الفصل الخامس

إدارة أمـن المـعـلومـات وأمانها

لقد تَعدَّدت الاصطلاحات التي تُشير إلى مجموع العمليَّات الآتية: كيفيَّة تَقييم المعلومات وإدارة الأخطار ووَضْع الإجراءات المضادَّة التي تَكفَل حماية المعلومات في حقل أمن المعلومات، فمِنْ هذه الاصطلاحات مصطلح (**أمن العمليَّات** Operations security) الذي استخدَمَته حكومة الولايات المتَّحدة الأمريكيَّة لاحتواء العمليَّات المذكورة، وإنَّ معظم المنشورات في هذا الحقل تُسمِّي مجموع العمليَّات المذكورة **إدارة الأخطار** Risk management، ولكن لأنَّ مجموع هذه العمليَّات يَهدُف في النهاية إلى وَضْع المعلومات في حالة الأمان (بغَضِّ النظر عن مستويات هذا الأمان) ويَندرِج ضِمْن توجيهٍ واحدٍ يَقوده، فيُمكِن تَسميته: (**إدارة أمن المعلومات** Information security management)، وإدارة أمن المعلومات هي مجموع العمليَّات التي تَضمَن إدخال المعلومات وإبقاءها في وَضْع الأمان من خلال تَقييمها، وتَحديد الأخطار التي تُحيط بها وبالمحيط الذي يَحتويها، وتخطيط وتطبيق إجراءات الأمن التي تَحميها، وتخطيط وتطبيق إجراءات الأمان التي تُحافِظ على إبقائها في وَضْع الأمان، ويَتمثَّل الهدف الأساسي لإدارة أمن المعلومات في حماية المعلومات من السرقة أو الإفشاء أو التخريب، ويُدعَى الفرد الذي يَتولَّى إدارة أمن المعلومات **مدير أمن المعلومات**، ومدير أمن المعلومات هو إمّا مالِك المعلومات الذي

يَمتلِك قيمتها بالكامل، ويَتحمَّل مسؤولية سرقتها أو إفشائها أو تخريبها، أو القيِّم الذي تَقَع على عاتقه مسؤوليَّة سرقة المعلومات أو إفشائها أو تخريبها.

تُطبَّق إدارة أمن المعلومات على نماذج المعلومات الخاصَّة الثلاثة، وهي المعلومات ذات القيمة الماديَّة، أو المعنويَّة، أو المَجازيَّة، ويُدعَى تطبيق إدارة أمن المعلومات على هذه النماذج الثلاثة: إدارة المعلومات ذات القيمة الماديَّة، أو المعنوية، أو المجازية على التوالي.

1.5 مفاهيم أساسيَّة

سوف يَتم الحديث فيما يأتي عن المفاهيم الأساسيَّة المرتَبِطة بإدارة أمن المعلومات.

1.1.5 تحديد المعلومات وتقييمها

لا بد عند تطبيق إدارة أمن المعلومات من معرفة المعلومات الخاصَّة المرَاد حمايتها وتحديدها، التي تَتطلَّب إجراءات أمن وإجراءات أمان محدَّدة تَتناسَب مع قيمتها أو مع الأخطار ومستوى الأمن المطلوب لها. إنَّ الخطوة الأساسيَّة في تطبيق إدارة أمن المعلومات هي تحديد المعلومات وتقييمها، ويَتم تحديد المعلومات الخاصَّة بتمييزها ضمن مجموعة من المعلومات العاديَّة أو البيانات المتوافِرة، ومن ثم إثبات أهميَّتها إمّا ماديًّا أو معنويًّا أو مجازيًّا بالنسبة إلى الطرفين مالِك المعلومات والخصم معًا، ومعنى (إثبات أهميَّتها بالنسبة إلى الطرفين) تأكيد وجود طرف آخر (وهو الخصم) لديه مصلحة أو منفعة من الوصول إلى هذه المعلومات تُؤذي المصالح الماديَّة أو المعنويَّة أو المَجازيَّة لمالِك المعلومات، وبعد تحديد المعلومات، تُقيَّم إمَّا ماديًّا أو معنويًّا أو مجازيًّا، والهدف من تقييم المعلومات هو ضمان عدم تَجاوز التكلفة الماليَّة لتطبيق إجراءات الأمن وإجراءات الأمان، والموضوعة جميعًا لحمايتها وإبقائها في وَضْع الأمان، فقيمة

المعلومات نفسها، سواء أكانت هذه القيمة ماليَّة (إذا كانت المعلومات ذات قيمة ماديَّة) أم اعتباريَّة (إذا كانت المعلومات ذات قيمة معنويَّة أو ذات قيمة مَجازيَّة)، وتُساعِد عملية تقييم المعلومات على تَوقُّع كَم التهديدات الموجَّهة إليها بشكلٍ مباشر ووَضْع تَصوُّر مبدئي حول مستوَيَي إجراءات الأمن وإجراءات الأمان الواجب تطبيقها، وإن مَهمَّة تحديد المعلومات وتقييمها، يَنبغي أن يَقوم بها مالِك المعلومات.

2.1.5 التهديدات

إنَّ مفهوم التهديدات المحتَمَلة والموجَّهة بشكلٍ مباشر إلى المعلومات أو إلى المحيط الذي يَحتويها ضروري لتكوين فكرة مبدئيَّة عن الأخطار الناجِمة عن تنفيذ تِلْك التهديدات من خلال الثغرات الكامِنة في محيط المعلومات، لتكوين تَصوُّرات مبدئيَّة حول إجراءات الأمن التي يُمكِن تخطيطها وحول إجراءات الأمان، و**التهديد** Threat، في حقل أمن المعلومات، هو أيّ شيء محتَمَل ومتوقَّع يُمكِن أن يُسبِّب سرقةً أو إفشاءً أو تخريبًا للمعلومات، ويُؤكِّد التعريف السابق أنَّ التهديد محتَمَل الحدوث في أيّ وقت، ومتوقَّع بالنسبة إلى مالِك المعلومات، ولكنَّه خارج عن إرادته وسيطرته، وسوف يُسبِّب تنفيذ التهديد لمالِك المعلومات خسائر إمّا ماديَّة أو معنويَّة أو مَجازيَّة، ويُمكِن أن يأتي التهديد إمّا من مصدر بشري، ويُسمَّى **تهديدًا بشريًّا** أو من مصدر غير بشري، ويُسمَّى **تهديدًا غير بشري**.

ثَمَّة أربعة أشكال رئيسة للتهديدات البشريَّة هي: **تهديد الهاكرز** Hackers threat، و**البرامج الخبيثة** Malicious code ، و**برامج التجسُّس** Spyware، و**تهديد المطَّلِعين المخادِعين** Malicious insiders threat.

الهاكر – بحسب تعريفه في حقل أمن المعلومات – هو أي شخص يَستطيع النَّفاذ خِفيةً إلى الأنظمة الحاسوبيَّة والعَبَث بالبرامج والمعلومات المخزَّنة فيها دون أن يَكون مخوَّلًا بذلك، وتُمثِّل أفعال الهاكرز تهديدًا بالغًا للمعلومات الرقميَّة فقط، ويَخترق

الهاكرز الأنظمة الحاسوبيَّة إمّا من أجل التَّفاخُر بخبرتهم في هذا المجال أو من أجل منفعة ماليَّة عائِدة من طرف ثالث يَعملون لمصلحته أو لحسابهم الخاص، ويَجب على الطرف المالِك للمعلومات أن يَفترِض وجود الهاكرز، حتَّى ولو لم يَشعر بهم أو بنتائج أفعالهم، ووجود الهاكرز ليس مقرونًا بأي حدث أو زمن، بل هم موجودون سواء أَردْنا حماية المعلومات أم لم نرد، وسواء تَمَّت حمايتها أم لم تتمّ. إذًا، التهديد الذي يُمكِن أن يَأتي من الهاكرز هو نفاذهُ خِفيةً إلى النظام الحاسوبي وسرقة المعلومات الرقميَّة المخزَّنة فيه أو إفشاؤها أو تخريبها.

التهديد الثاني الذي يُمكِن أن يُطلِقه البشر هو البرامج الخبيثة، مثل **الفيروسات** Viruses **والديدان** Worms **وأحصنة طروادة** Trojan horses، وهي برامج حاسوبيَّة تُؤدِّي أعمالًا تخريبيَّة عندما تُنفّذ داخل النظام الحاسوبي، ويُوجَّه التهديد الصادِر عن البرامج الخبيثة نحو المعلومات الرقميَّة فقط (كما هو الهاكرز)، وتَنتشِر البرامج الخبيثة إمّا تلقائيًّا أو بمساعدة غير شعوريَّة من المستخدِم الجاهِل بوجودها، ويَتراوَح أذى البرامج الخبيثة بين إظهار رسائل مزعجة على الشاشة إلى تهيئة أجهزة التخزين في الحاسوب وتدمير البيانات دون إرادة المستخدِم، وتَتمّ صناعة البرامج الخبيثة من قِبَل أطراف لديها نيات انتقاميَّة تَتجلَّى في التخريب الذي تُسبِّبه تِلْك البرامج داخل حاسوب الضحيَّة، ويُمكِننا استنتاج أنَّ البرامج الخبيثة بحَدِّ ذاتها، وما تَقوم به من أذى وتخريب داخل الأنظمة الحاسوبيَّة تُعدّ تهديدًا للمعلومات الرقميَّة فقط، ومن ثم الأنظمة أو المنظومات التي ترتبط بها.

برنامج التجسُّس هو البرنامج التنفيذي المركَّب على حاسوب المستخدِم الضحيَّة دون علمه، الذي يُراقب أنشطة المستخدِم ويجمع معلوماته، مثل ضربات المفاتيح، ولقطات الشاشة، وتسجيلات الكاميرا والمايكروفون و/أو الملفات، ثمَّ إرسالها إلى الطرف الذي يُدير ذلك البرنامج، وإنَّ عمليَّة جَمْع المعلومات وإرسالها إلى الطرف الذي يُدير برنامج التجسُّس هي بحَدِّ ذاتها تهديد للمعلومات الرقميَّة.

والتهديد البشري الرابع والأكثر خطورة هو تهديد المطَّلِعين المخادِعين، والمطَّلِعون المخادعون هم الأفراد المُجَاز لهم قانونيًّا استعمال المعلومات من قِبَل مالِك المعلومات، الذين يَستخدِمون تِلْك المعلومات خِفيةً لأغراض شخصيَّة سيِّئة، وهم من الأفراد المؤتَمَنين على المعلومات من قِبَل مالِك المعلومات والموجودين داخل محيطه، وقد يَكون المطَّلِعون المخادِعون إمّا أفرادًا ضِمْن البيت الواحد لمالِك المعلومات أو موظَّفين ذوي صلاحيَّات واسعة في منظَّمة ما (قيِّمين أو مستخدِمين) أو أفرادًا مسؤولين عن حماية المعلومات المصنَّفة سريَّة وحفظها في دولة ما (قيِّمين)، ويُعدّ تهديد المطَّلِعين المخادِعين الأكثر إيذاء؛ لأنَّه يَتضمَّن خيانة الثقة التي يَمنحَها مالِك المعلومات لهؤلاء المطَّلِعين. إذًا، يَقوم المطَّلِعون المخادِعون بسرقة المعلومات المؤتَمَنين عليها من قِبَل مالِك المعلومات أو إفشائها أو تخريبها، وتُمثِّل أفعالهم هذه تهديدًا للمعلومات الرقميَّة والورقيَّة.

