مكونات الذكاء الاقتصادي

سياسة الحماية إدارة مخاطر المعلومات

إن المقصود بمفهوم الحماية هي حماية التراث الفكري والمعلوماتي والدفاع عليه من جهة، ومن جهة أخرى الحرص على تأمين أنظمة المعلومات. ومن الجانب الأول فإن التحكم في التراث العلمي، التكنولوجي والتنافسي للمؤسسة وحمايته يكون إما عن طريق تحديد بشكل دقيق تراث المؤسسة المتواجد في المعلومات التي تملكها كبراءات الاختراع مثلا والتي تعد جزء من الترسانة الدفاعية للمؤسسة كما يحمي المعرفة التقنية، بالإضافة إلى أنماط العمل المعمول بها، أو خبرة الموظفين من جهة، أو عن طريق الحماية ضد التهديدات العرضية من جهة أخرى، كالأخطاء الناجمة عن عدم الانتباه أو نقص في المهارة أو الخبرة، والكوارث الطبيعية. ويتسع أمن المعلومات ليشمل الإجراءات والتدابير المستخدمة في المجالين الإداري والفني لحماية المصادر البيانية من التجاوزات والتدخلات غير المشروعة التي تقع عن طريق الصدفة أو عمدا عن طريق التسلل كالتجسس، سرقة البيانات والاحتيال.

لتحديد وحماية تراث المؤسسة تستخدم مناهج مختلفة، والأكثر شهرة يتمثل في المقاربة الأمنية، والتي تتمثل في تحديد ووضع تحت المراقبة العناصر العلمية، التكنولوجية والتنافسية للمؤسسة. كما لا تستند حماية موارد الشركة حصرا على النظم والإجراءات، إذ ينبغي أولا القيام بعمليات تثقيف، توعية وإشراك جميع العاملين في أنشطتهم اليومية.

ونلاحظ أن أحسن تقنية للحماية ضد تسرب المعلومات هو **توعية الموظفين**، إذ يجب على كل عامل في الشركة أن يكون على علم بالتحديات والاضطلاع بمسؤولياته، والمشاكل التي يمكن أن يواجهها، لذلك فإنه من المستحسن تقسيم وفهرسة المعلومات، من خلال وضع إجراءات لتداول الوثائق ومراقبة توزيعها وفقا لتصنيفاتها، وتقييد الوصول إليها إلا لمن لديه الحق بمعرفتها، والحد الأدنى للحماية هو فرض أو حظر تشفير البث الرقمي إذا كانت الرسالة حساسة جدا.

بالإضافة لذلك، يتواجد داخل الشركة أعضاء يمكن التلاعب بهم بسهولة للحصول للمعلومات، وفي هذه الحالة فإنه من المستحسن الكشف عن الأشخاص المحتمل جدا التعرض للتلاعبات التكتيكية الخبيثة(المحبطة، الهشة نفسيا ...)، وخاصة الأفراد الذين بإمكانهم الحصول على المعلومة الحساسة، والتحذير من خطر زعزعة الاستقرار الذي يمكن أن يقع على الموظفين، والتنبيه على الضغوطات، الابتزاز ومحاولات الفساد.

كما أنه في حالات التسلل والاختراق فإن بإمكان المؤسسة وضع تدابير وقائية كمراقبة مواقع الرصد(أنظمة الإنذار، بيوميتريات ...) وخلق مواقع للتخزين، بالإضافة إلى حماية نظام المعلومات(مفاتيح الدخول، أنظمة تشفيرية، مواقع مؤمنة...)، ومن أجل ذلك يمكن تشكيل يقظة أمنية وتكنولوجية تساهم في الحفاظ على المعلومات، واستعمال المعايير الأمنية ISO 13335:لإدارة أمن تكنولوجيا المعلومات والاتصالات، ISO 15408التقييم سلامة تكنولوجيا المعلومات والاتصالات، ISO 27001شهادة الجودة للممارسة، و ISO 27002مدونة قواعد السلوك لإدارة أمن المعلومات.

ومن الجانب الثاني تستخدم وظيفة الحماية في إدارة وتسيير مخاطر المعلومات، وبعبارة أخرى حماية المعلومات المحتفظ بها أو المصدرة من قبل المؤسسة، بما في ذلك المعتمد عليها من قبل المنافسين، وبالتالي فإن وظيفة إدارة مخاطر المعلومات تحافظ على تناسق وتماثل المعلومات لصالح الشركة التي تدير هذه المخاطر .

