعمل هذه الهجمات البرمجيات التي تصيب أجهزة حواسيب الهدف، وتعمل على تشفير كافة الملفات بحيث يفقد الضحايا الوصول إليها (99).

كما توقع تقرير صادر عن المنتدى الاقتصادي العالمي، أن تصل كلفة هجمات الفدية عالمياً إلى 20 مليار دولار بحلول 2021. وأضاف التقرير الذي يرصد مخاطر (كوفيد-19)، أن 50% من الشركات قلقة من تزايد الهجمات الإلكترونية عليها، خاصة في ظل التحول الكبير لمنظومة العمل عن بُعد، حيث استغل المهاجمون السيبرانيون جائحة كورونا كنافذة هجمات جديدة حدّثوا من خلالها أدواتهم التخريبية.

وعلى المستوى العالمي شهدت الشركات ارتفاعاً بنسبة 148% في هجمات برامج الفدية، مع استهداف كبير لقطاعي التمويل والرعاية الصحية، مع زيادة محتملة للتهديدات السيبرانية خلال الفترة المقبلة.

وشدد الدليل الإرشادي المشترك الصادر حديثاً من (W7Worldwide) للاستشارات الاستراتيجية والإعلامية، وفيرتشوبورت المتخصصة في حلول الأمن السيبراني، على أهمية استعداد الشركات بخطط اتصال استباقية لمواجهة أزمات الهجمات السيبرانية، خاصة أن الجائحة أسهمت في تسريع وتيرة الأعمال نحو التحول الرقمي.

واستعرض الدليل الإرشادي المعنون بـ (الاستراتيجيات الاتصالية الفعالة لمواجهة التهديدات السيبرانية) 7 خطوات رئيسية لمساعدة الشركات ومؤسسات القطاع العام على تخطي هذه الأزمات، وأكد أهمية تمتع القطاعات المستهدفة بالقدرة الكبيرة لحماية بيانات العملاء والموظفين وسمعتها المؤسسية من تداعيات تلك التهديدات (100).

هجمات حجب الخدمة الموزعة - DDoS:

توصلت نتائج استطلاع أجرته شركة كاسبرسكي لاب وB2B International، قد يتسبب هجوم واحد من هجمات حجب الخدمة الموزعة DDoS على موارد إحدى الشركات على الإنترنت في خسائر كبيرة تتراوح في المتوسط ما بين 52,000 دولار أميركي إلى 444,000 دولار أميركي اعتمادا على حجم الشركة.

وأكدت كاسبرسكي لاب أن هذه النفقات تُلحِق أضرارا بالغة بالميزانية العمومية بالنسبة للعديد من الشركات، بالإضافة إلى الإضرار بسمعتها نتيجة فقدان القدرة على الوصول إلى موارد الشركاء والعملاء عبر الإنترنت. كما أن التكاليف الإجمالية تعكس العديد من المشكلات التي تواجهها الشركات بعد التعرض لهجوم DDoS (101).

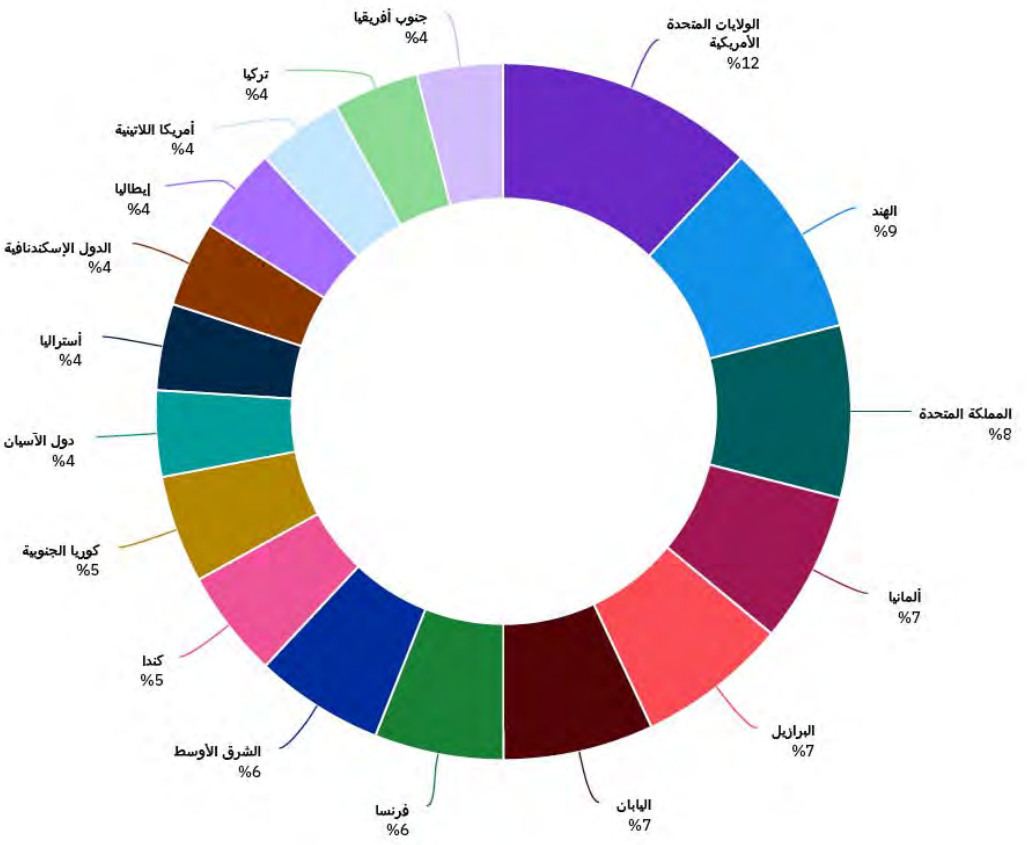
هجمات الإحتيال على شركات الإتصالات - Telecom fraud:

من أخطر أنواع هجمات الإحتيال على شركات الإتصالات هو ما يعرف بهجمات صندوق ال SIM (SIM Boxing) حيث تشير التقارير إلى أن مشغلي الهاتف المحمول والحكومات يخسرون ما يصل إلى 150 مليون دولار أمريكي كل عام للمحتالين الذين يقومون بإنهاء المكالمات الدولية بشكل غير قانوني كمكالمات محلية. هذا هو الصداع الجديد الذي يواجهه مشغلو الهواتف المحمولة الآن ، وهو أمر قد يحد من تطورات صناعة الهاتف المحمول في إفريقيا (102).

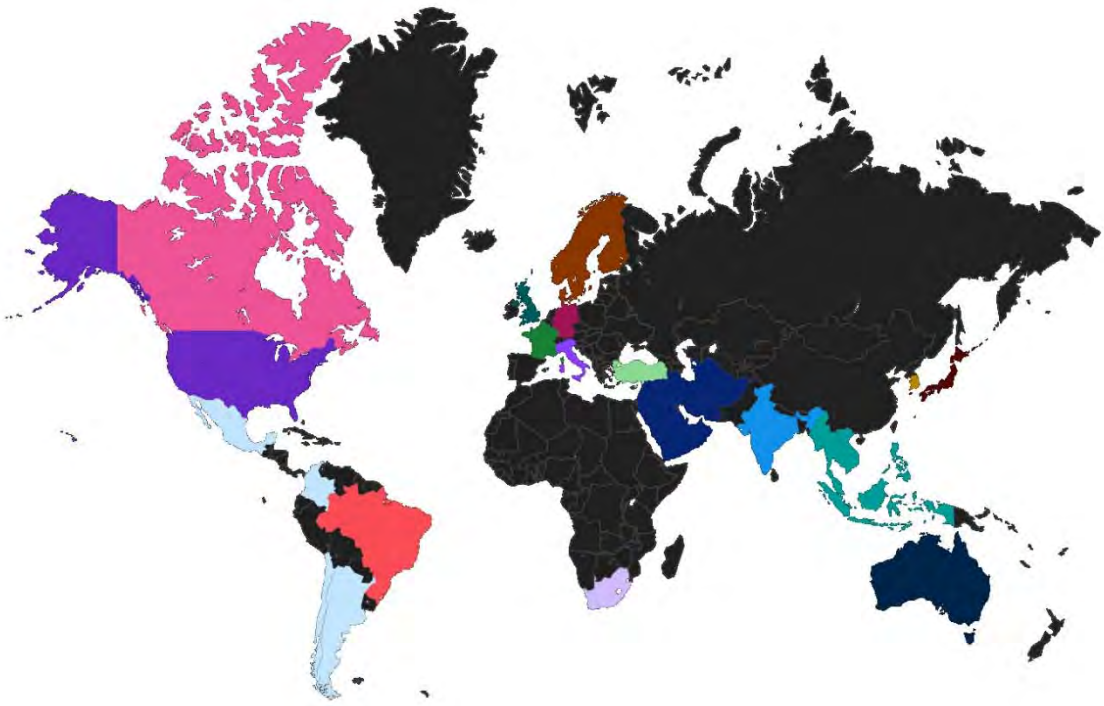
4.1.3 دراسة تكلفة خرق البيانات السنوي لعام 2020 (103):

أصدر معهد بونيمون ذ م م تقريره السنوي عن تكلفة خرق البيانات الذي يصدر بالاشتراك بين معهد بونيمون وأمن آي بي أم. أجرى البحث بشكل مستقل معهد بونيمون، ويتم رعاية النتائج وتحليلها والإبلاغ عنها ونشرها من قبل أمن آي بي إم. حيث تضمنت دراسة هذا العام 524 مؤسسة من مختلف الأحجام، تم أخذ عينات منها عبر مجموعة متسعة من المناطق الجغرافية والصناعات. أجريت دراسة 2020 على عينات من 17 دولة أو إقليمية و 17 مجال.

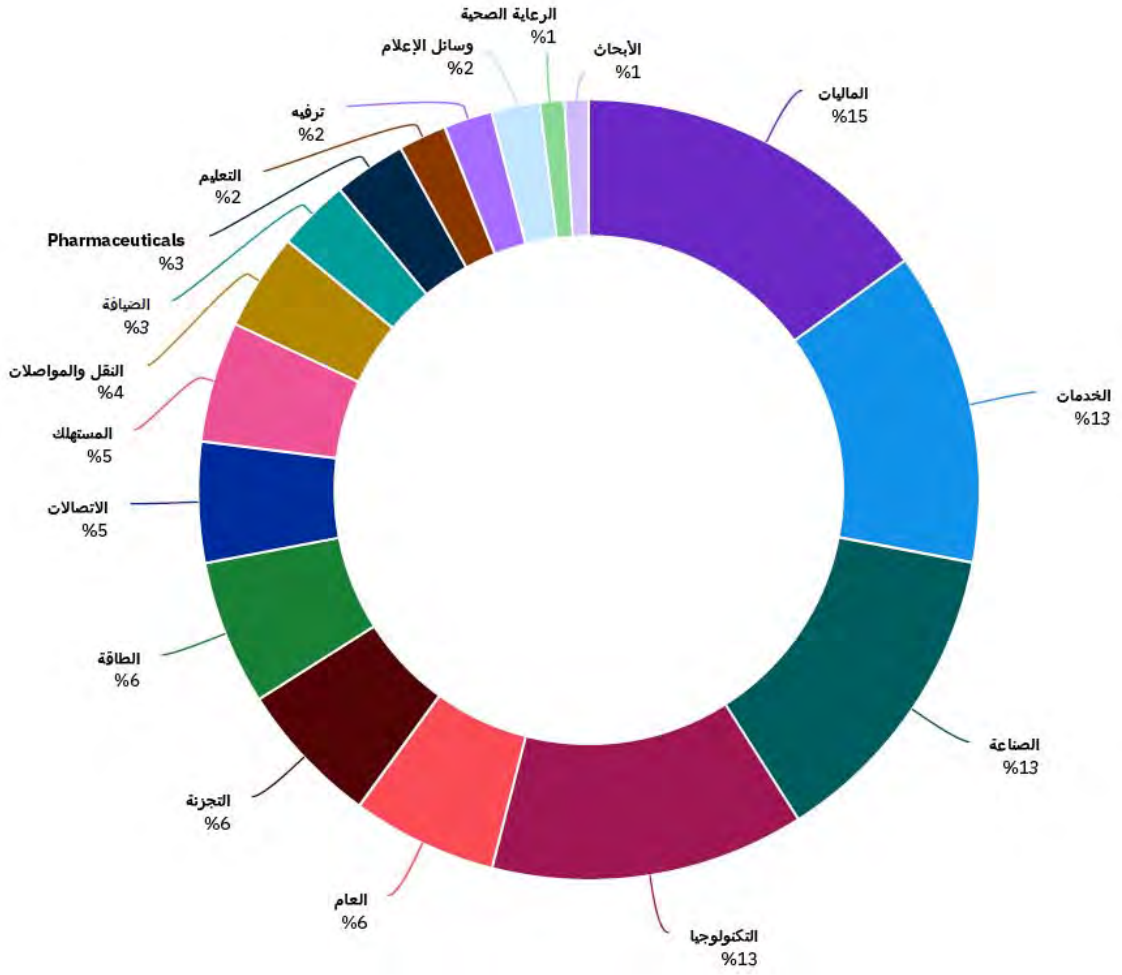
وغطت هذه الدراسة بلدان أو أقاليم من القارات الستة. شكل رقم 9 يوضح توزيع المؤسسات المرجعية حسب البلد أو الإقليم. حصلت الولايات المتحدة على أعلى تمثيل بنسبة 12 %، تليها الهند بنسبة 9%، والمملكة المتحدة بنسبة 8%. البلدان/الأقاليم ذات التمثيل الأقل كانت الآسيان وأستراليا والدول الاسكندنافية وإيطاليا وأمريكا اللاتينية وتركيا وجنوب إفريقيا.