وقد تَأتي التهديدات أيضًا من مصادر غير بشريَّة، وتُسمَّى عندها التهديدات غير البشريَّة، مثل الكوارث الطبيعيَّة والحوادث غير المتوقَّعة، ومن أمثلة الكوارث الطبيعيَّة الزلازل والفيضانات والعواصف، ومن أمثلة الحوادث غير المتوقَّعة زيادة الطاقة الكهربائيَّة في أجهزة تخزين المعلومات والحرائق وانهيارات الأبنية، وإذا وَقعَت الكوارث الطبيعيَّة أو الحوادث غير المتوقَّعة، فسوف تُسبِّب تخريبًا لمحيط المعلومات أو لمحيط مالِك المعلومات أو لكليهما، ومن ثم للمعلومات نفسها، وإنَّ وقوع الكوارث الطبيعيَّة والحوادث غير المتوقَّعة يُعدّ تهديدًا للمعلومات الرقميَّة والورقيَّة.

ثَمَّة نوع من التهديدات من المصدر البشري، يُدعَى **التخريب المتعمَّد للممتلَكات** Vandalism، ويَأتي تهديد التخريب المتعمَّد للممتلَكات من احتمال قيام أحد ما من داخل محيط مالِك المعلومات (كالمنزل أو المنظَّمة) عَمْدًا بتخريب أجهزة تخزين المعلومات إذا كانت المعلومات رقميَّة، أو تخريب الخَزْنات الحديديَّة أو حافظات الملفات والوثائق إذا كانت المعلومات ورقيَّة، وعلى الرغم من أنَّ التخريب في هذا التهديد يكون للممتلَكات،

وليس للمعلومات، إلا أنَّ الأذى الناتج عن ذلك التخريب سيَصِل للمعلومات في نهاية الأمر.

أخيرًا تُصَنَّفُ التهديدات وفق ثلاثة أصناف بحسب تواتر وقوعها وبحسب الأثر الذي يمكن أن تُحدِثَهُ، ويبين الشكل هذا التصنيف.

دارة الأخطار المعلوماتية من المنظور العملي

الوتيرة + الأثر	الوتيرة Likelihood		الأثر Impact		التصنيف
	عالي High	+	عالي High	=	عالي High
	عالي High	+	مخفض Low	=	متوسط Medium
	مخفض Low	+	مخفض Low	=	مخفض Low

المصدر: حسن الحربي، 2014م.

3.1.5 الثغرات

عندما تُوجَد عيوب في محيط مالِك المعلومات الخاصَّة تُؤدِّي باستثمارها من قِبَل الخصم إلى سرقة المعلومات أو إفشائها أو تخريبها، فنحن بصَدَد مفهوم الثغرات، **والثغرة** Vulnerability، في حقل أمن المعلومات، هي نقطة الضعف المحتَمَلة الموجودة في محيط مالِك المعلومات، التي يُمكِن استغلالها لسرقة المعلومات أو إفشائها أو تخريبها، وثَمَّة نوعان من هذه العيوب هما: **عيب أمن** Security flaw، و**عيب أمان** Safety flaw، وعندما تَكون الثغرة موجودة في محيط مالِك المعلومات قبل تطبيق إجراءات الأمن، تُسمَّى عندها عيب أمن، وعندما تَكون الثغرة موجودة في محيط مالِك المعلومات

بعد تطبيق إجراءات الأمن (أي بعد إدخال المعلومات في وَضْع الأمان) تُسمَّى عندها عيب أمان، وقد تُوجَد الثغرة، إمّا في محيط المعلومات الإلكتروني كالنظام الحاسوبي، وتُسمَّى عندها **ثغرة إلكترونيَّة**، أو في محيط المعلومات اليدوي كالخزنة الحديديَّة التي تَحتوي على وثائق ورقيَّة، وتُسمَّى عندها **ثغرة يدويَّة**، ومن أمثلة الثغرة الإلكترونيَّة عدم وجود برنامج مضاد فيروسات في نظام حاسوبي، وتُعدّ هذه الثغرة في الوقت نفسه عيب أمن، أو وجود برنامج مضاد فيروسات غير محدَّث في نظام حاسوبي، وتُعدّ هذه الثغرة في الوقت نفسه عيب أمان، ومن أمثلة الثغرة اليدويَّة عدم وجود قفْل على خزنة حديديَّة تَضُم معلومات ورقيَّة، وتُعدّ هذه الثغرة في الوقت نفسه عيب أمن، أو وجود قفل غير مُحكَم (أي غير آمن، ويمَكِن كَسْره بسهولة) على خزنة حديديَّة تَضُم معلومات ورقيَّة، وتُعدّ هذه الثغرة في الوقت نفسه عيب أمان، وقد تُوجَد الثغرة في محيط مالِك المعلومات كالمنزل أو المنظَّمة، ولكن لأنَّ محيط المعلومات هو جزء من محيط مالِك المعلومات، فاحتمال وجود الثغرة في محيط المعلومات هو احتمال وجودها نفسه في محيط مالِك المعلومات، وقد يكون إحداث الثغرة إمّا مقصودًا، وتُسمَّى **ثغرة متعمَّدة** Intentional vulnerability، أو غير مقصود، وتُسمَّى **ثغرة عرضيَّة** Accidental vulnerability، ومن أمثلة الثغرة المتعمَّدة تعطيل برنامج مضاد فيروسات في نظام حاسوبي، ومن أمثلة الثغرة العرضيَّة إهمال أو نسيان إحكام قفْل الخزنة الحديديَّة التي تَضم المعلومات الورقيَّة على نحوٍ متكرِّر.

وكما هو واضحٌ من تعريف الثغرة السابق، فإنَّ الثغرة بحدِّ ذاتها لا تُسبِّب سرقةً للمعلومات أو إفشاءها أو تخريبها، إلا إذا قابَلها تهديدٌ ما يَستغلُّها، وإنَّ التقاء الثغرة مع التهديد المقابِل هو ما سيُشكِّل الخطر الحقيقي على المعلومات، وهذا ما سيَتمّ الحديث عنه فيما يلي.

4.1.5 الأخطار

إنَّ الأخطار الحقيقيَّة على المعلومات ليست بإطلاق التهديدات وحدها، وهي ليست فقط بوجود الثغرات في محيط مالِك المعلومات، بل هي التقاء الثغرات مع التهديدات المقابِلة لها معًا، و**الخطر** Risk في حقل أمن المعلومات، هو احتمال حدوث أذى حقيقي للمعلومات أو محيطها أو محيط مالِكها، يُسبِّب في النهاية سرقة تِلْك المعلومات أو إفشاءها أو تخريبها. إذًا، يَتشكَّل الخطر في محيط مالِك المعلومات عندما تُوجَد فيه ثغرة ما، وفي الوقت نفسه يُطلَق تهديد مقابِل يَستغلُّ تِلْك الثغرة، ويُمكِننا أن نَنظُر إلى الخطر بصيَغ عدَّة، فمثلًا يُمكِن القول: إنَّ الخطر يَتشكَّل بتَقاطُع الثغرة مع تهديد مقابِل، أو أنَّ الخطر = الثغرة + التهديد، وإنَّ أمثلة تَشكُّل الأخطار كثيرة، ومن أبسطها وجود ثغرة إلكترونيَّة (ولتَكُن عدم وجود برنامج مضاد للفيروسات) في محيط معلومات إلكتروني (وليَكُن نظامًا حاسوبيًّا) مع إطلاق تهديد (وليَكُن برنامجًا خبيثًا أو فيروسًا) يُشكِّلان خطرًا على تِلْك المعلومات.

يُدعَى الخطر عند تَشكُّله باسم شكل التهديد البشري المقابِل، عندما يَكون التهديد بشريًّا، مثل خطر الهاكرز، وخطر المطَّلِعين المخادِعين، ويُدعَى الخطر عند تَشكُّله خطرًا غير بشري، عندما يكون التهديد غير بشري، أمّا التهديد المتمثِّل في التخريب المتعمَّد للممتلَكات فيُدعَى الخطرُ المقابِلُ له عند تَشكُّله خطرَ التخريب المتعمَّد للممتلَكات.

وتَتراوَح أساليب التَّعامُل مع الخطر بين محاولة الابتعاد عنه أو تقليل احتمال تَشكُّله أو قَبوله ونَقله إلى طرفٍ آخر، وثَمَّة أربعة خيارات للتَّعامُل مع الخطر ومَنْعِ تَشكُّله هي: **اجتناب الخطر** Risk avoidance، و**تخفيف الخطر** Risk mitigation، و**قَبول الخطر** Risk acceptance، و**تحويل الخطر** Risk transference [17، 13].

الخيار الأول هو اجتناب الخطر، ويَتم تَبنِّي هذا الخيار عندما تَكون المنفعة العائِدة من محاولة مَنْعِ تَشكُّل الخطر أقل بكثير من تكلفة مَنْعِ تشكُّله، ويَتم تطبيق هذا الخيار من

خلال اجتناب العوامل التي قد تُؤدِّي إلى تَشكُّل الخطر، ومن أمثلة اجتناب الخطر قيام إدارة منظَّمة ما بمَنْع موظَّفيها من تَبادُل رسائل بريد إلكتروني مع خارج المنظَّمة تَجنُّبًا لإرسالهم (سواء عَمْدًا أو عن غَير قَصْد) رسائل تَحوي معلومات أعمال خاصَّة.

والخيار الثاني من خيارات التَّعامُل مع الخطر ومَنْعِ تشكُّله هو تخفيف الخطر، وهو الأكثر شيوعًا، ويَتم تطبيق هذا الخيار من خلال اتِّخاذ إجراءات مضادَّة وقائيَّة متمثِّلةً في سَدِّ الثغرات الموجودة في محيط مالِك المعلومات ومَنْعِ تهديدات محدَّدة من استغلالها، ومن أبسط أمثلة تخفيف الخطر القيام بتركيب برنامج مضاد فيروسات في نظام حاسوبي للحماية من فيروس محدَّد.

والخيار الثالث هو قَبول الخطر، ويَتم قَبول الخطر عندما تَكون احتمالات تَشكُّله ضعيفة جدًّا، مثل احتمال وقوع زلزال شديد القوة في منطقة غير زلزالية تاريخيًّا، أو عندما تَكون تكلفة تَشكُّل الخطر صغيرة جدًّا مقارنةً بتكلفة تطبيق الإجراءات المضادَّة.

والخيار الرابع والأخير هو تحويل الخطر، ويَتم تطبيق هذا الخيار من خلال تحويل الخطر إلى طرف ثانٍ يَقبَل تَحمُّل أعباء تَشكُّل الخطر، والمثال الأبرز لهذا الخيار هو قيام شركة تأمين بتَحمُّل أعباء تَشكُّل الخطر مع مالِك المعلومات عن طريق قيام مالِك المعلومات بشراء بوليصة تأمين منها.

5.1.5 الإجراءات المضادَّة

المَهمَّة الأساسيَّة في إدارة أمن المعلومات هي تطبيق الإجراءات المضادَّة التي تَكفُل إحباط تَشكُّل الأخطار، **والإجراءات المضادَّة** Countermeasures في حقل أمن المعلومات، هي مجموعة من الأفعال العمليَّة والتنظيمية أو الإدارية التي تَهدُف إلى إحباط تَشكُّل الأخطار على المعلومات أو محيطها أو محيط مالِكها من خلال سَدِّ الثغرات ومَنْع التهديدات من استغلالها، والأفعال العمليَّة هي الأدوات التي يَتم استخدامها، مثل

البرامج الحاسوبيَّة والأنشطة، مثل حماية الأبنية التي تَحتوي على المعلومات الخاصَّة سواء رقميَّة أم ورقيَّة وبناء الأسوار حول تِلْك الأبنية، وما إلى ذلك. أمّا الأفعال الإدارية فتَعني السياسات التي تُلزِم الاضطلاع بالمسؤوليَّات المتعلِّقة بحماية المعلومات، والنصائح والتوجيهات المرتَبِطة بكيفيَّة الحفاظ على سلامة المعلومات، التي يَتم إصدارها من قِبَل المَعنيين والموجَّهة نحو الأفراد.

ولا يُمكِن في حقل أمن المعلومات الجزم بمواجَهة جميع التهديدات القائمة، ولكن يَكفي لمَنْع تَشكُّل الخطر سَدّ الثغرات التي من المُمكِن أن تَستغلّها التهديدات، وعمومًا فإن هَدَف تطبيق الإجراءات المضادَّة هو سَدّ الثغرات فقط؛ لأنَّ سَدّ الثغرة يُعدّ بحَدِّ ذاته مواجَهة للتهديد القائِم، ولكن من ناحية المَعني بحماية المعلومات، فمثلًا لا يُمكِن مواجَهة تهديد فيروس ما من خلال مقاوَمة انتشاره عالميًّا عَبْر الشبكة، ولكن يُمكِن سَدّ الثغرة التي قد يَستغلُّها تهديد ذلك الفيروس بتركيب برنامج مضاد فيروسات للحماية منه.

ثَمَّة نوعان من الإجراءات المضادَّة هما: **إجراءات أمن** Security measures، و**إجراءات أمان** Safety measures، وإجراءات الأمن هي الإجراءات المضادَّة التي يَتم تطبيقها من أجل إدخال المعلومات في وَضْع الأمان، وتُطبَّق إجراءات الأمن مرَّة واحدة على الأقل، ويُمكِن إعادة تطبيقها من جديد في حال تَمَّ تعديلها كليًّا أو جزئيًّا، وتُحاوِل إجراءات الأمن معالجة عيوب الأمن. أمّا إجراءات الأمان فهي الإجراءات المضادَّة التي يَتم تطبيقها بعد إدخال المعلومات في وَضْع الأمان، وتُطبَّق إجراءات الأمان باستمرار وعلى نحوٍ دوري بهَدَف إبقاء المعلومات في وَضْع الأمان، وتُحاوِل إجراءات الأمان معالجة عيوب الأمان التي قد تَظهَر عند ظهور تهديدات جديدة، وتَتَّخِذ الإجراءات المضادَّة (سواء أكانت إجراءات أمن أم إجراءات أمان) إمّا شكل **إجراءات وقائيَّة** Preventive measures أو شكل **إجراءات علاجيَّة** Remedial measures، والإجراءات الوقائيَّة هي الإجراءات المضادَّة التي تَسعى إلى مَنْع تَشكُّل الأخطار من خلال سَدِّ الثغرات التي

يُمكِن أن تَستغلّها تهديدات مقابِلة، أمّا الإجراءات العلاجيَّة فهي الإجراءات المضادَّة التي تُحاوِل تفكيك خطر (أو أخطار) بعد تَشكُّله من خلال القيام بسَدِّ الثغرة التي سَبَق، واستغلَّها التهديد واستعادة المعلومات السليمة إذا اختُرِقَ أمانها وإعادة محيط المعلومات إلى ما كان عليه قبل تَشكُّل الخطر، وتَتعامَل الإجراءات العلاجيَّة مع حوادث الأمان أيضًا (انظر الفقرة 3.8).

2.5 أمن المعلومات ذات القيمة الماديَّة

المعلومات ذات القيمة الماديَّة هي المعلومات التي يُمكِن أن تُعيد منافع ماليَّة عندما تُستثمَر آنيًّا، كأرقام الحسابات المصرفيَّة، ومعلومات الأعمال الخاصَّة، والمشروعات الاقتصاديَّة، ومالِك هذه المعلومات هو إمّا فردًا أو منظَّمةً أو حكومةً، وأمن هذه المعلومات هو تطبيق إدارة أمن المعلومات، كما تَمَّ تعريفها على المعلومات ذات القيمة الماديَّة، ويَتألَّف أمن المعلومات ذات القيمة الماديَّة من خمس مراحل هي:

1. المرحلة الأولى: تحديد المعلومات وتقييمها ماديًّا.
2. المرحلة الثانية: تحديد التهديدات المحتَمَلة وتحليلها.
3. المرحلة الثالثة: تحديد الثغرات وتحليلها.
4. المرحلة الرابعة: تقييم الأخطار.
5. المرحلة الخامسة: تطبيق الإجراءات المضادَّة.

1.2.5 المرحلة الأولى: تحديد المعلومات وتقييمها ماديًّا

تُعدّ هذه المرحلة مهمة جدًّا؛ لأنها تَرسم الإطار العريض حول المعلومات ذات القيمة الماديَّة التي يَنبغي الاهتمام بها وحمايتها من السرقة أو الإفشاء أو التخريب، والخطوة الأولى من هذه المرحلة هي تحديد المعلومات ذات القيمة الماديَّة، ويَتم تحديد ذلك من خلال تمييزها من بين مجموعة من المعلومات العاديَّة أو البيانات المتوافرة،

ومن ثمَّ إثبات أهميَّتها بالنسبة إلى الطرفين مالِك المعلومات والخصم معًا، ويَقتضي إثبات أهميَّة المعلومات ذات القيمة الماديَّة بالنسبة إلى الطرفين تأكيد وجود طرف آخر لديه مصلحة ماليَّة في الوصول إلى هذه المعلومات تُؤذي المصالح الماليَّة لمالِك المعلومات، ويَنبغي أيضًا معرفة هؤلاء الخصوم المحتَمَلين، وهم الأطراف البشريَّة المعروفون بالنسبة إلى مالِك المعلومات، مثل قريب أو صديق أو صاحب منظَّمة ما منافِسة (سواء أكانت تجاريَّة أم صناعيَّة) أو حكومة دولة ما منافِسة، وقد يَكون الخصم طرفًا بشريًّا مجهولًا مثل الهاكرز.

الآن، وبعد تحديد المعلومات ذات القيمة الماديَّة ومعرفة الخصوم المحتَمَلين، يَجب تجميع كل هذه المعلومات مع بعضها، ويَعني ذلك جَمْع المعلومات (سواء أكانت رقميَّة أم ورقيَّة) في مكان واحد دون النَّظَر إلى نسبة أهميَّة بعض المعلومات منها عن الأخرى، والسبب في ذلك هو أنَّ ثَمَّة معلومات منها قد تَعود بنفعٍ مالي صغير، لكنَّها مرتَبِطة بشكلٍ أو بآخر بمعلومات أخرى من الطبيعة نفسها تَعود بنفعٍ مالي كبير، بحيث لو تَمَّت سرقة المعلومات ذات النفع المالي الصغير أو إفشاؤها أو تخريبها سيُؤثِّر مع الوقت (عاجلًا أم آجلًا) في المعلومات ذات النفع المالي الكبير، وسيُسبِّب أذًى، ومن ثم يَجب تطبيق الإجراءات المضادَّة نفسها على المعلومات ذات النفع المالي الصغير والكبير، وعمليًّا يَتضمَّن تجميع كل هذه المعلومات تجميع الملفات التي تَحتوي على المعلومات في الحاسوب وتَضمينها في وسائط تخزين المعلومات الرقمية نفسها إذا كانت هذه المعلومات رقميَّة، أو تجميع الملفات التي تَحتوي على المعلومات في مكان واحد إذا كانت هذه المعلومات ورقيَّة، وإنَّ الهدف النهائي من تَجميع كل المعلومات ذات القيمة الماديَّة معًا هو تجهيزها بالكامل لتطبيق إجراءات الأمن وإجراءات الأمان عليها.

الخطوة الثانية من هذه المرحلة هي تقييم المعلومات ماديًّا، والهدف الأساسي من هذا التقييم هو ضَمان عدم تَجاوُز التكلفة الماليَّة لتطبيق الإجراءات المضادَّة النَّفْع المالي الذي يُمكِن أن تُعيده المعلومات عندما يَتم استثمارها، ويَتم تقييم المعلومات

ماديًّا من خلال حساب النَّفْع المالي من استثمار جميع هذه المعلومات آنيًّا، فعلى سبيل المثال، لو كانت المعلومات ذات القيمة الماديَّة عبارة عن أرقام الحسابات المصرفيَّة الشخصيَّة لطرفٍ ما، يكون النَّفْع المالي من استثمار هذه المعلومات آنيًّا مساويًا مجموع الأموال النقديَّة الموجودة في المصارِف، التي تَرتبِط بها أرقام الحسابات تِلْك، ولو كانت المعلومات ذات القيمة الماديَّة عبارة عن الأسرار الصناعيَّة لمنتَجٍ ما جديد، يكون النَّفْع المالي من استثمار هذه المعلومات آنيًّا مساويًا الأرباح الصافية التي يُمكِن أن تَعود بها صناعة المنتَج وبَيْعه. إذًا، لكل معلومات ذات قيمة ماديَّة طريقتها الخاصَّة في حساب النَّفْع المالي من استثمارها آنيًّا، ويتولى هذه المهمَّة مالِك المعلومات أو مدير أمن المعلومات، والمهم في النهاية هو أن تَكون التكلفة الماليَّة لتطبيق الإجراءات المضادَّة أقل من النَّفْع المالي من استثمار المعلومات آنيًّا.

2.2.5 المرحلة الثانية: تحديد التهديدات المحتَمَلة وتحليلها

تُحدِّد المعلومات ذات القيمة الماديَّة طبيعة التهديدات المحتَمَلة الموجَّهة بشكلٍ مباشر إليها وإلى محيطها، والخطوة الأولى من هذه المرحلة هي استقصاء جميع التهديدات المحتَمَلة، وتَنقسِم التهديدات المحتَمَلة والموجَّهة بشكلٍ مباشر إلى المعلومات ذات القيمة الماديَّة وإلى محيطها إلى قسمين هما: **تهديدات متعمَّدة** Intentional threats، و**تهديدات غير متعمَّدة** Unintentional threats، والتهديدات المتعمَّدة هي تهديد الهاكرز، وبرامج التَجسُّس، وتهديد المطَّلِعين المخادِعين، والتخريب المتعمَّد للممتلَكات، أمّا التهديدات غير المتعمَّدة فهي التهديدات غير البشريَّة.