الولايات المتحدة الأمريكية
%12
الهند
%9
المملكة المتحدة
%8
ألمانيا
%7
البرازيل
%7
اليابان
%7
فرنسا
%6
الشرق الأوسط
%6
كندا
%5
كوريا الجنوبية
%5
دول الآسيان
%4
أستراليا
%4
الدول الإسكندنافية
%4
إيطاليا
%4
أمريكا اللاتينية
%4
تركيا
%4
جنوب أفريقيا
%4

شكل (9)



ولقد تم جمع البيانات من خلال مقابلة 3200 شخص، كل على حدة في 524 مؤسسة عانت من خرق البيانات ما بين شهر أغسطس 2019 وإبريل من عام 2020 . بدأت مؤسسات التوظيف في أكتوبر2019 وانتهت المقابلات في 21 أبريل 2020 . شمل من أجريت معهم المقابلات متخصصون في تكنولوجيا المعلومات والامتثال وأمن المعلومات ممن هم على علم بخرق بيانات مؤسساتهم والتكاليف المرتبطة بحل الخرق. ولأغراض الخصوصية لم تجمع معلومات خاصة بالمؤسسة ذات الصلة ووزعت العينات حسب المجالات والتي شملت 17 مجالا كما هو موضح بالشكل رقم 10.



شكل (10)

ولحساب متوسط تكلفة خرق البيانات فلقد تم جمع كل من النفقات المباشرة وغير المباشرة التي تكبدتها المؤسسة. تشمل النفقات المباشرة الحصول على خدمات خبراء الطب الشرعي وتعهيد الدعم من خلال الخط الساخن وتوفير بطاقات ائتمان مجانية وخصومات على المنتجات والخدمات المستقبلية. تشمل

التكاليف غير المباشرة التحقيقات والاتصالات الداخلية، بالإضافة إلى قيمة خسارة العميل نتيجة التحولات أو انخفاض معدلات اكتساب العملاء.

واقتصر هذا البحث على عرض الأحداث المرتبطة بخرق البيانات مباشرة فقط. على سبيل المثال، قد تشجع اللوائح الجديدة كاللائحة العامة لحماية البيانات وقانون خصوصية المستهلك في كاليفورنيا المؤسسات على زيادة الاستثمارات في تقنيات حوكمة أمنها الإلكتروني، لكن دون التأثير على تكلفة خرق البيانات كما هو وضح في هذا البحث.

لتحقيق الاتساق مع السنوات السابقة استخدمت نفس طريقة تحويل العملات بدلاً من تعديل تكاليف المحاسبة.

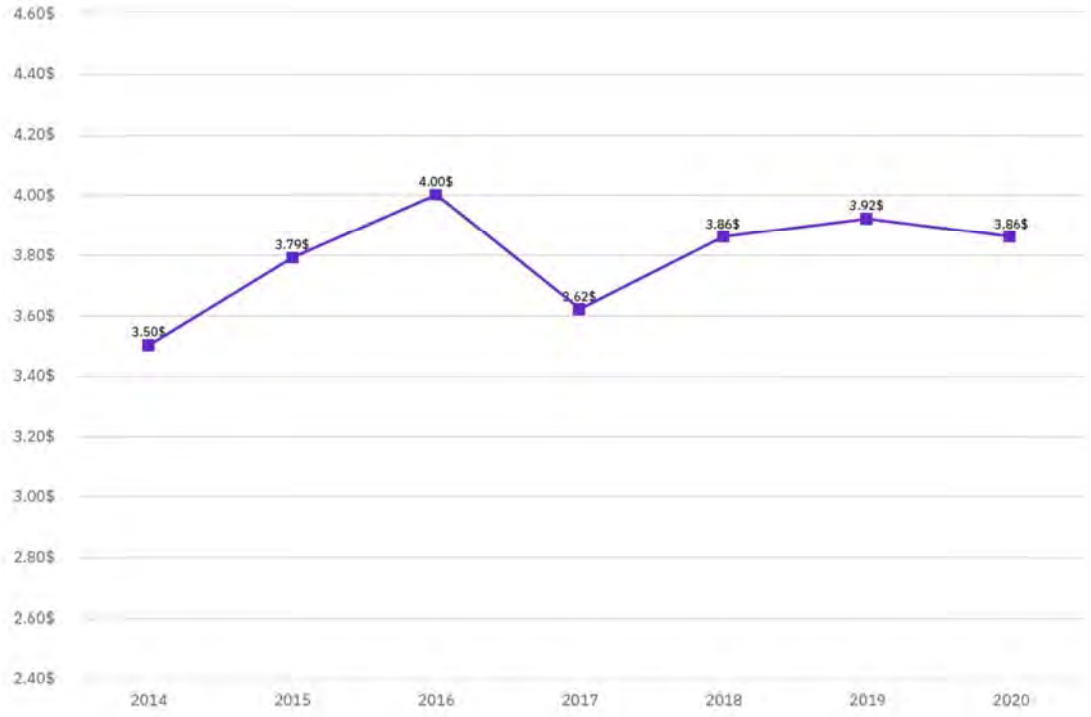
وتم إعتماد مصطلح خرق البيانات ليشمل حادث يعرض اسم الفرد وسجله الطبي أو المالي أو بطاقته الائتمانية للخطر - سواء بنسخة ورقية أو إلكترونية. وتراوحت السجلات المخترقة الواردة في هذه الدراسة ما بين 3400 إلى 997300 سجل.

واما مصطلح السجل فهو معلومات تعرف الشخص الطبيعى (الفرد) والتى تعرضت معلوماته للفقد أو السرقة نتيجة لخرق البيانات. ومن الأمثلة على ذلك قاعدة بيانات باسم الفرد ومعلومات بطاقته الائتمانية والبيانات التعريفية الشخصية الأخرى أو سجل طبي مثبت به اسم صاحب الوثيقة وبيانات الدفع.

فيما يلي ملخص للنتائج المفصلة لهذه الدراسة:

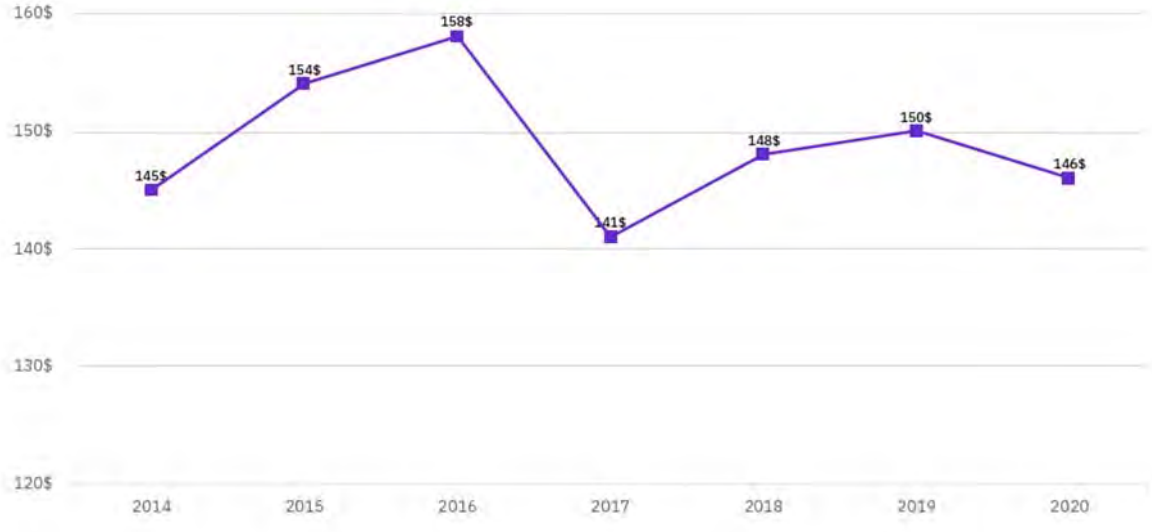
1 .النتائج العامة والمميزات

ارتفع إجمالي متوسط التكلفة لخرق البيانات بنسبة 10 ٪ منذ عام 2014 . شكل رقم 11 يُظهر هذا الشكل المتوسط العالمي للتكلفة الإجمالية لخرق البيانات على مدار 7 سنوات. كان إجمالي متوسط التكلفة المجمعة في دراسة عام 2020 3.86 مليون دولار، بانخفاض طفيف عن 3.92 دولار في عام 2019 . المتوسط المرجح 3.79 مليون دولار على مدار سبع سنوات.



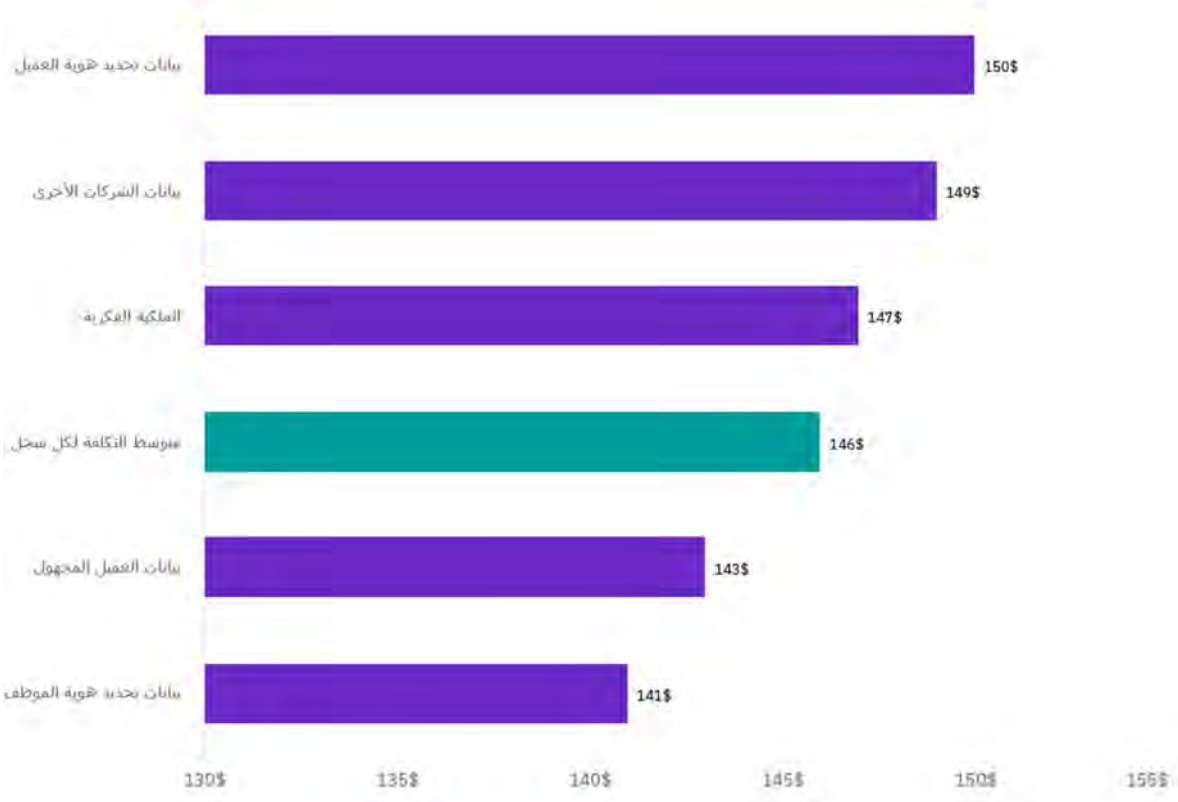
شكل (11)

حيث انخفضت تكلفة خرق للبيانات لكل سجل بشكل طفيف إلى 146 دولارًا. شكل رقم 12 يوضح متوسط تكلفة خرق البيانات للسجل المخترق على مدار السنوات السبع الماضية. المتوسط المرجح على مدار سبع سنوات هو 149 دولارًا لكل سجل.