الخطوة الثانية من هذه المرحلة هي تحليل التهديدات المحتَمَلة، فإنَّ الدافع وراء التهديدات المتعمَّدة هو الحصول على المنافع الماليَّة مهما كان مقدارها من خلال الوصول إلى المعلومات ذات القيمة الماديَّة، مهما كانت كَميَّتها، أمّا التهديدات غير المتعمَّدة فتؤدي على الأغلب إلى تخريب تِلْك المعلومات، وتَقَع من باب المصادفة، ويَنبغي

تركيز الاهتمام على التهديدات المتعمَّدة؛ لأنَّها تَقَع بنسبة أكبر من وقوع التهديدات غير المتعمَّدة، والسبب في ذلك هو أنَّ مُطلِقِي هذه التهديدات يُدرِكون أنَّ ثَمَّة منافع ماليَّة من الحصول على المعلومات ذات القيمة الماديَّة أو من إفشائها أو تخريبها، أمّا مُطلِقو التهديدات غير المتعمَّدة فيُوجِّهونها إلى جميع المعلومات سواء أكانت خاصَّة أم عامَّة، وسواء أكانت معلومات أم بيانات؛ لأنَّ دافعهم هو الإيذاء فقط.

وللهاكرز منافع ماليَّة من إدراك المعلومات ذات القيمة الماديَّة، وقد تَتَحقَّق هذه المنافع، إمّا بالحصول على هذه المعلومات، أو بإفشائها أو تخريبها لمصلحة أطراف أخرى، ويُوجَّه تهديد الهاكرز المتعمَّد في هذا النموذج من المعلومات الخاصَّة إلى المعلومات فقط، أمّا برامج التَجسُّس فتُطلِقها أطراف محدَّدة لها منافع ماليَّة أيضًا من إدراك المعلومات ذات القيمة الماديَّة، وتَتَحقَّق منافعهم هذه بالحصول على هذه المعلومات لمصلحتهم أو لمصلحة أطراف أخرى من خلال تركيبهم لتِلْك البرامج في حواسيب الضحايا، ويُوجَّه التهديد المتعمَّد المتمثِّل في برامج التَجسُّس في هذا النموذج من المعلومات الخاصَّة إلى المعلومات فقط، وأيضًا المطَّلِعون المخادِعون لهم منافع ماليَّة من الوصول إلى المعلومات ذات القيمة الماديَّة، وتَتَحقَّق منافعهم الماليَّة من خلال سرقة هذه المعلومات أو إفشائها أو تخريبها لمصلحتهم أو لمصلحة أطراف أخرى يتعامَلون معها، ويَقَع التهديد المتعمَّد الصادر عن هؤلاء بكثرة في المنظَّمات، ويُوجَّه تهديدهم المتعمَّد في هذا النموذج من المعلومات الخاصَّة إلى المعلومات وإلى محيطها أيضًا[1]، وأمّا التخريب المتعمَّد للممتلَكات فقد يقوم به أطراف لهم مصالح ماليَّة من قيامهم بهذا التخريب تَرتبِط بأطراف خارج محيط مالِك المعلومات، ويُسبِّب التخريب المتعمَّد للممتلَكات إيذاءً مباشرًا للمعلومات ذات القيمة الماديَّة، ويُوجَّه هذا

(1) السبب في أنَّ تهديد المطَّلِعين المخادِعين يُوجَّه إلى محيط المعلومات أيضًا هو أنَّ المطَّلِع المخادِع قد يَقوم أيضًا، من باب الأذى، بتخريب محيط المعلومات، سواء أكانت المعلومات رقميَّة أم ورقيَّة.

النوع من التهديد للممتلَكات في هذا النموذج من المعلومات الخاصَّة إلى المعلومات، وإلى محيطها، وإلى محيط مالِكها.

تُطلَق البرامج الخبيثة إلى جميع الأنظمة الحاسوبيَّة عَبْر الشبكات، وليسَ لمُطلِقي البرامج الخبيثة أيّ مصالح ماليَّة مباشرة، إلا أنَّ مصالحهم العامَّة تَتَحقَّق من خلال إصابة تِلْك البرامج للأنظمة الحاسوبيَّة، مسبِّبةً تخريبًا على الأقل للبيانات على نحوٍ عام، وللمعلومات ذات القيمة الماديَّة على نحوٍ خاص، ويُوجَّه التهديد المتمثِّل في البرامج الخبيثة في هذا النموذج من المعلومات الخاصَّة إلى المعلومات وإلى محيطها، وأمّا التهديدات غير البشريَّة فتُطلَق مصادفةً، وعلى أساس إطلاقها العَرَضيّ، فقد تُسبِّب تخريبًا لجميع المعلومات دون تحديد (سواء أكانت خاصَّة أم عاديَّة، وسواء أكانت ذات قيمة ماديَّة أم غيرها) وللبيانات على نحوٍ عام.

3.2.5 المرحلة الثالثة: تحديد الثغرات وتحليلها

قَبْل تحديد الثغرات، يَنبغي معرفة محيط المعلومات الذي يَضمّ المعلومات ذات القيمة الماديَّة، وتُساعِد عملية جَمْع هذه المعلومات على معرفة محيط المعلومات، والخطوة الأولى من هذه المرحلة هي تحديد الثغرات، ويَتم ذلك من خلال فَحْص كامِل محيط المعلومات (سواء أكان محيطًا إلكترونيًّا أم محيطًا يدويًّا) من أجل اكتشاف الثغرات التي يُحتَمَل أن تُوجَد فيه، وسوف تَكون الثغرات المحتَمَل وجودها في محيط المعلومات عيوب أمن؛ لأنَّ ظهورها سيَكون قبل تطبيق إجراءات الأمن، وتَختلِف آلية فَحْص محيط المعلومات الذي يَضم المعلومات ذات القيمة الماديَّة بين محيط المعلومات الإلكتروني ومحيط المعلومات اليدوي، فإذا كان محيط المعلومات إلكترونيًّا (مثل الأنظمة الحاسوبيَّة وشبكاتها)، عندها يُمكِن استعمال أدوات الفحص المؤتَمَتَة التجاريَّة التي تُساعِد على اكتشاف الثغرات التي يَستخدِمها الخصوم في شَنِّ هجماتهم، وإذا كان محيط المعلومات يدويًّا (مثل الخزنة الحديديَّة التي تَحتوي على الملفات

والوثائق الورقيَّة)، عندها يَنبغي فَحْص محيط المعلومات يدويًّا، وإنَّ عملية فَحْص محيط المعلومات اليدوي يدويًّا سهلة على خلاف المحيط الإلكتروني الذي يَتطلَّب أدوات حاسوبيَّة خاصَّة لفَحْصه، وبعد فَحْص محيط المعلومات، يَجب فَحْص محيط مالِك المعلومات الذي يَتَمثَّل في الإطار الفيزيائي الذي يُحيط المعلومات أيضًا، وذلك بهدف التَّأكُّد من عدم وجود عيوب أمن فيه، مثل هَشاشة الجدار الأسمنتي للغرفة وقابليَّة وقوعه على محيط المعلومات ومقاوَمة مناخ الغرفة للظروف الجويَّة، مثل ارتفاع درجة الحرارة ومقاوَمة الغرفة للحرائق.

الآن، وبعد تحديد الثغرات المحتَمَلة الموجودة في محيط المعلومات الإلكتروني أو اليدوي أو في محيط مالِك المعلومات، يُمكِن في الخطوة الثانية من هذه المرحلة تحليل هذه الثغرات من خلال مطابَقة التهديدات المقابِلة معها، فمثلًا لو كانت الثغرات التي تَمَّ تحديدها في الخطوة الأولى إلكترونيَّة، يُمكِن وَضْع تهديد الهاكرز، وبرامج التجسُّس، والبرامج الخبيثة، وتهديد المطَّلِعين المخادِعين، والتخريب المتعمَّد للممتلَكات في قائمة التهديدات المحتَمَلة، أما إذا كانت هذه الثغرات يدويَّة، فيُمكِن وَضْع تهديد المطَّلِعين المخادِعين، والتهديدات غير البشريَّة، والتخريب المتعمَّد للممتلَكات في قائمة التهديدات المحتَمَلة، ولو كانت الثغرات مكتَشَفة في محيط مالِك المعلومات، يُمكِن وَضْع التهديدات غير البشريَّة في قائمة التهديدات المحتَمَلة، ويَجب في الخطوة الثانية من هذه المرحلة أيضًا تحديد فيما إذا كانت الثغرات التي تَمَّ اكتشافها في الخطوة الأولى هي ثغرات متعمَّدة أم ثغرات عرضيَّة؛ لأنَّ التأكيد بأن تَكون الثغرة متعمَّدة هو التأكيد بوجود خصمٍ ما يُحاوِل إحداثَها وفقًا لمصالح خاصَّة به أو بأطراف أخرى، وإنَّ التأكيد بأن تَكون الثغرة عرضيَّة هو تأكيد بأنَّ هناك إهمالًا غير مقصود قد يَكون بسيطًا، ولكن يُؤدِّي تَجاهُله إلى استغلال الثغرة من قِبَل تهديدٍ ما مقابِل.

4.2.5 المرحلة الرابعة: تقييم الأخطار

من الصعب إضفاء قيمة ماليَّة محدَّدة لخطرٍ يهدد المعلومات ذات القيمة الماديَّة، وقبل الحديث عن تقييم الأخطار، يَنبغي أولًا ترتيب الأخطار على المعلومات ذات القيمة الماديَّة وفق مقدار الأذى الذي يُسبِّبه تَشكُّل الخطر، والترتيب الأساسي لهذه الأخطار من الأشَدِّ إلى الأخَفِّ وخيارات التَّعامُل مع كل واحد منها هو:

1. خطر الهاكرز، ويَتمّ التّعامُل معه بخيار (تخفيف الخطر).
2. خطر برامج التجسُّس، ويَتمّ التّعامُل معه بخيار (تخفيف الخطر).
3. خطر المطَّلِعين المخادِعين، ويَتمّ التّعامُل معه بخيار (اجتناب الخطر).
4. خطر البرامج الخبيثة، ويَتمّ التّعامُل معه بخيار (تخفيف الخطر).
5. خطر التخريب المتعمَّد للممتلَكات، ويَتمّ التّعامُل معه بخيار (تحويل الخطر).
6. خطر الحوادث غير البشرية، ويَتمّ التّعامُل معه بخيار (تحويل الخطر).

ويجري تقييم الأخطار على المعلومات ذات القيمة الماديَّة بتطبيق الخطوات الخمس الآتية:

1. الخطوة الأولى: إعداد قائمة كاملة بالثغرات التي تَمَّ اكتشافها في المرحلة الثالثة.
2. الخطوة الثانية: إعداد قائمة بالتهديدات المحتَمَلة ومطابقَتها مع قائمة الثغرات المعدَّة في الخطوة الأولى وإعداد قائمة بالأخطار التي يُحتَمَل تَشكُّلها من استغلال قائمة التهديدات المحتَمَلة المعدَّة في هذه الخطوة لقائمة الثغرات المعدَّة في الخطوة الأولى.
3. الخطوة الثالثة: ترتيب قائمة الأخطار وفقًا للترتيب الأساسي للأخطار الحقيقيَّة على المعلومات ذات القيمة الماديَّة من الأشَدِّ إيذاءً إلى الأخَفِّ إيذاءً والمذكور في الفقرة السابقة.

4. الخطـوة الرابعـة: إضفـاء مجمل القيمـة الماديَّة للمعلومات، لـكل خطر يُحتَمَل تَشـكُّله في القائمة المعدَّة في الخطوة الثالثة، والآن إذا احتَوَت قائمة الأخطار المحتَمَل تَشـكُّلها والمعدَّة في الخطوة الثالثة على خطر واحد على الأقل، يَجب علـى مديـر أمـن المعلومات أنَّ يُقرِّر رسـميًّا وبشـكلٍ صريح تطبيـق الإجراءات المضادَّة.
5. الخطـوة الخامسـة: تحديـد أسـاليب التّعامُـل مـع كل خطر في قائمـة الأخطار المعدَّة في الخطوة الثالثة وفقًا لخيارات التّعامُل مع كل خطر.