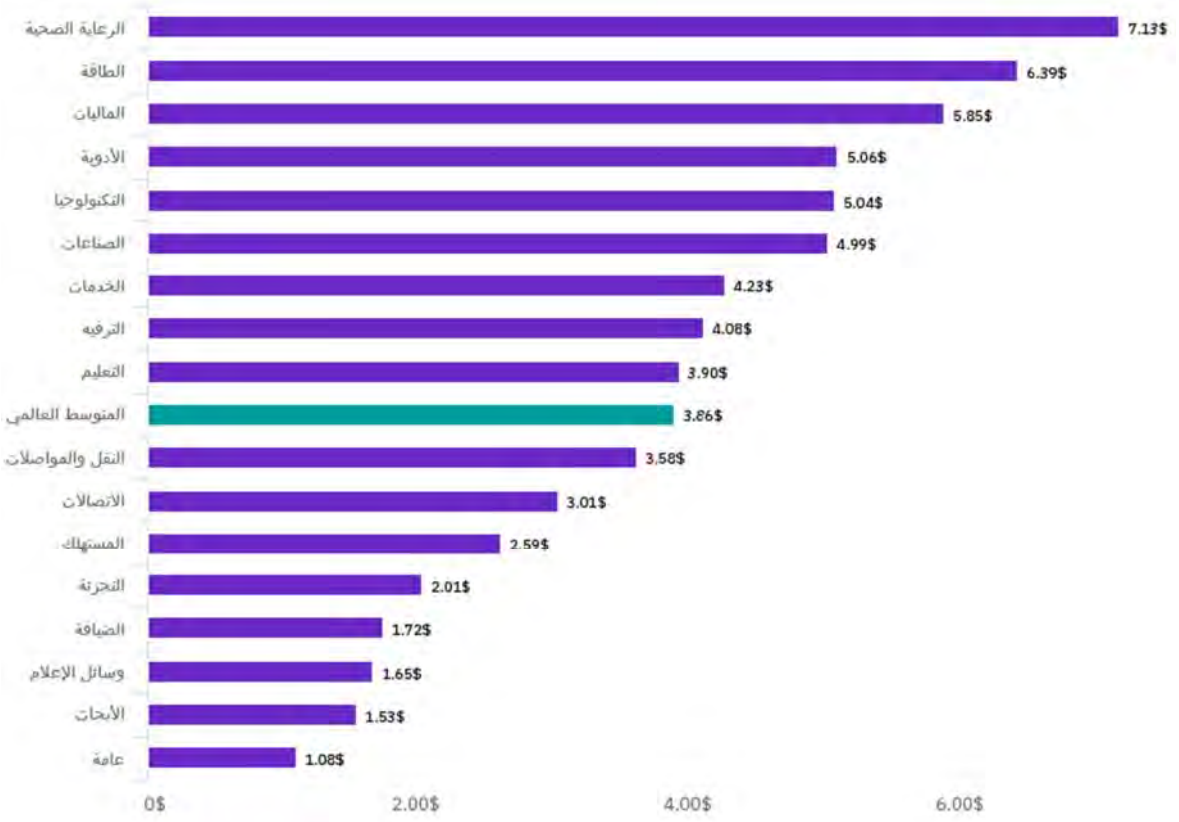
شكل (12)

أما متوسط تكلفة السجل حسب نوع البيانات المخترقة فكانت بيانات تحديد هوية العميل هي النوع لأكثر تكلفة من البيانات المعرضة للخرق نتيجة للخروقات. تكلفة البيانات الشخصية للعميل في المتوسط كانت 150 دولارًا لكل سجل مفقود أو مسروق، كما هو موضح في شكل رقم 13. الملكية الفكرية تكلف 147 دولارا للسجل، بينما تكلف بيانات العملاء المجهولين (بيانات تحديد الهوية الشخصية المجهولة) 143 دولارًا لكل سجل، وتكلفة بيانات تحديد الهوية الشخصية للموظفين 141 دولارًا لكل سجل.



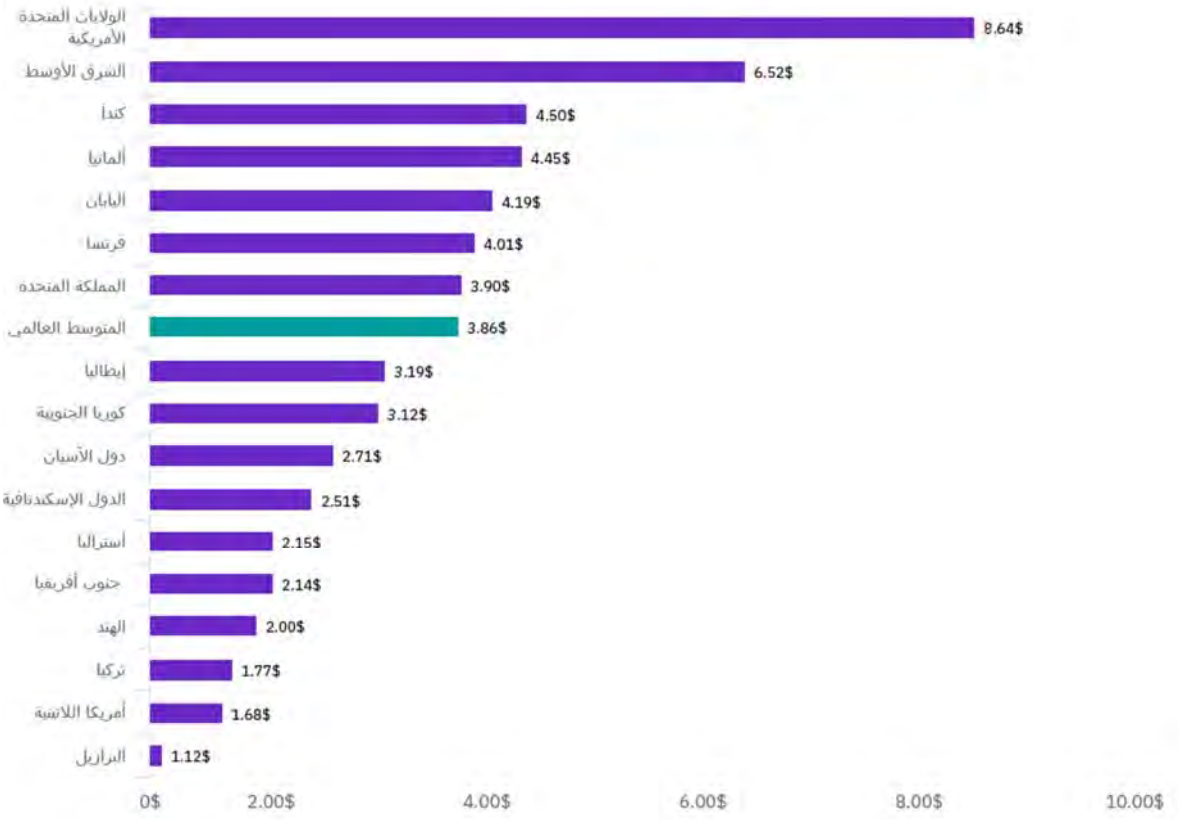
شكل (13)

وكان إجمالي متوسط تكلفة خرق البيانات حسب المجال موضح بالشكل رقم 14 حيث شهدت مجالات الرعاية الصحية والطاقة والخدمات المالية و المجالات الدوائية والتكنولوجيا متوسط تكلفة إجمالية لخرق البيانات أعلى بكثير من المجالات الأقل تنظيما مثل الضيافة والإعلام والبحث. تسجل مؤسسات القطاع العام تقليديا أقل تكلفة لخرق البيانات في هذا البحث، لأنه من غير المحتمل أن تشهد خسارة كبيرة للعملاء نتيجة لخرق البيانات.



شكل (14)

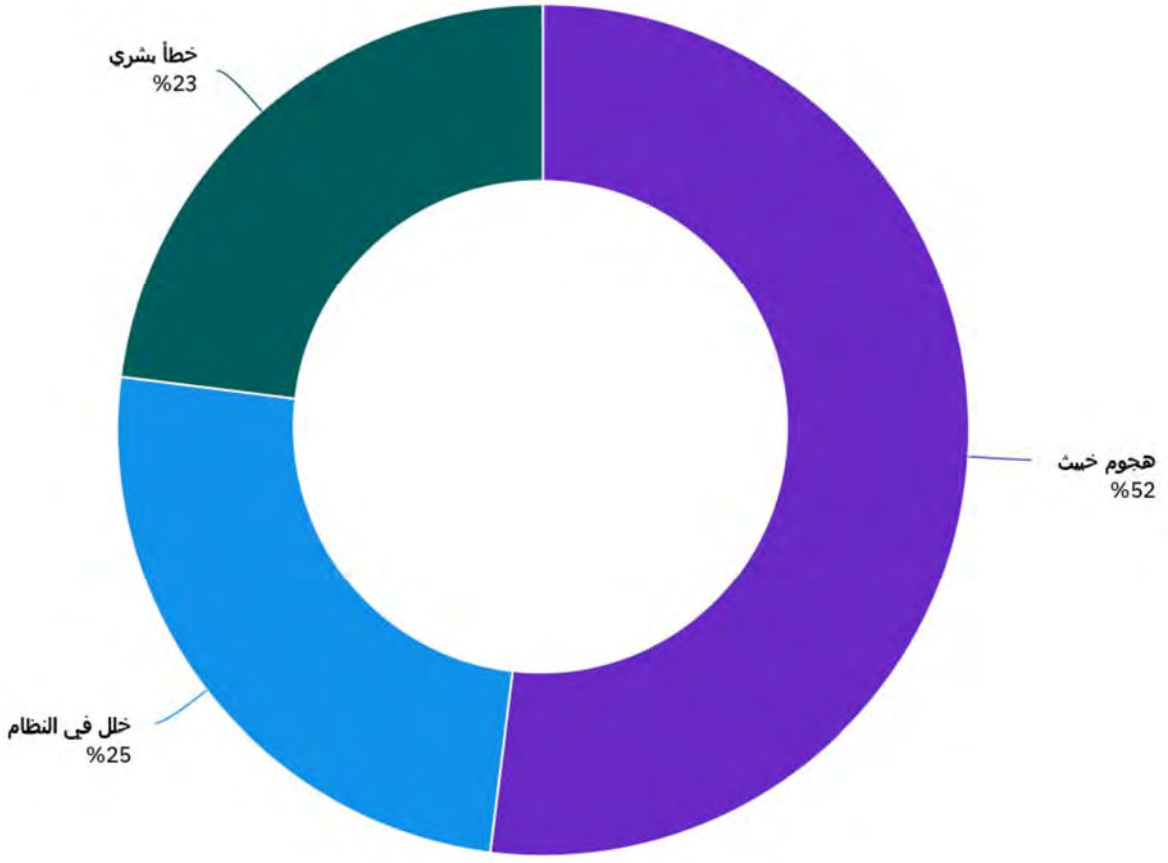
وأخيرا توضح الدراسة إجمالي متوسط تكلفة خرق البيانات حسب البلد أو المنطقة حيث يظهر الشكل رقم 15 رقم متوسط التكلفة الإجمالية لخرق البيانات لكل دولة. المؤسسات في الولايات المتحدة سجلت أعلى متوسط إجمالي للتكلفة بقيمة 8.64 مليون دولار، يليها الشرق الأوسط بمبلغ 6.52 مليون دولار. في المقابل سجلت مؤسسات أمريكا اللاتينية والبرازيلية أدنى متوسط بتكلفة إجمالية 1.68 مليون دولار و 1.12 مليون دولار على التوالي.



شكل (15)

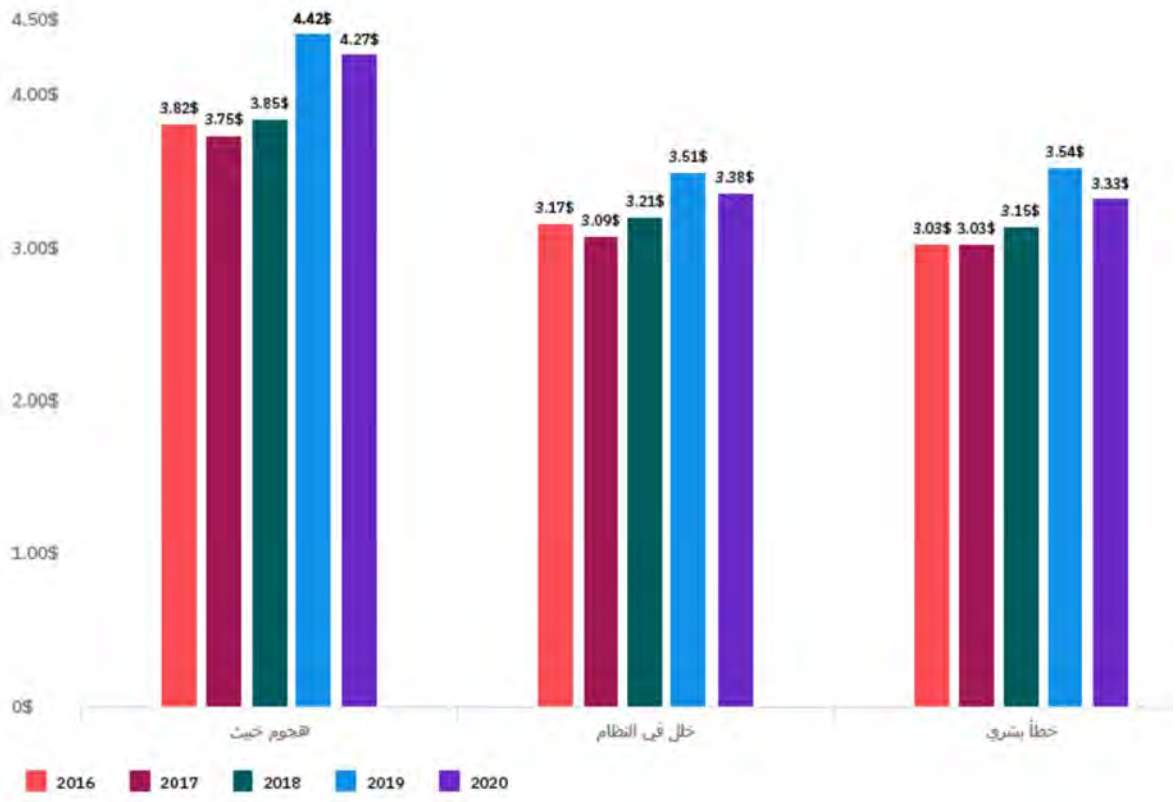
2 .الأسباب الجزرية لخرق البيانات

قامت هذه الدراسة البحثية لعدة سنوات بسؤال المشاركين لمعرفة سبب خرق البيانات. في السابق تم تجميع هذه الأسباب الجذرية في ثلاث فئات: مواطن الخلل في النظام، بما في ذلك كل من فشل جراءات تكنولوجيا المعلومات وإجراءات الأعمال؛ والخطأ البشري، بما في ذلك الموظفين أو المقاولين المهملين الذين يتسببون عن غير قصد في خرق البيانات؛ والهجمات الخبيثة، التي يمكن أن يتسبب فيها المتسللين أو المجرمين المطلعين من الداخل. تستمر دراسة هذا العام في إيراد الخروقات في هذه الفئات الثلاث. ومع ذلك ولتحليل أعمق طلب من المشاركين تقديم معلومات أكثر تفصيلاً حول سبب الهجمات الخبيثة، بما في ذلك عامل التهديد الأولي ونوع المهاجم. يوضح الشكل رقم 16 الأسباب الجذرية لخرق البيانات والتي تشمل ثلاث فئات. حيث تسببت الهجمات الخبيثة غالبية خروقات البيانات بمعدل 52 % من الحوادث ، مقارنة بنسبة 25 % بسبب خلل في النظام و 23 % بسبب خطأ بشري.



شكل (16)

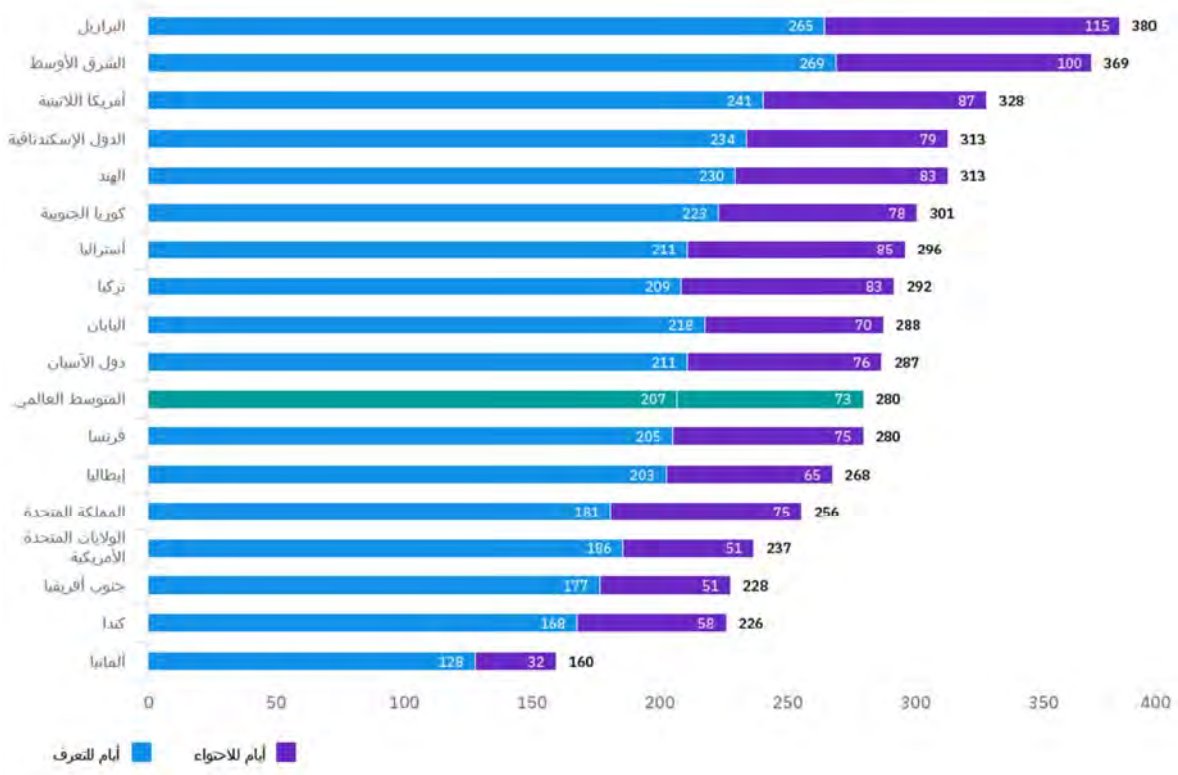
حيث ظلت الخروقات الخبيثة الأكثر تكلفة على مدار السنوات الخمس الماضية. شكل رقم 17 يوضح متوسط التكلفة الإجمالية للأسباب الجزرية الثلاثة لخرق البيانات على مدار السنوات الخمس الماضية. منذ دراسة 2016 ، ظل نمط الأسباب الجذرية ثابت إلى حد ما، مع انخفاض طفيف في التكاليف في دراسة عام 2020 مقارنة بعام 2019 . زاد إجمالي تكلفة الخروقات الخبيثة للبيانات بنسبة 12% منذ دراسة عام 2016 .



شكل (17)

5 .الوقت اللازم لتحديد واحتواء خرق البيانات

كانت الفجوات بين البلدان/الأقاليم في متوسط دورة حياة الخرق كبيرة. استغرق البرازيل والشرق الأوسط وقتًا أطول بكثير من المتوسط لتحديد واحتواء خرق البيانات، بمتوسط 380 يومًا و 369 يومًا على التوالي كما هو موضح بالشكل 18. واستغرقت جنوب أفريقيا وكندا وألمانيا وقتا أقصر بكثير، حيث استغرقت دورات حياة خرق البيانات، في المؤسسات الألمانية متوسط وقت 160 يومًا فقط لاحتواء الخرق.


البرازيل
265
115
380
الشرق الأوسط
269
100
369
أمريكا اللاتينية
241
87
328
الدول الإسكندنافية
234
79
313
الهند
230
83
313
كوريا الجنوبية
223
78
301
أستراليا
211
85
296
تركيا
209
83
292
اليابان
218
70
288
دول الآسيان
211
76
287
المتوسط العالمي
207
73
280
فرنسا
205
75
280
إيطاليا
203
65
268
المملكة المتحدة
181
75
256
الولايات المتحدة الأمريكية
186
51
237
جنوب أفريقيا
177
51
228
كندا
168
58
226
ألمانيا
128
32
160
0
50
100
150
200
250
300
350
400
أيام للتعرف
أيام للاحتواء

شكل (18)

الفصل الرابع

النتائج والتوصيات

النتائج

نتائج البحث:

من خلال البحث في تطبيق نظام إدارة أمن المعلومات وتتبع المخاطر التي يتعرض لها، خرجت الدراسة بعدة نتائج هامة يمكن إيجازها في النقاط التالية:

1. يتعرض أمن المعلومات للعديد من المخاطر والتهديدات التي تتم في بيئة الإنترنت مع عدم مواكبة التدابير التقنية المضادة لسرعة تطور الطرق الحديثة المستخدمة في عمليات الاعتداءات على أمن المعلومات.

2. ضعف التشريعات الموجودة على ارض الواقع سواء على المستوى الدولي أو الوطني مع وجود بطء ملحوظ في العمل على كفاية التشريعات الموجودة للحد من عمليات التعدي على أمن المعلومات.

3. قلة خبرة العاملين داخل المنشآت المعلوماتية مما يؤدي إلى حدوث مخاطر من داخل النظام نفسه والعاملين فيه ويساعد ذلك على ظهور جرائم الاحتيال والهندسة الاجتماعية.

4. قلة خبرة مستخدم الإنترنت نفسه في التعامل مع الوسائل التي يستخدمها المهاجمين.

5. التطور السريع للأساليب والتقنيات المستخدمة في الجرائم الإلكترونية مما يصعب من مهمة شركات البرمجيات المضادة للفيروسات، ووضع ضغوط مستمرة على الهيئات التشريعية.

أن القوانين المتبعة في حماية أمن المعلومات الرقمية تبطئ من عمل المديرين في أمن المعلومات لعدم مواكبتها للأساليب الحديثة المتبعة في الهجمات الإلكترونية لأنها ليست فعاله بالشكل الكافي، وتفتقر إلى آلية التطبيق نظرا لتنوع هذه الهجمات وتطورها المستمر.

التوصيات

توصيات البحث:

خرج البحث بعدة توصيات من خلال دراسة تطبيق نظام إدارة أمن المعلومات من الجانب التقني في قطاع الخدمات والإتصالات السورية وما تتعرض له من جرائم بالإضافة إلى دراسة بعض التدابير اللازمة للحد من هذه الجرائم، وهي كالتالي:

1. ضرورة تدريب العاملين داخل نظام أمن المعلومات والقيام بالعديد من الدورات التي تنمي مهاراتهم وقدراتهم المعرفية والتقنية في مجال أمن المعلومات.

2. ضرورة القيام بدورات لتوعية المستخدمين أنفسهم على حماية بياناتهم الشخصية على الإنترنت.

3. العمل على ملاحقة التطورات التي تظهر في أساليب وتقنيات الجرائم الإلكترونية عن طريق عمل برمجيات مضادة للحد من هذه الجرائم.

4. ضرورة تطوير التشريعات الخاصة بأمن المعلومات بشكل مستمر على المستويين الوطني والدولي لمعاقبة مرتكبي مثل هذه الجرائم والعمل على ردع من يقوم بمثل هذه الاعتداءات.

قائمة المراجع

المراجع:

(1) DataReportal. Digital 2020 October Global Statshot Report, Available At:
https://datareportal.com/reports/digital-2020-october-global-statsho.

(2) DataReportal. Digital 2020 January Global Statshot Report, Available At:
https://datareportal.com/reports/digital-2020-iran.

(3) DataReportal. Digital 2020 January Global Statshot Report, Available At:
https://datareportal.com/digital-in-syria.

(4) القحطاني، ذيب بن عايض. **أمن المعلومات (نصائح من خبراء).** مدينة الملك عبدالعزيز للعلوم والتقنية، السعودية-الرياض. 2015.

(5) MacAfee. Economic Impact of Cybercrime: No Slowing Down, 2018,
https://csisprod.s3.amazonaws.com/s3fs-public/publication/economic-impact-cybercrime.pdf

(6) Grant Gross. The Cost of Cybercrime, Internet Society 2018,
https://www.internetsociety.org/blog/2018/02/the-cost-of-cybercrime

(8) Tony Campbell. Practical Information Security Management, Berlin: Springer International Publishing Ag, 2016, P.14,
http://link.springer.com/10.1007/978-1-4842-1685-9

(17) John Adams. How to protect your small business from cyber-attacks, United States: Colorado Technical University, Management Dep. (PhD), 2018,
https://www.securityskeptic.com/2019/09/how-to-protect-your-small-business-from-cyber-attacks.html

(18) Ibrahim Ghafir, Jibran Saleem, Mohammad Hammoudeh... et al. Security Threats to Critical Infrastructure: The Human Factor, The Journal of Supercomputing, Vol. 74, No. 10, USA: Springer, Gross Mark, 2018,
https://link.springer.com/article/10.1007%2Fs11227-018-2337-2

(20) Rolf H. Weber, Evelyne Studer. Cybersecurity in the Internet of Things: Legal Aspects, Computer Law & Security Review, Vol. 32, No. 5, Switzerland: Elsevier, 2016,
https://www.sciencedirect.com/science/article/abs/pii/S0267364916301169?via%3Dihub

(23) Sagar Ajay Rahalkar. Certified Ethical Hacker (CEH) Foundation Guide: Information Security Basic, India: Press, 2016, P. 91,
https://link.springer.com/book/10.1007/978-1-4842-2325-3

(28) John M.D. Hunter. An Information Security Handbook, London: Springer, 2010, P. 7,
https://www.springer.com/gp/book/9781852331801

(34) Gattiker Urs E. The Information Security: Defining the Terms That Define Security for E-Business, Internet, Information and Wireless Technology, New York: Kluwer Academic Publishers, 2015, P. 91,
https://www.springer.com/gp/book/9781402078897

(37) Chinese Academy of Cyberspace Studies. Improving Capacity of Cyber Security Safeguarding in Chinese Academy of Cyberspace, Berlin: Springer, 2019, P. 103,
https://link.springer.com/chapter/10.1007/978-3-662-57521-5_6

(38) Theodoros T., Loukas K. Online Social Network Phishing Attack, Encyclopedia of Social Network Analysis and Mining, New York: Springer, 2018, P. 38,
https://link.springer.com/content/pdf/10.1007%2F978-1-4939-7131-2_348.pdf

(56) Alice Hutchings, Russell G. Smith, Lachlan Hames. Criminals in the Cloud: Crime, Security Threats, and Prevention Measures, Switzerland: Palgrave Macmillan, 2015, P. 158,
https://link.springer.com/content/pdf/10.1057%2F9781137474162_10.pdf

(64) Qiuyan Tian, Hao Kang, Ting Ai. Analysis and Comparison of Network Information Security Encryption Technology, Advanced in Engineering, Vol. 166, China: Atlantis Press, 2018, P. 679,
https://download.atlantis-press.com/article/25895751.pdf

(68) Richard Stanley. Information Security, Cybercrimes: A Multidisciplinary Analysis, Berlin: Springer, 2011, P. 117, https://link.springer.com/book/10.1007/978-3-642-13547-7

(21) John M. Broky, Thomas H. Bradley. Protecting Information with Cybersecurity, Berlin: Springer International Publishing AG, 2019, Pp. 350-351,
https://www.semanticscholar.org/paper/Protecting-Information-with-Cybersecurity-Borky-Bradley/e304bac8cb6f2ec82ea9ff361f9156ced20f428e

(69) John M. Broky, Thomas H. Bradley. Op. Cit, P. 383.