بَعْد تقييم الأخطار في الخطوات الخمس السابقة، يُمكِن الانتقال إلى المرحلة الخامسة والأخيرة من أمن المعلومات ذات القيمة الماديَّة، لتطبيق الإجراءات المضادَّة بحسب أساليب التّعامُل مع كل خطر والمحدَّدة في الخطوة الخامسة من تقييم الأخطار.

5.2.5 المرحلة الخامسة: تطبيق الإجراءات المضادَّة

يَجري في هذه المرحلة تطبيق الإجراءات المضادَّة التي تَكفل مَنْع تَشكُّل الأخطار. عمومًا، ثَمَّة نوعان من الإجراءات المضادَّة سيَتم تطبيقهما في هذه المرحلة، هما: إجراءات أمن، وإجراءات أمان، وتَضمَن إجراءات الأمن إدخال المعلومات الخاصَّة في وَضْع الأمان، أمّا إجراءات الأمان فتَضمَن إبقاء المعلومات الخاصَّة في وَضْع الأمان.

يَنبغي قَبْل كلِّ شيء أن يُدرِك مدير أمن المعلومات المكلف بالتطبيق ضرورة الموازَنة بين القيمة الماديَّة للمعلومات وتكلفة تطبيق إجراءات الأمن وإجراءات الأمان، وإنَّ تكلفة تطبيق هذه الإجراءات لا تَشمَل تكلفة وَضْعها وتخطيطها؛ لأنَّ هذه الإجراءات مخطَّطة وموضوعة مسبقًا، ولذا تَنطوي التكلفة فقط على تطبيقها، وفي البداية يَجب أن يَختار مدير أمن المعلومات تطبيق جميع الإجراءات المضادَّة، ويَقوم بحساب تكلفة ذلك، وإذا كانت تكلفة تطبيق الإجراءات المضادَّة أكبر من القيمة الماديَّة للمعلومات، فعندها يَنبغي اختيار عدد أقل من إجراءات الأمن وإجراءات الأمان، وبعدها حساب

تكلفة تطبيقها من جديد، وتَعود آليَّة اختيار الإجراءات المضادَّة ذات التكلفة الأقل لتطبيقها إلى مدير أمن المعلومات؛ لأنَّ هذا الأمر له احتمالات متعدِّدة مثل تَوافُر أو عدم تَوافُر بعض الإجراءات في المُتناوَل لتطبيقها وجَواز أو عدم جَواز تطبيق بعض الإجراءات من قِبَل السلطات الحكوميَّة.

إن إجراءات أمن المعلومات ذات القيمة الماديَّة هي بالترتيب:

1. اختيار الموقع الفيزيائي المناسِب (أي محيط مالِك المعلومات) إمّا للأجهزة والمعدَّات الحاسوبيَّة التي ستَحتَوي على المعلومات إذا كانت المعلومات رقميَّة، أو للمعدَّات اليدويَّة التي ستَحتفِظ بالوثائق والمستندات التي تَضمّ المعلومات إذا كانت المعلومات ورقيَّة.
2. توظيف الأفراد الموثوقين والمؤتَمَنين المفوَّض إليهم استعمال المعلومات الخاصَّة.
3. إذا كانت المعلومات الخاصَّة رقميَّة ومشتَرَكة، وتتطلب التواصل في بيئة كبيرة (كمنظَّمة مثلًا)، يَنبغي عندها حماية الشبكة الحاسوبيَّة التي سيَتم عَبرها تَبادُل المعلومات الخاصَّة من خلال اختيار إحدى طُرُق التصميم المُثلَى للشبكة لحمايتها، كتَقسيم الشبكة، وتركيب جدار ناري، وتركيب نظام اكتشاف التطفُّل، أو استعمال شبكة خاصَّة افتراضيَّة.
4. تركيب برامج موثوقة مضادَّة للبرامج الخبيثة وبرامج التَجسُّس في الأنظمة الحاسوبيَّة التي تُخزِّن المعلومات إذا كانت المعلومات رقميَّة.
5. نَسْخُ جميع المعلومات الخاصَّة احتياطيًّا من خلال إجراء نُسَخ رقميَّة عدَّة إذا كانت المعلومات رقميَّة، أو تصوير الوثائق والمستندات التي تَضمّ المعلومات مرات عدَّة إذا كانت المعلومات ورقيَّة.
6. حماية مَضمون جميع المعلومات الأصليَّة من خلال تَعميتها (تشفيرها) باستخدام إحدى المُعمِّيات المعياريَّة أو التجاريَّة الموثوقة أو المطورة محليًّا،

ومفتـاح سـرِّي طويل نسـبيًّا ومختَلَط المحـارِف إذا كانت المعلومـات رقميَّة، أو الاحتفـاظ بهـا في خزنـة حديديَّة مُحكَمـة الإقفال إذا كانـت المعلومات ورقيَّة. بعدهـا، يَنبغـي حماية مَضمون جميـع المعلومات الرقميَّة المنسـوخَة من خلال تَعميتهـا بالمعمِّـي نفسـه الـذي اسـتُعمِلَ في تَعميـة المعلومـات الأصليَّـة، ولكن بمفتـاح سـرِّي ومختَلِف عن المفتاح السـرِّي الذي اسـتُخدِم لتعميـة المعلومات الأصليَّة، والهدف من اسـتعمال مفتاح سـرِّي مختَلِف هو تَفادي مشـكلة نَسـيان المفتـاح السـرِّي الـذي اسـتُعمِلَ لتَعميـة المعلومـات الأصليَّـة أو ضَياعـه، وأمّـا حمايـة مَضمـون جميع المعلومات الورقيَّة المنسـوخَة فتَتمّ من خلال الاحتفاظ بهـا فـي خزنة حديديَّة أخـرى مُحكَمة الإقفال على أن تَكـون موضوعة في مكان مختلـف عن مكان الخزنة التي تَحتوي على المعلومات الورقيَّة الأصليَّة، ويَنبغي الاحتفـاظ بالمفتاحيـن السـرِّيَّين اللذَيـن اسـتُخدِما لتَعميـة جميـع المعلومات الأصليَّـة والمنسـوخَة في مكان آمـن للعودة إليهما من قِبَل الأطراف المشـارِكة فـي اسـتعمال المعلومات إذا كانت هذه المعلومات مشـتَرَكة، أو الاحتفاظ بهما لدى مالِك المعلومات شخصيًّا إذا كانت هذه المعلومات غير مشتَرَكة.

7. أمّـا إذا كانـت المعلومـات ورقيَّـة فيَنبغـي الاحتفـاظ بالمفتاحيـن اليدويَّيـن للخزنتَيـن اللتَيـن تَحويـان جميـع الوثائـق والمسـتندات التـي تَضـمّ المعلومات الأصليَّـة والمنسـوخة في مكان آمن جدًّا، بحيث تَسـهُل العـودة إليهما إذا كانت المعلومات مشتَرَكة أو في مكان سرِّي لا يَعلمُه إلا مالِك المعلومات شخصيًّا إذا كانت المعلومات غير مشتَرَكة.

أمّا إجراءات أمان المعلومات ذات القيمة الماديَّة فهي بالترتيب:

1. اسـتخدام ضوابِـط الأمن الفيزيائي فـي محيط مالِك المعلومـات الذي يَحتوي علـى المعـدَّات والأجهـزة الرقميَّـة أو المعـدَّات اليدويَّـة التي تَضـمّ المعلومات الرقميَّة أو الورقيَّة.

2. فَحْص محيط المعلومات دوريًّا من خلال استعمال أدوات الفَحْص المؤَتمَتة التجاريَّة التي تُساعِد على اكتشاف الثغرات في الأنظمة الحاسوبيَّة وفي الشبكة الداخليَّة لمنظَّمة ما مثلًا إذا كانت المعلومات رقميَّة، أو التَّأكُّد من سلامة محيط المعلومات بالنَّظَر إليه بالعين المجرَّدة وتَحديد فيما إذا كانت ثَمَّة عيوب فيه أم لا إذا كانت المعلومات ورقيَّة.
3. تحديث البرامج المضادَّة للبرامج الخبيثة وبرامج التَّجسُّس باستمرار.
4. التَّحقُّق من الخلفية الائتمانية للموظَّفين الموكَّلين باستخدام المعلومات الخاصَّة في منظَّمة ما، مثلًا بين مدةٍ وأخرى، ويَتم ذلك من خلال تَركيب برامج تَجسُّس في الأنظمة الحاسوبيَّة التي يَتم فيها استخدام المعلومات الخاصَّة واستثمارها، التي يَعمَل عليها هؤلاء الموظَّفون لتسجيل جميع أنشطتهم على هذه الأنظمة الحاسوبيَّة؛ وذلك بهَدَف حماية المعلومات الخاصَّة من أن تَتم سرقتها وتسريبها لخارج محيط مالِك المعلومات، واستعمال التسجيلات ونتائج المراقبة كدليل إدانة للموظَّف الذي أَقدَم على هذه الخطوة من الخيانة والسرقة، ولا يُعدّ هذا انتهاكًا لخصوصيَّة الفرد؛ لأنَّ المعلومات الخاصَّة والأنظمة الحاسوبيَّة التي تَضمّها ليست ملكًا لهذا الفرد.

وعليه فإنَّ أي أمر يَقوم به الموظف مستخدِمًا المعلومات الخاصَّة أو النظام الحاسوبي الذي يَضمّها خارج صلاحيات عمله يُعدّ انتهاكًا من قِبَله لأمان هذه المعلومات، ولا يَملك أي حَقّ للشكوى من التجسُّس عليه، الآن لمَنْع الموظَّف من تركيب برمجيات تَمنَع برامج التَّجسُّس في النظام الحاسوبي الذي يَعمَل عليه من أداء عملها داخل محيط مالِك المعلومات، يُمكِن استخدام برامج متخصِّصة تَمنَع أي تلاعب سواء إضافة أو إزالة أو تعديل لأي برنامج في النظام الحاسوبي.

5. تطبيـق آليَّـة متكامِلـة للولوج إلـى المعلومات الخاصَّـة، بحيث تَمْنَـح الموظَّفين داخـل منظَّمـة ما حَقّ الوصول إلى المعلومات التـي يَحتاجون إليها فقط، وتُقيِّد حريَّتهم بالوصول إلى المعلومات التي لم يُرخَّص لهم استعمالها.
6. إتلاف المعلومات الخاصَّة الرقميَّة أو الورقيَّة عند الانتهاء من استثمارها على نحوٍ يَستحيل استرجاعها كليًّا أو جزئيًّا.