(87) MacLennan A. Information Governance and Assurance, International Journal of Information Management, Vol. 35, London: Elsevier Fact Publisher, 2015, P. 174,
https://081010y2c-1105-yhttps-ac-els--cdn-com.mplbci.ekb.eg

(89) طارش، أحمد علي عبد الله، **رؤية إستراتيجية لتحقيق الأمن المعلوماتي في هيئة التحقيق والادعاء العام في المملكة العربية السعودية،** (أطروحة ماجستير)، الرياض ، 2015 ، ص71
https://core.ac.uk/download/pdf/80744102.pdf

(93) Kaspersky - A global cybersecurity company,
https://me.kaspersky.com/resource-center/threats/what-is-a-security-breach

(94) وحدة الدراسات والتقارير (3) ، هل أصبحت الهجمات الإلكترونية بديلا عن الحروب التقليديّة ؟، **المركز الأوروبي لدراسات مكافحة الإرهاب والإستخبارات**
https://www.europarabct.com/?p=57441

(94) Kaspersky - A global cybersecurity company,
https://me.kaspersky.com/about/press-releases/2019_cyber-defense-summit-arabic

(95) 7 أغسطس 2019، 18% ارتفاع هجمات حجب الخدمة في الربع الثاني ، **صحيفة دار الخليج**
https://www.europarabct.com/?p=57441

(96) 11 ديسمبر 2020، خسائر صادمة بسبب الهجمات الإلكترونية.. كم تكبد العالم؟، **العربية.نت**
https://www.alarabiya.net/ar/aswaq/economy/2019/10/23/خسائر-صادمة-بسبب-الهجمات-الالكترونية-كم-تكبد-العالم؟

(97) TechRepublic - Helps IT decision-makers identify technologies and strategies to empower workers and streamline business processes,
https://www.techrepublic.com/article/how-dns-attacks-threaten-organizations/

(98) Nick Ismail, Information Age, Telcos struggling to mitigate the threats of cyber attacks,
https://www.information-age.com/telcos-cyber-attacks-123476699

(99) 20 مايو 2020، تخيل كم بلغت تكاليف هجمات طلب الفدية؟، **دبي - البوابة العربية للأخبار التقنية**،
https://www.alarabiya.net/ar/technology/2017/07/28/تخيل-كم-بلغت-تكاليف-هجمات-طلب-الفدية؟

(100) 15 سبتمبر 2020، 20 مليار دولار كلفة هجمات الفدية المتوقعة عالمياً بحلول 2020 ، **منصة الرؤية - بوابة إعلامية عربية إماراتية**،
https://www.alroeya.com/117-53/2165032-20--مليار-دولار-كلفة-هجمات-الفدية-المتوقعة-عالميا-بحلول-2021

(101) Kaspersky - A global cybersecurity company,
https://me.kaspersky.com/about/press-releases/2015_one-out-of-five-ddos-attacks-continues-its-impact-for-days-or-even-weeks

(102) Standard Timespress, One prosecution not good enough,
https://webcache.googleusercontent.com/search?q=cache:sQ4BFlbgrdcJ:https://standardtimespress.org/%3Fp%3D5791+&cd=5&hl=en&ct=clnk

(103) 21 أكتوبر 2012، تعليم وتدريب ، مصطلحات امن المعلومات ، **المركز العربي لأبحاث الفضاء الإلكتروني**،
http://accronline.com/article_detail.aspx?id=4713

ملاحق البحث

1- المصطلحات (103).

Term	Definition	تعريف المصطلح	المصطلح
Access Authority	An entity responsible for monitoring and granting access privileges for other authorized entities.	الكيان المسؤول عن مراقبة ومنح صلاحيات الوصول للجهات المُصرَّح لها.	هيئة الوصول
Access Control	The process of granting or denying specific requests:	قبول أو رفض طلبات معينة تختص بـ	التحكم في الوصول
	1) for obtaining and using information and related information processing services; and	**1)** الحصول على (حيازة) معلومات واستخدامها و كذلك الحصول على خدمات تتعلق بمعالجتها	
	2) to enter specific physical facilities (e.g., Federal buildings, military establishments, and border crossing entrances).	**2)** الدخول إلى منشآت مادية محددة مثل المباني الحكومية والمؤسسات العسكرية ونقاط العبور الحدودية.	
Accreditation	The official management decision given by a senior agency official to authorize operation of an system and to explicitly accept the risk to agency operations (including mission, functions, image, or reputation), agency assets, or individuals, based on the implementation of	قرار الإدارة الرسمية صادر من أحد الكوادر العليا لهيئة ما للتصريح بالموافقة على تشغيل نظام معلومات والقبول صراحةً بتعريض عمليات تلك الهيئة للمخاطرة (بما في ذلك رسالتها أو وظائفها أو مصداقيتها أو سمعتها) أو أصولها أو منسوبيها بناءً على تطبيق مجموعة	إصدار/اعتماد الموافقة

	an agreed-upon set of security controls.	عناصر التحكم الأمني المتفق عليها	
Accreditation Boundary	All components of an information system to be accredited by an authorizing official and excludes separately accredited systems, to which the information system is connected.	كل ما يقوم "موظف إصدار التصريح" بالموافقة عليه من مكونات نظام معلومات باستثناء ما تم الموافقة عليه بشكل منفصل من أنظمة يتصل بها نظام المعلومات.	حدود الاعتماد
Accreditation Package	The evidence provided to the authorizing official to be used in the security accreditation decision process. Evidence includes, but is not limited to:	الأدلة المقدمة إلى موظف "إصدار التصريح" لاستخدامها في عملية إصدار قرار الموافقة الأمنية. تتضمن تلك الأدلة على سبيل المثال وليس الحصر:	حيثيات الاعتماد
	1) the system security plan;	**1)** الخطة الأمنية للنظام	
	2) the assessment results from the security certification; and	**2)** نتائج التقييم الصادرة عن التوثيق الأمني	
	3) the plan of action and milestones.	**3)** خطة العمل ومراحله.	
Accrediting Authority	Official with the authority to formally assume responsibility for operating an information system at an acceptable level of risk to agency	الجهة المخول لها رسمياً سلطة أن تكون مسؤولة عن تشغيل نظام معلومات معين ضمن حد مقبول من المخاطرة بعمليات هيئة معينة بما يشمل رسالتها	جهة الاعتماد

	operations (including mission, functions, image, or reputation), agency assets, or individuals.	ووظائفها ومصداقيتها وسمعتها بالإضافة إلى أصولها أو منسوبيها.	
Attack Signature	A specific sequence of events indicative of an unauthorized access attempt.	مجموعة متسلسلة من الأحداث تشير إلى وجود محاولة وصول غير مصرح بها.	بصمة هجوم
Attribute Authority	An entity, recognized by the Federal Public Key Infrastructure (PKI) Policy Authority or comparable Agency body as having the authority to verify the association of attributes to an identity.	جهة تحددها هيئة السياسات الفيدرالية لسياسات البنية التحتية للمفتاح العام أو وكالة مماثلة بحيث يكون لها سلطة التحقق من توافق الخصائص مع هوية معينة.	هيئة التحقق من خصائص الهوية
Audit	Independent review and examination of records and activities to assess the adequacy of system controls, to ensure compliance with established policies and operational procedures, and to recommend necessary changes in controls, policies, or procedures	مراجعة مستقلة وفحص للسجلات والأنشطة لتقييم كفاية عناصر تحكم النظام للتأكد من موافقتها للسياسات وإجراءات التشغيل المقررة، وإصدار التوصيات حول ما هو ضروري من تغييرات في عناصر التحكم أو السياسات أو الإجراءات.	التدقيق والفحص
Audit Data	Chronological record of system activities to enable the reconstruction and examination of the sequence of events and changes in an event.	سجل تاريخي لأنشطة النظام لتوفير إمكانية إعادة بناء وفحص سلسلة من الأحداث و التغييرات التي شهدها حدث معين.	بيانات التدقيق والفحص

Audit Reduction Tools	Preprocessors designed to reduce the volume of audit records to facilitate manual review. Before a security review, these tools can remove many audit records known to have little security significance. These tools generally remove records generated by specified classes of events, such as records generated by nightly backups.	معالجات تم إعدادها مسبقاً لخفض حجم سجلات الفحص والتدقيق بغرض تسهيل المراجعة اليدوية. قبل إجراء المراجعة الأمنية تستطيع هذه الأدوات إزالة العديد من سجلات التدقيق والفحص المعروفة بانخفاض أهميتها الأمنية. تقوم هذه الأدوات عموماً بإزالة أنواع محددة من الأحداث مثل تلك السجلات الناتجة عن عمليات النسخ الاحتياطي الدورية التي تحدث في نهاية كل ليلة.	أدوات تيسير التدقيق والفحص
Audit Trail	A record showing who has accessed an Information Technology (IT) system and what operations the user has performed during a given period.	سجل يوضح من قام بالدخول إلى نظام تقنية معلومات و العمليات التي قام بتنفيذها أثناء فترة معينة.	سجل الفحص و المراجعة
Authenticate	To confirm the identity of an entity when that identity is presented.	التأكد من هوية جهة معينة عند تقديم تلك الهوية.	يصدِّق على / يتحقق من هوية
Authentication	Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in an information system. The process of establishing confidence of authenticity. Encompasses identity verification, message origin authentication,	التأكد من صحة هوية الخاصة بأحد المستخدمين أو العمليات أو الأجهزة. يكون ذلك عادة كأحد متطلبات السماح بالوصول إلى الموارد الموجودة في نظام معلومات معين. عملية تأسيس الثقة وتشمل التحقق من صحة الهوية والتحقق من مصدر	التصديق / التحقق من الهوية

	and message content authentication. A process that establishes the origin of information or determines an entity's identity.	الرسالة ومحتواها. عملية تهدف إلى تحديد مصدر المعلومات أو هوية جهة ما.	
Authentication Code	A cryptographic checksum based on an approved security function (also known as a Message Authentication Code (MAC)).	معادلة تشفير حسابية تعتمد على وظيفة أمنية صادر بشأنها موافقة (تعرف أيضاً باسم شفرة رسالة التصديق) .	شفرة التحقق من الهوية
Electronic Authentication	The process of establishing confidence in user identities electronically presented to an information system.	عملية إثبات الثقة في هويات المستخدمين التي تقدم الكترونياً لنظام معلومات.	التحقق من الهوية الكترونياً
Authentication Mechanism	Hardware or software-based mechanisms that force users to prove their identity before accessing data on a device.	آليات تعتمد على الأجهزة أو البرامج بحيث تُجبِر المستخدمين على إثبات هوياتهم قبل الوصول للبيانات الموجودة على أحد الأجهزة.	آلية التحقق من الهوية
Authentication Mode	A block cipher mode of operation that can provide assurance of the authenticity and, therefore, the integrity of data.	وضعية تشغيل تستخدم قالب ترميز معين يمكنها تأمين الثقة في هوية المستخدم وبالتالي في تكامل البيانات.	وضعية التحقق من الهوية
Authentication Protocol	A well specified message exchange process that verifies possession of a token to remotely authenticate a claimant. Some	عملية تبادل للرسائل محددة بدقة يجري خلالها التحقق من صحة امتلاك احد الرموز المميزة بغرض التحقق عن بعد	برتوكول التحقق من الهوية

	authentication protocols also generate cryptographic keys that are used to protect an entire session, so that the data transferred in the session is cryptographically protected.	من هوية الشخص الذي يطلب التعامل مع نظام معين. بعض برتوكولات التصديق تقوم بإنشاء مفاتيح تشفير تُستخدَم لتوفير الحماية طوال فترة التعامل مع النظام ولذلك تكون البيانات المنقولة خلال تلك الفترة محمية بفضل تشفيرها.	
Authentication Tag	A pair of bit strings associated to data to provide assurance of its authenticity.	زوجين من السلاسل النصية مرتبطة بالبيانات للتأكد من مصداقيتها.	علامة التصديق
Authentication Token	Authentication information conveyed during an authentication exchange.	معلومات التحقق المتبادلة أثناء التحقق من صحة الهوية	الرمز المميز للتحقق من الهوية
Authenticity	The property of being genuine and being able to be verified and trusted; confidence in the validity of a transmission, a message, or message originator.	خاصية أن تكون أصلياً وقابل للتحقق من هويتك والوثوق بها من خلال منح الثقة في صحة الإرسال والرسالة ومرسلها.	خاصية المصداقية
Authorization	The official management decision given by a senior agency official to authorize operation of an information system and to explicitly accept the risk to agency operations (including mission, functions, image, or reputation), agency assets, or	قرار الإدارة الرسمية الصادر من أحد الكوادر العليا لهيئة ما لاعتماد الموافقة على تشغيل نظام معلومات والقبول علانيةً بتعريض عمليات تلك الهيئة للمخاطرة (بما في ذلك رسالتها ووظائفها ومصداقيتها وسمعتها) أو أصولها أو منسوبيها بناءاً	تصريح

	individuals, based on the implementation of an agreed-upon set of security controls.	على تنفيذ مجموعة من عناصر التحكم الأمني المتفق عليها.	
Authorizing Official	Official with the authority to formally assume responsibility for operating an information system at an acceptable level of risk to agency operations (including mission, functions, image, or reputation), agency assets, or individuals. Synonymous with Accreditation Authority.	الموظف (الكيان) المسؤول رسمياً عن تشغيل نظام معلومات معين ضمن حد مقبول من المخاطرة بعمليات هيئة معينة (بما يشمل رسالتها ووظائفها ومصداقيتها وسمعتها) بالإضافة إلى أصولها أو منسوبيها.	موظف إصدار التصريح
Authorizing Official	Individual selected by an authorizing official to act on their behalf in coordinating and carrying out the necessary activities required during the security certification and accreditation of an information system.	شخص يختاره موظف إصدار التصريح للعمل نيابة عنه في تنسيق وتنفيذ الأنشطة الضرورية المطلوبة أثناء التوثيق و الاعتماد الأمني لأحد أنظمة المعلومات.	مندوب إصدار التصريح
Automated Key Transport	The transport of cryptographic keys, usually in encrypted form, using electronic means such as a computer network (e.g., key transport/agreement protocols).	نقل مفاتيح التشفير (عادة بطريقة مشفرة) باستخدام وسائل الكترونية مثل شبكات الحاسوب كما هو الحال في بروتوكولات نقل مفتاح التشفير وقبوله.	النقل الآلي للمفتاح

Automated Password Generator	An algorithm which creates random passwords that have no association with a particular user.	خوارزمية تقوم بإنشاء كلمات مرور العشوائية غير مرتبطة بمستخدم معين.	مولد كلمة المرور الآلي
Availability	Ensuring timely and reliable access to and use of information.	التأكد من إمكانية الوصول إلى المعلومات واستخدامها في الوقت المناسب وبشكل يُعتمَد عليه.	استمرارية توفر الخدمة
Information Security Awareness	Activities which seek to focus an individual's attention on an (information security) issue or set of issues.	الأنشطة التي تسعى لجذب انتباه الأفراد إلى موضوع أو مجموعة من الموضوعات في أمن المعلومات.	الوعي بأمن المعلومات
Backup	A copy of files and programs made to facilitate recovery if necessary.	نسخة من الملفات والبرامج لتسهيل عملية الاسترجاع في حالة الضرورة.	نسخة احتياطية
Baseline Security	The minimum security controls required for safeguarding an IT system based on its identified needs for confidentiality, integrity and/or availability protection.	الحد الأدنى من عناصر التحكم الأمنية المطلوبة لحماية نظام معلومات معين بناءاً على الاحتياجات المحددة لحماية سرية وتكامل و/أو استمرارية توفر خدمة هذا النظام.	الحد الأدنى من الأمن
Baselining	Monitoring resources to determine typical utilization patterns so that significant deviations can be detected.	مراقبة الموارد لتحديد نماذج الاستخدام الأمثل بهدف كشف الانحرافات الخطيرة.	الرقابة والمتابعة والضبط

Bastion Host	A bastion host is typically a firewall implemented on top of an operating system that has been specially configured and hardened to be resistant to attack.	هو جدار حماية نموذجي يجرى تنصيبه على نظام تشغيل جرى إعداده وتقويته خصيصاً ليكون مقاوم للهجمات.	جهاز المضيف المحصن
Behavioral Outcome	What an individual who has completed the specific training module is expected to be able to accomplish in terms of IT security-related job performance.	ما يتوقع من شخص تلقى تدريباً خاصاً يمِّكنه من إظهار مردود ما تعلمه عن أمن المعلومات من خلال أداءه الوظيفي.	المحصلة السلوكية
Binding	Process of associating two related elements of information. An acknowledgement by a trusted third party that associates an entity's identity with its public key. This may take place through	عملية ضم عنصرين مرتبطين من عناصر المعلومات. اعتراف من طرف ثالث موثوق يقوم بربط هوية جهة معينة بمفتاح التشفير العام لتلك الجهة. يمكن أن يتم تطبيق ذلك من خلال	الربط
	(1) a certification authority's generation of a public key certificate,	**1)** قيام هيئة توثيق بإصدار شهادة مفتاح التشفير العام	
	(2) a security officer's verification of an entity's credentials and placement of the entity's public key and identifier in a secure database, or	**2)** قيام موظف أمن بالتحقق من بيانات دخول تلك الجهة ووضع مفتاح التشفير العام لتلك الجهة مع رقم مميز في قاعدة بيانات آمنة أو	

	(3) an analogous method.	**3)** إتباع الأسلوب التناظري.	
Biometric	A physical or behavioral characteristic of a human being. A measurable, physical characteristic or personal behavioral trait used to recognize the identity, or verify the claimed identity, of an applicant. Facial images, fingerprints, and handwriting samples are all examples of biometrics.	ميزة جسدية أو سلوكية من مميزات الإنسان. ميزة جسدية أو صفة سلوك الشخصي قابلة للقياس تُستخدَم في تعريف شخصية مقدم الطلب أو التحقق منها. تعد صور الوجه وبصمات الأصابع ونماذج الكتابة من أمثلة القياسات الحيوية.	قياس حيوي
Biometric Information	The stored electronic information pertaining to a biometric. This information can be in terms of raw or compressed pixels or in terms of some characteristic (e.g. patterns.)	هي تلك المعلومات الالكترونية المخزنة بخصوص مقياس حيوي معين و تكون في شكل نقاط خام أو مضغوطة أو في شكل له بعض الخصائص مثل النماذج.	معلومات القياس الحيوي
Biometric System	An automated system capable of:	نظام آلي قادر على:	نظام قياس حيوي
	1) capturing a biometric sample from an end user;	**1)** الحصول على عينة قياس حيوية من المستخدم النهائي	
	2) extracting biometric data from that sample;	**2)** استخلاص بيانات القياس الحيوي من تلك العينة	

	3) comparing the biometric data with that contained in one or more reference templates;	**3)** مقارنة بيانات القياس الحيوي بتلك الموجودة في نموذج أو أكثر	
	4) deciding how well they match; and	**4)** تقدير مدى التماثل بينهما و	
	5) indicating whether or not an identification or verification of identity has been achieved.	**5)** الإشارة إلى ما إذا كان التعرف أو التحقق من صحة الشخصية قد تم إنجازه أم لا.	
Biometric Template	A characteristic of biometric information (e.g. minutiae or patterns.)	أحد خواص معلومات القياس الحيوي (تفاصيل أو شكل مثلاً) .	نموذج قياس حيوي
Blended Attack	Malicious code that uses multiple methods to spread.	شفرة برمجية خبيثة تستخدم عدة أساليب كي تدعم انتشاره.	الهجوم المختَلَط
Block	Sequence of binary bits that comprise the input, output, State, and Round Key. The length of a sequence is the number of bits it contains. Blocks are also interpreted as arrays of bytes.	تسلسل من وحدات البت الثنائية يشكل المدخلات والمخرجات والحالة والمفاتيح المتعاقبة. طول ذلك التسلسل هو عدد وحدات البت التي يتضمنها. تُفسر القوالب أيضاً على أنها مصفوفة من وحدات البايت.	قالب
Block Cipher	A symmetric key cryptographic algorithm that transforms a block of information at a time using a cryptographic key. For a block cipher	خوارزمية تشفير متناظرة تُحوِّل قالب من المعلومات في وقت واحد مستخدمة مفتاح تشفير. من صفات تلك الخوارزمية أن طول	تشفير القالب

	algorithm, the length of the input block is the same as the length of the output block.	قالب المدخلات هو نفس طول قالب المخرجات.	
Block Cipher Algorithm	A family of functions and their inverses that is parameterized by a cryptographic key; the function maps bit strings of a fixed length to bit strings of the same length.	مجموعة من الدوال الحسابية ومعكوساتها يجري توحيدها معيارياً باستخدام مفتاح تشفير حيث تقوم الدالة بتحويل سلسلة ذات طول محدد من وحدات البت إلى سلسلة من وحدات البت لها نفس الطول.	خوارزمية تشفير القالب
Boot Sector Virus	A virus that plants itself in a system's boot sector and infects the master boot record.	فيروس يقوم بزراعة نفسه داخل قطاع تشغيل نظام معين ثم يصيب سجل التشغيل الرئيسي.	فيروس قطاع التشغيل
Boundary Protection	Monitoring and control of communications at the external boundary between information systems completely under the management and control of the organization and information systems not completely under the management and control of the organization, and at key internal boundaries between information systems completely under the management and control of the organization, to prevent and detect malicious and other unauthorized	فرض الرقابة والتحكم في الاتصالات على الحدود الخارجية بين أنظمة المعلومات الخاضعة بالكامل لإدارة ورقابة منظمة معينة وتلك الأنظمة التي لا تخضع لإدارتها ورقابتها بشكل كامل، بالإضافة إلى فرضهما على الحدود الداخلية الرئيسية بين نظم المعلومات التي تخضع بأكملها لإدارة ورقابة تلك المنظمة بغرض منع واكتشاف محاولات الاتصال الخبيثة وغير المصرح بها وكذلك استعمال وسائل اتصال	حماية حدود النظام

	communication, employing controlled interfaces (e.g., proxies, gateways, routers, firewalls, encrypted tunnels).	يمكن التحكم بها مثل الوكيل وبوابات الوصول والموجهات وجدران الحماية والقنوات المشفرة.	
Boundary Router	A boundary router is located at the organizations boundary to an external network.	موجه خارجي يوضع على نقاط اتصال المنظمات مع شبكة خارجية.	موجه اتصال خارجي
Brute Force Password Attack	A method of accessing an obstructed device through attempting multiple combinations of numeric and/or alphanumeric passwords.	أسلوب لمحاولة الدخول على أحد الأجهزة التي تمثل عائقاً من خلال إجراء المحاولات باستخدام كلمات مرور متنوعة تجمع عدد من الحروف و/أو الأرقام.	طريقة الاستقصاء في الهجوم على كلمة المرور
Buffer Overflow	A condition at an interface under which more input can be placed into a buffer or data holding area than the capacity allocated, overwriting other information. Attackers exploit such a condition to crash a system or to insert specially crafted code that allows them to gain control of the system.	شرط في قناة الاتصال يمكن من خلاله وضع عدد اكبر من المدخلات في منطقة مخصصة لاحتجاز البيانات بما يفوق قدرتها الاستيعابية لذلك من خلال استبدال المعلومات الموجودة بالكتابة عليها. يستخدم المهاجمون ذلك الشرط لإسقاط النظام أو إدخال شفرات خاصة تم إعدادها بمهارة عالية تسمح لهم بالسيطرة على النظام والتحكم فيه.	إغراق ذاكرة التخزين المؤقت

Buffer Overflow Attack	A method of overloading a predefined amount of space in a buffer, which can potentially overwrite and corrupt data in memory.	أسلوب التحميل الزائد للبيانات داخل مساحة محددة سلفاً في منطقة حفظ البيانات مما يؤدى إلى احتمالية الكتابة على الكتابة الموجودة في الذاكرة أو تخريبها.	الهجوم بإغراق ذاكرة التخزين المؤقت
Business Continuity Plan (BCP)	The documentation of a predetermined set of instructions or procedures that describe how an organization's business functions will be sustained during and after a significant disruption.	توثيق مجموعة من التعليمات والإجراءات المُعَدّة سلفاً لوصف كيفية الحفاظ على وظائف العمل داخل منظمة معينة أثناء وبعد حدوث خلل خطير.	خطة الحفاظ على استمرارية العمل
Business Impact Analysis (BIA)	An analysis of an information technology (IT) system's requirements, processes, and interdependencies used to characterize system contingency requirements and priorities in the event of a significant disruption.	تحليل لما يخص نظام تقنية المعلومات من متطلبات وعمليات وعلاقات متبادلة تُستخدَم في توصيف ما يخص النظام من متطلبات طارئة وأولويات في حالة حدوث خلل خطير.	تحليل متطلبات الطوارئ
Business Recovery-Resumption Plan – (BRP)	The documentation of a predetermined set of instructions or procedures that describe how business processes will be restored after a significant disruption has occurred.	توثيق لمجموعة من التعليمات والإجراءات المحددة سلفاً تصف كيفية استعادة حركة العمل بعد حدوث خلل خطير.	خطة استعادة حركة العمل