3.5 أمن المعلومات ذات القيمة المعنويَّة

المعلومات ذات القيمة المعنويَّة هي المعلومات التي تَفوق أهميَّتها وحساسيَّتها أي قيمة ماديَّة لها مهما بَلَغ مقدار هذه القيمة، وهذا يُشير إلى أنَّ المعلومات ذات القيمة المعنويَّة هي المعلومات المصنَّفة سريَّة لدى حكومات الدول، والمعلومات الدوليَّة المصنَّفة سريَّة التي يَتشارَك بها طرف دولي، ويَعني ذلك أنَّ ملكيَّة المعلومات ذات القيمة المعنويَّة جماعيَّة، وتَعود إلى دولة أو إلى طرف دولي، وأمن المعلومات ذات القيمة المعنويَّة هو تطبيق إدارة أمن المعلومات عليها، ويتألَّف هذا الأمن من خمس مراحل أيضًا هي:

1. المرحلة الأولى: تحديد المعلومات وتقييمها معنويًّا.
2. المرحلة الثانية: تحديد التهديدات المحتَمَلة.
3. المرحلة الثالثة: تحديد الثغرات.
4. المرحلة الرابعة: تقييم الأخطار.
5. المرحلة الخامسة: تطبيق الإجراءات المضادَّة.

1.3.5 المرحلة الأولى: تحديد المعلومات وتقييمها معنويًّا

يَتمّ تحديد المعلومات في هذه المرحلة من خلال اختيار المعلومات المصنَّفة سريَّة فقط (إذا كانت متعلِّقة بدولة ما) أو المعلومات الدوليَّة المصنَّفة سريَّة (إذا كانت

متعلِّقة بطرف دولي) من بين مجموعة من المعلومات الخاصَّة الأخرى[1]. ليسَ من مهام مدير أمن المعلومات إضفاء أو إلغاء صفة السريَّة على المعلومات الخاصَّة الحكوميَّة أو المعلومات الخاصَّة المرتَبِطة بطرف دولي، إنَّما تَقتصِر مَهمَّته في هذه المرحلة فقط في اختيار المعلومات الخاصَّة التي قَامَت السلطات الحكوميَّة العليا في الدولة أو السلطات العليا في الطرف الدولي رسميًّا بإقرارها مصنَّفة سريَّة، ويُمكِن تحديد الخصوم المحتَمَلين الذين لهم مصلحة في إدراك هذه المعلومات على أنَّهم الأعداء القائِمون الظاهريون والمَخفيون لدولة معنيَّة أو للمجموعة التي تُشكِّل طرفًا دوليًّا.

على خلاف العمليَّة التي تَمَّ فيها تقييم المعلومات ماديًّا، لا توجد عمليَّة واضحة وسهلة تَستطيع تقييم المعلومات معنويًّا.

2.3.5 المرحلة الثانية: تحديد التهديدات المحتَمَلة

تَختلِف التهديدات المحتَمَلة والموجَّهة إلى المعلومات ذات القيمة المعنويَّة وإلى محيطها عن التهديدات المحتَمَلة والموجَّهة إلى المعلومات ذات القيمة الماديَّة وإلى محيطها، فالتهديدات المحتَمَلة والموجَّهة إلى المعلومات ذات القيمة الماديَّة وإلى محيطها تَحتوي على جميع أشكال التهديدات البشريَّة والتهديدات غير البشريَّة، أمّا التهديدات المحتَمَلة والموجَّهة إلى المعلومات ذات القيمة المعنويَّة وإلى محيطها فلا تَحتوي إلا على ثلاثة أشكال منها، والسبب يَعود إلى طبيعة المعلومات الخاصَّة التي تَقتصِر هنا على المعلومات المصنَّفة سريَّة بمستوياتها المختلفة، فالمعلومات المصنَّفة سريَّة عمومًا، سواء أكانت حكوميَّة أم مرتَبِطة بطرف دولي بعيدة كل البعد على أن تَكون مخزَّنة أو مشارَكًا بها في الطُّرُق التقليديَّة نفسها المستخدَمة في تخزين أو مشارَكة المعلومات ذات القيمة الماديَّة أو حتَّى المعلومات ذات القيمة المَجازيَّة، وهي قد تَكون

(1) تُترَك حماية المعلومات الخاصَّة الأخرى غير المعلومات المصنَّفة سريَّة إلى جهات حكوميَّة عاديَّة يُمكِنها استعمال أدوات مناسبة لذلك.

مشارَكًا بها في شبكة داخل محيط مالِك المعلومات، ولكنَّها بالتأكيد معزولة تمامًا عن الشبكة الخارجيَّة كالإنترنت، وهذا نابعٌ من إدراك المَعنيين بإقرار سريَّة هذه المعلومات لأهميَّتها البالغة.

عمومًا، ثَمَّة ثلاثة تهديدات محتَمَلة وموجَّهة إلى المعلومات ذات القيمة المعنويَّة هي: تهديد المطَّلِعين المخادِعين، والتهديدات غير البشريَّة، والتخريب المتعمَّد للممتلَكات، وإنَّ احتمال وقوع التهديدات غير البشريَّة والتخريب المتعمَّد للممتلَكات ضعيف بسبب حِرْص الحكومة أو الطرف الدولي على التأمين الفيزيائي الشديد للمعلومات ومحيطها ومحيط مالِكها، أمّا تهديد المطَّلِعين المخادِعين فهو التهديد الأكثر وقوعًا في كثير من الدول، وإنَّ أمثلة وقوع ذلك كثيرة، ومن هذه الأمثلة ذلك الذي شَكَّل قضيَّة شَغَلت الرأي العام الأمريكي في منتصف عام 2013م عندما قَام الموظَّف السابق في وكالة الأمن القومي الأمريكيَّة Edward Snowden بتصوير الوثائق الورقيَّة المصنَّفة سريَّة التي احتَوَت على ممارسات الوكالة بمراقبة الاتصالات الهاتفيَّة والمعامَلات الإلكترونيَّة عبر الإنترنت، ثمَّ تسليمها إلى الصحافة العالميَّة لنَشرها، فقد أَحرَج الأمر الذي قَام به Snowden الحكومة الأمريكيَّة أمام الرأي العام الأمريكي والرأي العام العالمي، وسَبَّب أذًى كبيرًا لأمن الجيش الأمريكي (على حَدِّ قولهم) وخسائر وَصَلت قيمتها لبلايين الدولارات، وأيضًا من أمثلة وقوع تهديد المطَّلِعين المخادِعين الوثائق الورقيَّة المصنَّفة سريَّة وبعضها من مستوى التصنيف (سرِّي جدًّا) التي تَمَّ تسريبها ونَشْرَها في موقع WikiLeaks الإلكتروني.

3.3.5 المرحلة الثالثة: تحديد الثغرات

تُحَدَّدُ الثغرات في هذه المرحلة بالأسلوب نفسه الذي تَمَّ فيه تحديد الثغرات في أمن المعلومات ذات القيمة الماديَّة، وذلك من خلال فَحْص كامِل محيط المعلومات (سواء أكان محيطًا إلكترونيًّا أم محيطًا يدويًّا) من أجل اكتشاف الثغرات التي يُحتَمَل

أن تُوجَد فيه، وعلى ما يُعتَقَد أنَّ الثغرات التي يُمكِن أن تَستغلّها التهديدات غير البشريَّة والتخريب المتعمَّد للممتلَكات والموجَّهة إلى المعلومات ذات القيمة المعنويَّة ضعيفة نسبيًّا بسبب مَتانة محيط مالِك المعلومات، ولكنَّ الثغرة التي يُمكِن أن يَستغلَّها تهديد المطَّلِعين المخادِعين، والتي تَتمثَّل في إهمال الحَذَر من قيام أحد القيِّمين أو أحد المستخدِمين للمعلومات الخاصَّة المصنَّفة سريَّة (الحكوميَّة أو الدوليَّة) بخيانة الثقة وسرقة هذه المعلومات أو إفشائها أو تخريبها، فهي جَليَّة.

4.3.5 المرحلة الرابعة: تقييم الأخطار

في البداية يَنبغي معرفة الأخطار على المعلومات ذات القيمة المعنويَّة وترتيبها قبل تقييمها، والأخطار الحقيقيَّة على المعلومات ذات القيمة المعنويَّة وترتيبها بحسب مقدار الأذى الذي يُسبِّبه تَشكُّل تِلْك الأخطار من الأشدِّ إلى الأخفِّ وخيارات التَّعامُل مع كل واحد منها هي:

1. خطر المطَّلِعين المخادِعين- ويَتم التّعامُل معه بخيار (اجتناب الخطر).
2. خطر التخريب المتعمَّد للممتلَكات- ويَتم التّعامُل معه بخيار (اجتناب الخطر).
3. الخطر غير البشري- ويَتم التّعامُل معه بخيار (اجتناب الخطر).

تَنطوي جميع خيارات التّعامُل مع الأخطار على المعلومات ذات القيمة المعنويَّة تحت (اجتناب الخطر)؛ لأنَّ المَعنيين بهذه المعلومات، المُمثَّلين بالسلطات العليا، سواء في الدولة أو في الطرف الدولي، لا يُريدون تَدخُّل أي جهة كانت لمَنْع تَشكُّل الخطر إلا الأطراف البشريَّة الموظَّفة والمُجَازة من قِبَلهم.

ولأنَّ خطر التخريب المتعمَّد للممتلَكات والخطر غير البشري صغيران بالنسبة إلى خطر المطَّلِعين المخادِعين، يُمكِن تَركيز الاهتمام على الخطر الأخير، والآن إذا كان هناك احتمال قيام أحد القيِّمين أو المستخدِمين للمعلومات المصنَّفة سريَّة (مهما كانت درجة وظيفتهم) بخيانة الثقة، عندها يُمكِن إقرار ذلك بوصفه تهديدًا محتَمَلًا

واعتبار إهمال الحَذَر منه كثغرة وإقرار احتمال تَشكُّل الخطر رسميًّا، ولكن على خلاف الخطوة الرابعة في تقييم الأخطار على المعلومات ذات القيمة الماديَّة، التي يَجب فيها إقرار تطبيق الإجراءات المضادَّة، يَنبغي هنا تطبيق إجراءات الأمن قبل مراحل تحديد التهديدات وتحديد الثغرات وتقييم الأخطار، ومن ثمَّ تطبيق إجراءات الأمان بعد مرحلة تقييم الأخطار، والسبب في اتِّخاذ هذه الخطوة الاستباقيَّة هو أنَّ أهميَّة المعلومات ذات القيمة المعنويَّة تَتطلَّب القيام بإجراءات احتياطيَّة قبل مناقشة جميع التهديدات والثغرات والأخطار المحتَمَلة، فإذا تَمَّ بعدها الإحساس باحتمال إطلاق تهديد ووجود ثغرة مسبقًا، يُمكِن عندها التّعامُل مع الخطر المشكَّل ضمن إجراءات الأمان، وليس إجراءات الأمن، وهذا لا يَعني دون شك تطبيق إجراءات الأمان فقط عند الإحساس باحتمال تَشكُّل خطر، بل إنَّ محاولة مَنْع تشكُّل خطر تَقَع ضمن إجراءات الأمان، إذْ يَنبغي تطبيق إجراءات الأمان على نحوٍ دوري فَوْر تطبيق إجراءات الأمن، وقد يَعتقِد بعضهم أنَّ تكلفة تطبيق إجراءات الأمن قبل مراحل تحديد التهديدات وتحديد الثغرات وتقييم الأخطار قد تَكون أكبر من قيمة المعلومات نفسها، ولكنَّ هذا الأمر غير صحيح؛ لأنَّه أولًا، المعلومات ذات القيمة المعنويَّة محدَّدة مسبقًا ومقرَّرة بصفة معلومات مصنَّفة سريَّة أو معلومات دوليَّة مصنَّفة سريَّة. وثانيًا، لا يَهتَم المعنيُّون بهذه المعلومات بأيّ تكلفة ماليَّة ضخمة يَتحمَّلونها لتطبيق إجراءات الأمن قبل تقييم الأخطار؛ لأنَّ هذه المعلومات تَرتبِط بالمصلحة العامَّة للمجتمع.

5.3.5 المرحلة الخامسة: تطبيق الإجراءات المضادَّة

إنَّ هذه المرحلة هي أهم مرحلة في أمن المعلومات ذات القيمة المعنويَّة؛ لأنَّها تُشكِّل حاجزَين أساسيَّين أمام سرقة المعلومات أو إفشائها أو تخريبها، وهذان الحاجزان هما إجراءات الأمن وإجراءات الأمان، ولكن على الرغم من احتواء هذه المرحلة على كلٍّ من إجراءات الأمن وإجراءات الأمان، إلا أنَّه، وكما ذَكرنا سابقًا، يَجب تطبيق إجراءات

الأمن قبل مراحل تحديد التهديدات وتحديد الثغرات وتقييم الأخطار، فإجراءات الأمن هي الحاجِز الأول الذي يَسعى إلى تأخير محاولة سرقة المعلومات المصنَّفة سريَّة أو إفشائها أو تخريبها، وأمّا إجراءات الأمان فهي الحاجز الثاني الذي يَستطيع مَنْع المطَّلِعين المخادِعين من القيام بأيّ محاولة ضارة.

إجراءات أمن المعلومات ذات القيمة المعنويَّة هي بالترتيب:

1. اختيار الموقع الفيزيائي الآمن، إمّا للأجهزة والمعدَّات الحاسوبيَّة التي ستَحتوي على المعلومات إذا كانت المعلومات رقميَّة، أو للمعدَّات اليدويَّة التي ستَحتفِظ بالوثائق والمستندات التي تَضم المعلومات إذا كانت المعلومات ورقيَّة، ويَنبغي أن يَكون الموقع الفيزيائي آمنًا من التهديدات غير البشريَّة، كالكوارث الطبيعيَّة والحوادث غير المتوقَّعة، وآمنًا من الهجمات البشريَّة مهما كان مَصدرها، ولإضافة هامش أمان إلى المكان الفيزيائي للمعلومات ذات القيمة المعنويَّة، يَنبغي أن يَكون الموقع مَخفيًّا عن الأعين، بحيث لا تُوجد شارات أو لافتات تَدلُّ على صفته أو على ماذا يَحتوي.
2. استخدام ضوابِط الأمن الفيزيائي الكَشفيَّة والوقائيَّة في محيط المكان الذي يَضم المعدَّات والأجهزة الرقميَّة أو المعدَّات اليدويَّة التي تَضم المعلومات الرقميَّة أو الورقيَّة، والسبب في عدم استخدام الضوابِط الرادِعة هو احتواؤها على أدوات ومواد إعلاميَّة تَدلُّ على طبيعة المكان، وذلك يُخالِف الإجراء الأول السابق.
3. تَوظيف أفراد موثوقين ومؤتَمَنين جدًّا بوصفهم قيِّمين أو مستخدِمين للمعلومات المصنَّفة سريَّة أو المعلومات الدوليَّة المصنَّفة سريَّة، ويَتم هذا الإجراء من خلال دراسة السيرة الذاتيَّة والتَحقُّق من الخلفيَّة الائتمانيَّة لكل فرد منهم قبل إسناد المَهام إليهم.

4. عَـزْلُ جميع الأنظمة الحاسـوبيَّة المخطَّط لها أن تَضـم المعلومات ذات القيمة المعنويَّة عن أي شبكة خارجيَّة أو داخليَّة، وعدم تَركيب أي برامج لا تَمُتّ بصلة (من قريب أو من بعيد) للتّعامُل مع هذه المعلومات في الأنظمة الحاسوبيَّة التي ستُخزِّنها، وذلك إذا كانت المعلومات الخاصَّة رقميَّة.
5. الاحتفـاظ بالمعلومـات الرقميَّة على وسـائط تخزين تَكون صالحـة مدة طويلة جـدًّا، وهذا يَعني أنه يَنبغي أيضًا مجاراة الصناعة الحديثة لوسـائط التخزين باسـتمرار؛ لمتابعـة حِفْـظ المعلومات الخاصَّـة الرقميَّة المخطَّط لهـا أن تَبقى مَحميَّة مدَّة طويلة.
6. عدم نَسْخِ أيٍّ من المعلومات الرقميَّة أو تصوير الوثائق والمستندات التي تَضم المعلومات الورقيَّة.
7. حماية مضمون جميع المعلومات المصنَّفة سـريَّة من خلال تَعميتها باستخدام أدوات تَعمويَّـة موثوقـة وقويَّـة وخاصَّـة بهـذه المعلومـات وغيـر معروفـة تجاريًّا ومفتـاح سـرِّي طويل نسـبيًّا ومختَلَط المحـارِف إذا كانت المعلومـات رقميَّة، أو الاحتفـاظ بهـا في خزنـة حديديَّة مُحكَمَـة الإقفال إذا كانـت المعلومات ورقيَّة. بعدهـا، يَجـب الاحتفـاظ بالمفتاح السـرِّي الرقمـي أو المفتاح اليـدوي مع أكثر القيِّمين ائتمانًا.

أمّا إجراءات أمان المعلومات ذات القيمة المعنويَّة فهي بالترتيب:

1. فَحْـص محيط مالِك المعلومات دوريًّا؛ للتَأكُّد من سـلامته وخُلوِّه من أي عيوب أمان والتَّحقُّق من عدم وجود أي ثغرة مهما كانت صغيرة.
2. التَّحقُّـق باسـتمرار مـن الخلفيـات الائتمانيَّـة لجميـع القيِّميـن والمسـتخدِمين للمعلومـات ذات القيمـة المعنويَّة؛ للتَأكُّد من اسـتمراريَّة أمانتهم تجاه التّعامُل مـع هـذه المعلومـات، وأفضل الطُّرُق للتحقُّـق من الخلفيـات الائتمانيَّة للقيِّمين

والمستخدِمين هي مراقبتهم فيما يَتعلَّق بتَحرُّكاتهم المرتَبِطة من قريب أو من بعيد بتَعامُلهم مع المعلومات ذات القيمة المعنويَّة.

3. تطبيق آليَّة دقيقة لولوج المستخدِمين إلى المعلومات الخاصَّة ذات القيمة المعنويَّة، بحيث تَمنَح المستخدم الذي يَحتاج فعلًا إلى هذه المعلومات، وبترخيص من رؤسائه، حَقّ الوصول المحدود، وتُقيِّد حريَّة وصول المستخدِمين إلى المعلومات التي لا يَحتاجون إليها أصلًا في عَمَلهم، ولم يُرخَّص لهم ذلك من رؤسائهم.
4. إتلاف جميع المعلومات الخاصَّة ذات القيمة المعنويَّة الرقميَّة أو الورقيَّة عند الانتهاء من استخدامها على نحوٍ يَستحيل تمامًا استرجاعها كليًّا أو جزئيًّا.

4.5 أمن المعلومات ذات القيمة المَجازيَّة

عندما تَكون ثَمَّة معلومات شخصيَّة تَخصُّ طرفًا بشريًّا ليست ذات قيمة معنويَّة وفي الوقت نفسه لا تَحمِل قيمةً ماديَّةً، فهذه المعلومات هي معلومات ذات قيمة مَجازيَّة، وأمثلة هذه المعلومات كثيرة، منها حسابات صناديق البريد الإلكتروني، والمذكِّرات الشخصيَّة، وما إلى ذلك. ولهذا النوع من المعلومات أيضًا إدارة أمن معلومات تُطبَّق عليها، ويُدعَى تطبيقها أمن المعلومات ذات القيمة المَجازيَّة.

إنَّ عمليَّة تحديد المعلومات المجازية وتقييمها بسيطة، وتَتم من خلال اختيار المعلومات التي تَحتوي على خصوصيَّات شخصيَّة فقط، ولكنَّها لا تَحمِل أي قيمة ماديَّة. مما لا شك فيه، فلن تَكون ثمّة معلومات ذات قيمة مَجازيَّة مختَلَطة مع معلومات ذات قيمة معنويَّة، ولكن إذا كانت المعلومات الخاصَّة ذات القيمة المَجازيَّة تَرتبِط من قريب أو من بعيد بمعلومات ذات قيمة ماديَّة، يَنبغي عندها عَزْلُ المعلومات ذات القيمة الماديَّة عنها لتطبيق أمن المعلومات ذات القيمة الماديَّة عليها، ويَتم تقييم المعلومات ذات القيمة

المَجازيَّة بأنها لا تَحمِل أي مؤشِّر مادِّي، إلا أنَّها تَدلُّ على أنَّ هذه المعلومات شخصيَّة فقط.

وعلى الرغم من اختلاف المعلومات ذات القيمة المَجازيَّة عن المعلومات ذات القيمة الماديَّة، إلا أنَّ التهديدات الموجَّهة إليها هي التهديدات نفسها الموجَّهة إلى المعلومات ذات القيمة الماديَّة، والسبب هو أنَّ طبيعة محيط مالِك المعلومات ذات القيمة المَجازيَّة قريبة جدًّا من طبيعة محيط مالِك المعلومات ذات القيمة الماديَّة، وهذا يَقتضي أيضًا أنَّ الثغرات التي يُمكِن أن تُوجَد في محيط مالِك المعلومات ذات القيمة المَجازيَّة هي نفسها الموجودة في محيط مالِك المعلومات ذات القيمة الماديَّة. أما التهديدات المحتَمَلة الموجَّهة إلى المعلومات ذات القيمة المَجازيَّة فهي: تهديد الهاكرز، والبرامج الخبيثة، وبرامج التَجسُّس، والتهديدات غير البشريَّة، ولم يُذكَر تهديد المطَّلِعين المخادِعين والتخريب المتعمَّد للممتلَكات في السَّرْد السابق؛ لأنَّ الحافِظ الوحيد للمعلومات ذات القيمة المَجازيَّة هو مالِكها فقط، ولا تَستدعي طبيعة هذه المعلومات أن تَكون مؤتَمَنة مع أيِّ كان، وإنَّ مالِكها سيَشعُر بانتهاك خصوصيَّته الشخصيَّة إذا اخترق أحدٌ غيره هذه المعلومات.

بعد تعرُّف التهديدات المحتَمَلة والثغرات التي يُمكِن أن تَستغلَّها تِلْك التهديدات، يُمكِن ترتيب الأخطار الحقيقيَّة على المعلومات ذات القيمة المَجازيَّة المحتَمَل تَشكُّلها بحسب مقدار الأذى الذي قد تُسبِّبه من الأشدِّ إلى الأخفِّ، وعَرْض خيارات التّعامُل مع كلٍّ منها على النحو الآتي:

1. خطر الهاكرز- ويَتم التّعامُل معه بخيار (تخفيف الخطر).
2. خطر برامج التَّجسُّس- ويَتم التَّعامُل معه بخيار (تخفيف الخطر).
3. خطر البرامج الخبيثة- ويَتم التّعامُل معه بخيار (تخفيف الخطر).
4. الخطر غير البشري- ويَتم التّعامُل معه بخيار (قَبول الخطر).