Capture	The method of taking a biometric sample from an end user.	أسلوب الحصول على عينة قياس حيوي من مستخدم نهائي.	التقاط
Cardholder	An individual possessing an issued Personal Identity Verification (PIV) card.	شخص معين يمتلك بطاقة شخصية لتحديد الهوية.	حامل البطاقة
Certificate	A digital representation of information which at least	شكل رقمي للبيانات يوفر على الأقل ما يلي	شهادة رقمية
	1) identifies the certification authority issuing it,	**1)** تحديد هيئة التوثيق التي أصدرت الشهادة	
	2) names or identifies its subscriber,	**2)** أسماء المشتركين فيها	
	3) contains the subscriber's public key,	**3)** المفتاح العام للمشترك	
	4) identifies its operational period, and	**4)** يحدد الفترة التي تكون خلالها تلك الشهادة صالحة للعمل	
	5) is digitally signed by the certification authority issuing it. A set of data that uniquely identifies an entity, contains the entity’s public key and possibly other information, and is digitally signed by a trusted party, thereby binding the public key	**5)** يحمل التوقيع الالكتروني لهيئة التوثيق التي أصدرت الشهادة. مجموعة من البيانات التي تشير بشكل منفرد إلى كيان واحد بحيث تحتوى على المفتاح العام لذلك الكيان وأي معلومات أخرى ممكنة. تكون	

	to the entity. Additional information in the certificate could specify how the key is used and its cryptoperiod.	الرسالة مُصَدق عليها رقمياً من طرف ثالث موثوق به وعليه يتم ربط المفتاح العام بذلك الكيان. هناك معلومات إضافية في الشهادة الرقمية يمكن من خلالها تحديد كيفية استخدام المفتاح ومدة تشفيره.	
Certificate Policy (CP)	A Certificate Policy is a specialized form of administrative policy tuned to electronic transactions performed during certificate management. A Certificate Policy addresses all aspects associated with the generation, production, distribution, accounting, compromise recovery and administration of digital certificates. Indirectly, a certificate policy can also govern the transactions conducted using a communications system protected by a certificate-based security system. By controlling certificate extensions, such policies and associated enforcement technology can support provision of the security services	شكل خاص من السياسات الإدارية يتواءم مع معاملات إلكترونية تُطبق أثناء إدارة الشهادة الرقمية. تعالج سياسة الشهادة الرقمية كل النواحى المرتبطة باصدارها واستخراجها وتوزيعها وحساباتها واستعادتها وكذلك إدارتها. وبشكل غير مباشر يمكن لسياسة الشهادة الرقمية أن تتحكم فى المعاملات المُنجزة بنظام اتصالات تتوفر له الحماية من خلال نظام أمن يعتمد على الشهادة الرقمية. من خلال التحكم في الامتدادات الخاصة بالشهادات الرقمية الحرجة يمكن لتلك السياسات وما يصاحبها من تقنية المتابعة والضبط دعم تدابير الخدمات الأمنية التي تطلبها تطبيقات معينة.	سياسة الشهادة الرقمية

	required by particular applications.		
Certificate Management Authority (CMA)	A Certification Authority (CA) or a Registration Authority (RA).	هيئة توثيق أو هيئة تسجيل.	هيئة إدارة الشهادات الرقمية
Certificate-Related Information	Information, such as a subscriber's postal address, that is not included in a certificate. May be used by a Certification Authority (CA) managing certificates.	معلومات غير مضافة للشهادة الرقمية مثل العنوان البريدي للمشترك. ربما تستخدم هيئة توثيق معين تلك البيانات لإدارة الشهادات الرقمية.	معلومات مرتبطة بالشهادات الرقمية
Certificate Revocation List (CRL)	A list of revoked public key certificates created and digitally signed by a Certification Authority.	قائمة شهادات المفتاح العام الملغية. يتم إصدار تلك القائمة والتوقيع عليها رقمياً بواسطة هيئة توثيق.	قائمة الشهادات الرقمية الملغاة
Certificate Status Authority	A trusted entity that provides on-line verification to a Relying Party of a subject certificate's trustworthiness, and may also provide additional attribute information for the subject certificate.	كيان موثوق فيه توفر بشكل مباشر لطرف تابع امكانية التحقق من مصداقية شهادة رقمية معينة وربما أيضاً يوفر معلومات إضافية عن الشهادة الخاضعة للفحص .	هيئة تحديد حالة الشهادة الرقمية

Certification	A comprehensive assessment of the management, operational, and technical security controls in an information system, made in support of security accreditation, to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system.	تقييم شامل لكل عناصر التحكم والرقابة الإدارية والتشغيلية والفنية داخل نظام معلومات دعماً للحصول على الموافقة الأمنية بغرض تحديد مدى تُطبيق عناصر التحكم تطبيقاً سليماً ومدى عملها طبقاً للطريقة المقصودة وتحقيقها للنتائج المرجوة لتلبية متطلبات أمن النظام	توثيق
Certification Agent	The individual, group, or organization responsible for conducting a security certification.	الفرد أو المجموعة أو المنظمة المسؤولة عن إدارة التوثيق الأمني.	وكيل التوثيق الأمني
Certification Authority (CA)	A trusted entity that issues and revokes public key certificates. The entity in a public key infrastructure (PKI) that is responsible for issuing certificates and exacting compliance to a PKI policy.	كيان موثوق يقوم بإصدار وإلغاء شهادات المفتاح العام. ذلك الكيان الموجودة في البنية التحتية للمفتاح العام حيث يتولى مسؤولية إصدار الشهادات والتأكد من الالتزام بسياسة البنية التحتية للمفتاح العام.	هيئة التوثيق
Certification Authority Facility	The collection of equipment, personnel, procedures and structures that are used by a Certification Authority to perform	مجموعة الأجهزة والموظفين والإجراءات والمباني التي تستخدمها هيئة التوثيق لإصدار شهادة التوثيق وإلغاءها.	مرفق هيئة التوثيق

	certificate issuance and revocation.		
Certification Practice Statement (CPS)	A statement of the practices that a Certification Authority employs in issuing, suspending, revoking and renewing certificates and providing access to them, in accordance with specific requirements (i.e., requirements specified in this Certificate Policy, or requirements specified in a contract for services).	إعلان بالممارسات التي تتخذها هيئة التوثيق في سبيل إصدار أو وقف أو إلغاء أو تجديد الشهادات بالإضافة إلى توفير إمكانية الوصول إليها في ظل متطلبات معينة كتلك المحددة في سياسة الشهادة أو عقد توفير الخدمات.	بيان بممارسة أعمال التوثيق
Chain of Custody	A process that tracks the movement of evidence through its collection, safeguarding, and analysis lifecycle by documenting each person who handled the evidence, the date/time it was collected or transferred, and the purpose for the transfer.	عملية تتبع حركة الدليل من خلال جمعه وحمايته وتحليل دورة تطوره بواسطة توثيق كل شخص تناوله بالتغيير وكذلك تاريخ ووقت تجميعه أو نقله والغرض من ذلك النقل.	سلسلة متابعة الدليل

Challenge-Response Protocol	An authentication protocol where the verifier sends the claimant a challenge (usually a random value or a nonce) that the claimant combines with a shared secret (often by hashing the challenge and secret together) to generate a response that is sent to the verifier. The verifier knows the shared secret and can independently compute the response and compare it with the response generated by the claimant. If the two are the same, the claimant is considered to have successfully authenticated himself. When the shared secret is a cryptographic key, such protocols are generally secure against eavesdroppers. When the shared secret is a password, an eavesdropper does not directly intercept the password itself, but the eavesdropper may be able to find the password with an off-line password guessing attack	بروتوكول تصديق يقوم فيه المسؤول عن التحقق من الهوية بإرسال سؤال إلى صاحب الطلب الذي يقوم بدوره بدمج ذلك السؤال مع سر مشترك (عادة يتم دمج السؤال والسر معاً) لتوليد إجابة تُرسَل إلى المسؤول عن التحقق حيث يكون لديه علم بإجابة السؤال المشترك ويمكنه معرفتها بشكل مستقل ومقارنتها بالإجابة التي تلقاها من صاحب الطلب. إذا تطابقت الإجابتين يعتبر صاحب الطلب قد نجح فى الحصول على تصديق لهويته. عندما يكون السؤال المشترك عبارة عن مفتاح تشفير فإن مثل هذه البرتوكولات عموماً تتسم بالأمان ضد محاولات التصنت. أما إذا كان السؤال المشترك "كلمة مرور" فان المتصنت لا يتعرض لكلمة السر مباشرة ولكنه ربما يستطيع الحصول عليها من خلال شن هجوم لتخمين كلمة السر دون الاتصال بالشبكة.	بروتوكول سؤال وإجابة تحديد الهوية
Chief Information Officer (CIO)	Agency official responsible for:	موظف الوكالة المسؤول عن:	رئيس قطاع المعلومات

	1) Providing advice and other assistance to the head of the executive agency and other senior management personnel of the agency to ensure that information technology is acquired and information resources are managed in a manner that is consistent with laws, executive orders, directives, policies, regulations, and priorities established by the head of the agency;	**1)** إسداء النصيحة ومد يد العون لرئيس الوكالة التنفيذي والآخرين من كوادر الإدارة العليا للتأكد من تحصيل تقنية المعلومات وترتيب موارد البيانات بشكل يتوافق مع القوانين والأوامر التنفيذية والتعليمات والسياسات واللوائح والأولويات التي أرساها رئيس الوكالة.	
	2) Developing, maintaining, and facilitating the implementation of a sound and integrated information technology architecture for the agency; and Promoting the effective and efficient design and operation of all major information resources management processes for the agency, including improvements to work processes of the agency.	**2)** إعداد وصيانة وتسهيل تطبيق بنية معلوماتية سليمة تتسم بالتكامل داخل الوكالة	
		3) إنشاء تصميم فَعَّال وطريقة تشغيل متقنة لكل موارد المعلومات الرئيسية بما في ذلك تحسين	

		إجراءات العمل داخل الوكالة.	
Cipher	Series of transformations that converts plaintext to ciphertext using the Cipher Key.	سلسلة من التحويلات التي تحول نص غير مُشفَّر إلى نص مُشَفَر باستخدام مفتاح ترميز.	عملية الترميز
Cipher Block Chaining-Message Authentication Code (CBC-MAC)	A secret-key block-cipher algorithm used to encrypt data and to generate a Message Authentication Code (MAC) to provide assurance that the payload and the associated data are authentic.	خوارزمية قالب تشفير ذات مفتاح سرى تُستخدَم في تشفير البيانات واستخراج شفرة التصديق الخاصة بالرسالة بغرض التأكد من موثوقية الرسالة ومحتوياتها من بيانات.	قالب الترميز المسلسل- شفرة التصديق الخاصة بالرسالة
Cipher Key	Secret, cryptographic key that is used by the Key Expansion routine to generate a set of Round Keys; can be pictured as a rectangular array of bytes, having four rows and Nk columns.	مفتاح تشفير سرى تستخدمه دالة تمديد المفتاح لتوليد مجموعة من المفاتيح المتعاقبة ويمكن تصويرها كمصفوفة مستطيلة من وحدات البايت تتألف من أربعة صفوف وعدد غير محدد من الأعمدة.	مفتاح الترميز
Cipher Suite	Negotiated algorithm identifiers. Cipher suites are identified in human readable form using a pneumonic code.	مجموعة من عناصر التعريف تتسم بقابلية خوارزميتها للنقاش. يجري تعريف حزم الترميز بطريقة مقروءة بشرياً باستخدام شفرة مخزنة يمكن تذكرها.	حزمة الترميز

Ciphertext	Data output from the Cipher or input to the Inverse Cipher.	مخرجات البيانات من عملية الترميز أو مدخلاتها في عملية الترميز المعكوس.	نص الترميز
Claimant	A party whose identity is to be verified using an authentication protocol. An entity which is or represents a principal for the purposes of authentication, together with the functions involved in an authentication exchange on behalf of that entity. A claimant acting on behalf of a principal must include the functions necessary for engaging in an authentication exchange. (e.g., a smartcard (claimant) can act on behalf of a human user (principal))	الطرف الذي يُتحقَق من هويته باستخدام بروتوكول التصديق. كيان يكون هو نفسه رئيساً أو ممثلاً عن رئيس لاستيفاء أغراض التحقق من الهوية بالإضافة إلى الوظائف التي تتطلب تبادل لبيانات التصديق. المدعى الذي يؤدى العمل نيابة عن الرئيس يجب أن يتحلى بالصلاحيات اللازمة للشروع في تبادل بيانات التصديق على سبيل المثال امتلاك البطاقات الذكية الخاصة بالمدعى يمكن أن ينوب عن العنصر البشرى وهو الرئيس في تلك الحالة.	مقدم الطلب / المدعى
Classified Information	Information that has been determined pursuant to Executive Order (E.O.) 13292 or any predecessor order to require protection against unauthorized disclosure and is marked to indicate its classified status when in documentary form.	معلومات تم تصنيفها بناءاً على القرار التنفيذي رقم 13292 أو أي قرارات تالية بغرض الحماية ضد الكشف غير المصرح به ويتم تميزها للإشارة إلى سريتها عند تحويلها إلى الأرشيف كملفات وثائقية.	معلومات سرية / مصنفة

Client (Application)	A system entity, usually a computer process acting on behalf of a human user, that makes use of a service provided by a server.	أحد مكونات نظام معين عادة ما تكون عملية حاسوبية تعمل نيابة عن أحد العناصر البشرية حيث تستفيد من أحد الخدمات التي يوفرها خادم معين.	العميل (برنامج/تطبيق)
Cold Site	A backup facility that has the necessary electrical and physical components of a computer facility, but does not have the computer equipment in place. The site is ready to receive the necessary replacement computer equipment in the event that the user has to move from their main computing location to an alternate site.	منشأة احتياطية تضم ما يلزم من تجهيزات كهربية ومادية لتكون منشأة للحاسوب ولكنها لا تحتوى على أجهزة الحاسوب. يكون الموقع على استعداد لاستقبال أجهزة الحاسوب البديلة في حال وجوب انتقال المستخدمين من مبنى الحاسوب الرئيسي إلى مبنى آخر بديل.	موقع بارد
Collision	Two or more distinct inputs produce the same output.	اثنين أو أكثر من عناصر المدخلات تنتج نفس المخرجات.	تعارض/تصادم
Common Security Control	Security control that can be applied to one or more agency information systems and has the following properties:	الرقابة الأمنية التي يمكن تطبيقها على واحد أو أكثر من أنظمة معلومات وكالة حيث تتسم بالخصائص التالية:	الرقابة الأمنية المشتركة
	1) the development, implementation, and assessment of the control can be assigned to a responsible official or organizational	**1)** من الممكن إسناد تطوير وتنفيذ وتقييم الرقابة إلى موظف مسؤول أو أحد عناصر	

	element (other than the information system owner); and	المنظمة (غير مالك نظام المعلومات) و	
	2) the results from the assessment of the control can be used to support the security certification and accreditation processes of an agency information system where that control has been applied.	**2)** يمكن استخدام نتائج تقييم الرقابة لدعم التوثيق الأمني واعتماد الموافقة على العمليات الخاصة بنظام معلومات الوكالة التي تم تطبيق الرقابة فيها.	
Common Vulnerabilities and Exposures (CVE)	A dictionary of common names for publicly known IT system vulnerabilities.	قاموس يضم الأسماء الشائعة لأشهر الثغرات في أنظمة المعلومات.	الثغرات والمخاطر الأمنية الشائعة
Compensating Controls	The management, operational, and technical controls (i.e., safeguards or countermeasures) employed by an organization in lieu of the recommended controls in the low, moderate, or high security control baselines, that provide equivalent or comparable protection for an information system.	عناصر التحكم الإدارية والتشغيلية والفنية مثل إجراءات الوقاية وعوامل المقاومة التي يتم العمل بها داخل منظمة بدلاً من عناصر التحكم الموصى بها في الحد الأدنى من عناصر التحكم الأمني المنخفض أو المتوسط أو المرتفع بغرض توفير درجة مساوية أو مكافئة من الحماية لنظام معلومات معين.	عناصر التحكم المكافئة
Compensating Security Controls	The management, operational, and technical controls (i.e., safeguards or countermeasures)	عناصر التحكم الإدارية والتشغيلية والفنية مثل إجراءات الوقاية وعوامل المقاومة التي يتم العمل بها داخل منظمة بدلاً من	عناصر التحكم الأمني المكافئة

	employed by an organization in lieu of the recommended controls in the low, moderate, or high baselines described in NIST Special Publication 800-53, that provide equivalent or comparable protection for an information system.	عناصر التحكم الموصى بها في الحد الأدنى من عناصر التحكم الأمني المنخفض أو المتوسط أو المرتفع المذكورة في المنشور الخاص رقم 53-880 الصادر من المعهد الوطني للمقاييس والتقنية في أمريكا بغرض توفير درجة مساوية أو مكافئة من الحماية لنظام معلومات.	
Compromise	Disclosure of information to unauthorized persons, or a violation of the security policy of a system in which unauthorized intentional or unintentional disclosure, modification, destruction, or loss of an object may have occurred. The unauthorized disclosure, modification, substitution or use of sensitive data (including plaintext cryptographic keys and other critical security parameters).	الإفصاح عن معلومات لأشخاص غير مصرح لهم أو انتهاك السياسة الأمنية لنظام بالإفصاح عن أو تغيير أو تخريب أو فقد شيء سواء بنية مبيتة أو عن غير قصد. الإفصاح عن بيانات حساسة أو تغيير ها أو تبديلها أو استخدامها بدون تصريح (بما في ذلك مفاتيح تشفير النصوص غير المُشفَّرة وغيرها من المعايير الأمنية الحرجة.	انتهاك أمنى
Computer Forensics	The practice of gathering, retaining, and analyzing computer-related data	جمع بيانات متعلقة بالحاسوب والاحتفاظ بها وتحليلها من أجل أغراض	التحليل الجنائي لبيانات الحاسوب

	for investigative purposes in a manner that maintains the integrity of the data.	تقصى الحقائق بطريقة تحافظ على تكامل البيانات.	
Computer Security Incident	A violation or imminent threat of violation of computer security policies, acceptable use policies, or standard computer security practices.	انتهاك أو تهديد خطير بانتهاك السياسات الأمنية للحاسوب أو سياسات الاستخدام المتفق عليها أو الممارسات القياسية لأمن الحاسوب.	حادثة أمن الحاسوب
Computer Security Incident Response Team (CSIRT)	A capability set up for the purpose of assisting in responding to computer security-related incidents; also called a Computer Incident Response Team (CIRT) or a CIRC (Computer Incident Response Center, Computer Incident Response Capability).	قوة مهيئة للمساعدة فى الاستجابة للحوادث المرتبطة بأمن الحاسوب. يطلق عليها أيضاً فريق الاستجابة لحوادث الحاسوب أو مركز الاستجابة لحوادث الحاسوب أو قوة الاستجابة لحوادث الحاسوب	فريق التعامل مع الحوادث الأمنية للحاسوب
Computer Security Object (CSO)	A resource, tool, or mechanism used to maintain a condition of security in a computerized environment. These objects are defined in terms of attributes they possess, operations they perform or are performed on them, and their relationship with other objects.	مورد أو أداة أو آلية تُستَخدم للحفاظ على حالة من الأمن في بيئة تقوم على الحاسوب. توصف هذه العناصر طبقاً للخواص التي تمتلكها والعمليات التي تُنَفذها أو ما يتم تنفيذه عليها من عمليات بالإضافة إلى علاقاتها بالعناصر الأخرى.	عنصر أمن الحاسوب

Computer Security Objects Register	A collection of Computer Security Object names and definitions kept by a registration authority.	مجموعة من أسماء وتعريفات عناصر أمن الحاسوب محفوظة بواسطة هيئة للتسجيل.	سجل عناصر أمن الحاسوب
Computer Virus	A computer virus is similar to a Trojan horse because it is a program that contains hidden code, which usually performs some unwanted function as a side effect. The main difference between a virus and a Trojan horse is that the hidden code in a computer virus can only replicate by attaching a copy of itself to other programs and may also include an additional "payload" that triggers when specific conditions are met.	يشبه فيروس الحاسوب حصان طروادة لأنه برنامج يحتوى على شفرة مخفية يقوم عادة بتنفيذ بعض الوظائف غير المرغوبة. الاختلاف الرئيسي بين الفيروس وحصان طروادة هو أن الشفرة المخفية داخل فيروس الحاسوب يستطيع التكاثر من خلال إلصاق نسخة منه ببرامج أخرى وربما تحتوى أيضاً على عوامل تخريب تعمل فقط إذا توفرت شروط معينة.	فيروس الحاسوب
Confidentiality	Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.	الاحتفاظ بقيود مصرح بها على الوصول إلى المعلومات و الإفصاح عنها بما في ذلك وسائل حماية معلومات الخصوصية و الملكية الشخصية. خاصية أن تظل البيانات الحساسة غير معلن عنها للذين لم يُصرَح لهم من الأفراد أو الكيانات أو العمليات.	مبدأ السرية والخصوصية

Configuration Control	Process for controlling modifications to hardware, firmware, software, and documentation to ensure the information system is protected against improper modifications prior to, during, and after system implementation.	عملية للتحكم في إجراء التغييرات للأجهزة والبرمجيات وبرامج التشغيل المثبتة في ذاكرة القراءة والوثائق للتأكد من حماية نظام المعلومات ضد التغييرات الخاطئة قبل أو أثناء أو بعد تطبيق النظام.	التحكم في تهيئة/إعدادات النظام
Contingency Plan	Management policy and procedures designed to maintain or restore business operations, including computer operations, possibly at an alternate location, in the event of emergencies, system failures, or disaster.	ما تم تخطيطه من سياسة وإجراءات إدارية لحفظ واسترجاع عمليات التشغيل بما فيها عمليات الحاسوب على الأرجح في مكان بديل وذلك لاستخدامه في حالات الطوارئ وسقوط النظام والكوارث.	خطة الطوارئ
Continuity of Operations Plan (COOP)	A predetermined set of instructions or procedures that describe how an organization's essential functions will be sustained for up to 30 days as a result of a disaster event before returning to normal operations.	مجموعة من التعليمات والإجراءات المحددة سلفاً تُبين كيفية استمرار تشغيل الوظائف الأساسية لمنظمة معينة لمدة 30 يوم نتيجة لحدوث كارثة وذلك قبل العودة إلى الطريقة المعتادة في تشغيل العمليات.	خطة استمرار التشغيل
Continuity of Support Plan	The documentation of a predetermined set of instructions or procedures mandated by Office of Management and Budget (OMB) A-130 that describe how to	توثيق لمجموعة من التعليمات والإجراءات المحددة سلفاً فرضها رسمياً مكتب الإدارة والميزانية A-130 حيث تبين كيفية استمرار عمل التطبيقات الرئيسية	خطة استمرار الدعم

	sustain major applications and general support systems in the event of a significant disruption.	وأنظمة الدعم العام في حال حدوث خلل خطير.	
Control Information	Information that is entered into a cryptographic module for the purposes of directing the operation of the module.	المعلومات المُدخلة إلى وحدة تشفير نمطية بغرض إدارة تشغيل الوحدة.	معلومات التحكم
Controlled Interface	Mechanism that facilitates the adjudication of different interconnected system security policies (e.g., controlling the flow of information into or out of an interconnected system).	آلية تُيسر الحكم على سياسات أمنية لأنظمة مترابطة مختلفة (مثل التحكم في تدفق المعلومات من و إلى نظام مرتبط بغيره)	التحكم في الربط بين السياسات الأمنية
Cookie	A piece of information supplied by a web server to a browser, along with requested resource, for the browser to store temporarily and return to the server on any subsequent visits or requests.	معلومة يُرسلها خادم الويب إلى برنامج المتصفح مرفقة بالمورد المطلوب. يقوم المتصفح بتخزين تلك المعلومة مؤقتاً على أن يعيدها لخادم الويب مرة أخرى في الزيارات أو الطلبات التالية.	ملفات جمع البيانات
Counter with Cipher Block Chaining-Message Authentication Code (CCM)	A mode of operation for a symmetric key block cipher algorithm. It combines the techniques of the Counter (CTR) mode and the Cipher Block Chaining-Message Authentication Code	وضعية تشغيل لخوارزمية تشفير قالب بمفتاح متناظر. وهي تجمع بين أساليب وضعية العداد و خوارزمية "مسلسل قالب التشفير / شفرة التصديق الخاصة بالرسالة" للتأكيد	أسلوب العداد

	(CBC-MAC) algorithm to provide assurance of the confidentiality and the authenticity of computer data.	على سرية و مصداقية بيانات الحاسوب	
Countermeasures	Actions, devices, procedures, techniques, or other measures that reduce the vulnerability of an information system. Synonymous with security controls and safeguards.	أعمال أو أدوات أو إجراءات أو أساليب أو معايير أخرى تعمل على تقليل الثغرات الأمنية في نظام المعلومات. تعتبر مرادفاً لعناصر التحكم الأمني وإجراءات الوقاية.	عوامل المقاومة
Credential	An object that authoritatively binds an identity (and optionally, additional attributes) to a token possessed and controlled by a person. Evidence attesting to one's right to credit or authority.	عنصر يعمل على الربط رسمياً بين الهوية (وبشكل اختياري بعض الخواص الإضافية) وبين رمز مميز يمتلكه ويتحكم فيه شخص معين. أدلة تؤيد مصداقية أو صلاحية شخص معين.	عناصر اعتماد المصداقية