وتَتمثَّل الإجراءات المضادَّة في أمن المعلومات ذات القيمة المَجازيَّة في مجموعة من التدابير الاحترازيَّة، ومهمَّة هذه التدابير ضَمان عدم اختراق أي طرف بشري للمعلومات ذات القيمة المَجازيَّة العائِدة لطرف بشري آخر، وتَدمُج هذه التدابير إجراءات الأمن وإجراءات الأمان معًا، والسبب في تسمية مجموعة الإجراءات المضادَّة هنا التدابير الاحترازيَّة هو أنَّ الإجراء المضادّ بحَدِّ ذاته (سواء أكان إجراء أمن أم إجراء أمان) ذو تكلفة ماليَّة، ولو كانت قليلة، أمّا التدبير الاحترازي فهو ليس سوى فِعْل لا يَحتاج إلى ممارسة أو خبرة، وتكلفته الماليَّة قليلة تَصِل إلى الصفر في أغلب الأحيان، وعمومًا التدابير الاحترازيَّة لحماية المعلومات ذات القيمة المَجازيَّة، وهي بالترتيب:

1. تَركيب برنامج تجاري موثوق (وقليل التكلفة) مضادّ للبرامج الخبيثة وبرامج التَجسُّس في النظام الحاسوبي الذي يُخزِّن هذه المعلومات إذا كانت المعلومات رقميَّة.
2. نَسْخُ جميع المعلومات الرقميَّة ذات القيمة المَجازيَّة والاحتفاظ بها في قرص ليزري أو مُخزِّن بيانات بعيد عن النظام الحاسوبي.
3. حماية مضمون جميع المعلومات ذات القيمة المَجازيَّة من خلال تَعميتها باستخدام إحدى المُعميِّات التجاريَّة العاديَّة ذات التكلفة الماليَّة القليلة ومفتاح سرِّي قصير وآمن إذا كانت المعلومات رقميَّة، أو الاحتفاظ بها في مكان آمن قريب من مالِكها وبعيد عن الأعين وعن متناوَل الأيدي إذا كانت المعلومات ورقيَّة.
4. تَحديث البرنامج المضادّ للبرامج الخبيثة وبرامج التَجسُّس باستمرار.
5. إتلاف المعلومات الخاصَّة ذات القيمة المَجازيَّة الرقميَّة أو الورقيَّة عند الانتهاء من استخدامها على نحوٍ يَستحيل استرجاعها.

5.5 المعيار العالمي في إدارة حماية المعلومات ISO 27001/2

طوّرت منظمة المقاييس الدولية ISO سلسلة من المعايير أو المواصفات الدولية متخصصة بأمن المعلومات، وهي ISO27001 وISO27002، التي يطلق عليها نظم إدارة حماية المعلومات (المتطلبات)، إذ تعطي المواصفة ISO27001 نموذجًا عامًّا لتطبيق نظم إدارة حماية المعلومات وتشغيلها وتحسينها Information Security Management ISMS System. إن غاية منظمة ISO التنسيق بين معايير ISO27001 لإدارة حماية المعلومات مع معايير نظم الإدارة الأخرى مثلًا ISO9001:2000 التي تتعلق بنظم إدارة الجودة، وكذلك ISO14001:2004 التي تخاطب نظم إدارة البيئة.

تزود مواصفة ISO27001 وISO27002 إدارات المنظمات الصناعية والخدمية بتوجيهات لتطبيق نظم إدارة حماية المعلومات ISMS، فضلًا على حصولها على شهادة الطرف الثالث[1] الدولية لإثبات كفاءة المنظمة في حماية معلوماتها، التي تعمل طبقًا لمتطلبات المعايير الدولية، إضافة إلى مراقبة نظام ISMS واستدامته من قبل منظمة ISO، وبهذا يعالج نظام إدارة حماية المعلومات كل أطوار الهيكل التنظيمي، والسياسات، وخطط النشاط، والمسؤوليات، والممارسات، والإجراءات، والعمليات، وأخيرًا مصادر المعلومات.

إن التطبيق الفعّال لـ ISO27001 وISO27002 يوفر للإدارة العليا وسائل المراقبة والسيطرة على حماية المعلومات، ويقلل من أخطار العمل الناشئ عن عدم الحصول على المعلومات بالدقة المطلوبة، وكذلك من خطر تسرب المعلومات، فبعد تطبيق المنظمة المواصفة تضمن حماية معلوماتها رسميًّا للتواصل مع الزبون وشرعية (قانونية) المنظمة، إضافة إلى إرضاء متطلبات أصحاب المصالح لدى المنظمة.

تُعدُّ المواصفتان ISO27001 وISO27002 قاعدةً لتقييم نظام إدارة حماية المعلومات (ISMS) المتكامل، وإنها الوثيقة التي تقيّم أي نظام لإدارة حماية المعلومات.

---

(1) وهي الجهة المانحة للشهادة ISO27001.

عمليات المعالجة ISO27001:2013 وفوائد تطبيقها:

تُعَدُّ المواصفة ISO27001 التي صدرت عام 2005م، ثم تطورت لتصدر عام 2013م، والمواصفة ISO27002 معيارَي الحماية الدولي الرسمي المقدم لأي منظمة ترغب في الحصول على شهادة مستقلة لنظام إدارة حماية المعلومات، لهذا تحدد المواصفة المتطلبات الإلزامية لتأسيس نظام ISMS وتطبيقه وتوثيقه، وتحديد متطلبات التحكم لحماية المعلومات التي ستطبق وفق حاجات المنظمة الخاصة بها، وتشمل المواصفة الأولى منهما (11) مركزًا للتحكم و(39) هدفًا للسيطرة، إضافة إلى (133) موقعًا للسيطرة متوافقًا مع المواصفة ISO17799 التي تعمل من خلال أنموذج (PDCA) Plan – Do – Check – Act الذي يقوم بعمل التحسين المستمر، ويشتمل على مرحلتي أمن وأمان المعلومات الذي وصفناه باختصار في مطلع الفصل، وبهذا تستند المواصفة ISO27001 في عملها على تسعة أجزاء للمعالجة التي حددها تحالف صناعة حماية شبكات الإنترنت [1] CSIA يمكن تلخيصها فيما يأتي:

1. تعريف المجال لنظام إدارة حماية المعلومات ISMS.
2. تعريف سياسة حماية المعلومات.
3. تقييم الأخطار/ التحليل.
4. إدارة الخطر.
5. تحديد الأهداف للسيطرة والسيطرة الفعلية عليها/ التطبيق.
6. تجهيز بيان (كشف) التطبيق.
7. تطبيق ISMS وتشغيله.
8. استمرار المراقبة ومراجعة ISMS.
9. إدامة ISMS وتحسينه.

---

(1) Cyber Security Industry Alliance.

أما المعيار الثاني ISO27002، لمنظمة المواصفات الدولية ISO، فيُطبّق بوصفه تعليمات تساعد على تطبيق ISO27001 لإنجاز نظام ISMS بشكل فعال من خلال الآتي:

1. تقييم الأخطار والمعالجة.
2. سياسة الحماية.
3. تنظيم حماية المعلومات؟
4. إدارة الموجودات.
5. حماية معلومات الموارد البشرية.
6. حماية الطبيعة والبيئة.
7. إدارة العمليات والاتصالات.
8. السيطرة على دخول قواعد البيانات.
9. الحصول على نظم المعلومات، والتطوير، والإدامة.
10. إدارة حوادث لحماية المعلومات.
11. إدارة استمرارية العمل.
12. الالتزام (الالتزام بتطبيق بنود المواصفة).

وتجدر الإشارة في نهاية هذه الفقرة إلى أن ثمة فوائد ومنافع عدة واضحة من العمل على الحصول على شهادة المواصفة ISO27001:2005.

6.5 توجهات عامة عالمية في تحقيق الأمن والأمان المعلوماتي

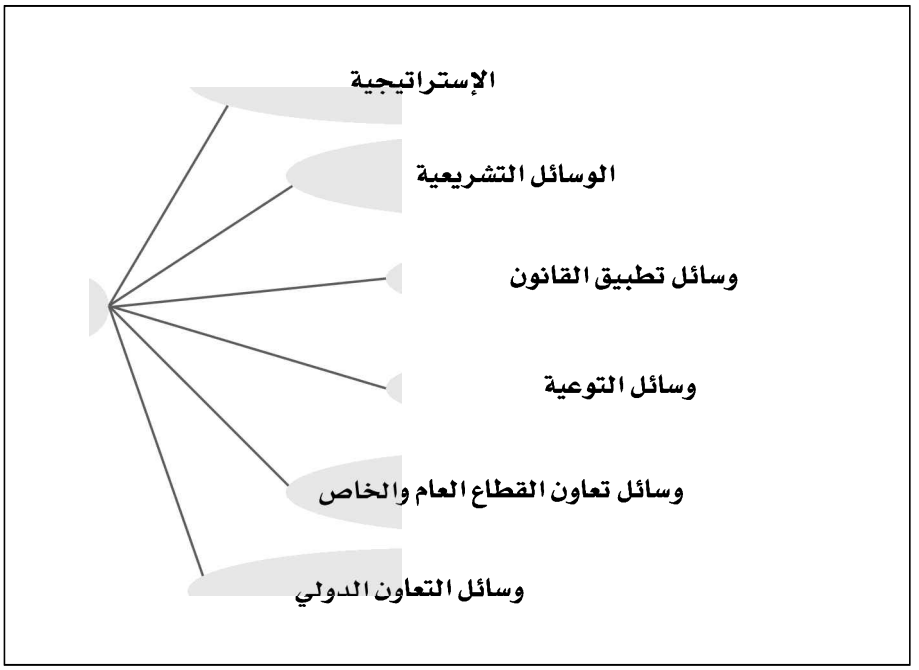
فيما يأتي لمحة عن الجهود العامة المبذولة على الصعيد العالمي المتمثلة في خمسة أنواع من التوجهات نبوّبها فيما يأتي[1]، ويبيّن الشكل توضيحًا لمعالمها الرئيسة:

(1) المصدر: اللجنة الاقتصادية والاجتماعية لغربي آسيا، الإسكوا.

1. التوجهات التشريعية:

- تطبيق التشريعات التقليدية على الجرائم المعلوماتية (السيبرانية).
- تحديث التشريعات.
- التقيد بالحياد التقني للتشريع.
- تحقيق التوازن في التشريع والتنسيق مع الآليات الأخرى.

إطار عام للسلامة السيبرانية في المنطقة العربية



2. التوجهات في تطبيق القانون والتنظيم:

- وضع سياسة خاصة بالسلامة المعلوماتية.
- إيجاد المحاكم المتخصصة وأجهزة التحقيق المتخصصة.
- استعمال الأدلة الرقمية في التحقيقات الجزائية.
- إنشاء مراكز الاستجابة السريعة لطوارئ الحاسوب.

3. التعاون بين الدول:

- تفعيل التعاون القضائي الرسمي وغير الرسمي.
- إيجاد حلول لتنازع الاختصاص القضائي.

4. التوجهات التقنية والإدارية والتنظيمية:

- اعتماد نموذج للأمن المعلوماتي (السيبراني).
- تفعيل التوجهات التقنية الخاصة بمقدمي الخدمات التقنية والشركات.
- تفعيل التوجهات المرتبطة بالعوامل الاجتماعية.

5. التوجهات المتعلقة بالتوعية والتدريب:

- توعية المستخدمين.
- توعية فئات خاصة في المجتمع.
- التدريب.