سياسة التأثير

بعض الخبراء يستعملون مفهوم الضغط والتأثير، ويمكن أن يصنف مفهوم التأثير على أساس أنه عملية كامنة وواردة تمارس على شخص أو شيء ما. إن أي استراتيجية تأثير تتطلب بناء هوية واضحة، وينعكس هذا من خلال فهم البيئة، ومعرفة الأشخاص الذين يتخذون القرارات ولديهم القدرة على التأثير.

إن وظيفة التأثير تسعى إلى تغيير وتعديل البيئة من خلال الضغوط المعلوماتية، حيث تعد "عمليات اللوبي (lobbying) "من عمليات التأثير الكلاسيكية الممارسة من طرف الشركات، ولكن يوجد هناك أنواع أخرى يمكن جمعها في فئتين: التنسيق والإحباط. حيث تقوم الشركات ببعث إشارات التنسيق عندما يريدون تجنب تصادم مع الشركات المنافسة (التجنب)، أو مع المؤسسات الشريكة (التي تكون معها على اتفاق). أما فيما يتعلق بإحباط أو تثبيط الشركات المنافسة يكون عن طريق تضليل نظام استعلامهم (نظام ذكائهم) من أجل أن توقعهم في الخطأ أو تشلهم، وتكمن عمليات التضليل في: الإعلان عن عمليات الاسترداد أي عمليات إعادة الشراء الوهمية، أو من خلال احتلال مكان الرائد على نطاق سوق غير معروف.

كما يمكن أن تستعمل المؤسسة الشبكات والاتصالات المستهدفة بغية الوصول إلى مرادها: تقوية صورتها في السوق، تعزيز مصالحها، جلب زبائن المؤسسات المنافسة وموردیهم وغيرها، والعمل حسب احتياجاتها. كما أن التأثير على حلفائها، إضعاف صورة المؤسسات الأخرى أو إرباك موظفيها تعد من العمليات(ضد المنافس) السرية في عملية الذكاء الاقتصادي. وغلبت على هذه العمليات أكثر فأكثر الجانب المعلوماتي، بحيث أن البعض أدخل مفهوم "معركة المعلومات" للتعبير عن هذا التطور، وفي هذا السياق يوجد ثلاث استراتيجيات ممكنة: الحرب من أجل المعلومات، الحرب ضد المعلومات، والحرب باستعمال المعلومات، وتسعى الأولى إلى التقاط أو تسريب المعلومات الاستراتيجية والسرية، أما الثانية فتهدف إلى حرمان المنافس من الوصول إلى المعلومات، والأخيرة تقع بوضوح في منظور من التضليل والتلاعب باستعمال المعلومة، إلا أن مفهوم الذكاء الاقتصادي لا ينحصر على هذه العمليات فقط .

من اليقظة إلى الذكاء الاقتصادي

إن المقاربة التسييرية لليقظة تستجيب إلى الحاجة إلى معرفة قدر أكبر من المعلومات الممكنة، وعدم خسارة أي شيء مما هو متاح. في حين أن المقاربة الاستراتيجية للذكاء الاقتصادي تستجيب وتلبي الحاجة إلى اتخاذ القرار، تستجيب إلى الحاجة إلى معرفة المعلومات اللازمة، وأن تعمل على أن تتقدم نحو

وضع أحسن. كما يتحدد الفرق ما بين المكلف بالذكاء الاقتصادي، في أنه المسؤول عن مصادر المعلومات الاقتصادية والتنافسية وتعزيز قيمتها لخدمة استراتيجية المؤسسة، أما المكلف باليقظة فهو المسؤول عن مختلف النشاطات المرتبطة بكل أنواع اليقظة. يأتي الذكاء الاقتصادي في الوقت الذي نجحنا فيه على استخراج المعلومات الصادرة من يقظة نشطة، معظم البيانات الهامة (ذات الصلة) التي سيتم استخدامها من قبل صناع القرار. حيث يتم وصف الذكاء الاقتصادي كتتويج لعملية طويلة يرجع أصلها إلى اليقظة المعلوماتية. ويبين الجدول تدرج من المعلومات واليقظة إلى حين الوصول إلى الذكاء الاقتصادي.

الوصول إلى الذكاء الاقتصادي

تحديد المعلومات **Documentation** ↓	– **استعمال المعلومات ذات المصادر الرسمية بشكل جيد.** – **المعرفة التامة والكاملة للمصادر** – **مراقبة وتدقيق المعلومات بشكل مستمر.**
اليقظة المتخصصة **(التكنولوجية، القانونية، التجارية، والتنافسية..)** **Veille spécialisée** ↓	– استغلال المعلومات ذو المصادر الغير الرسمية. – البحث عن مفهوم المعلومات المتحصل عليها وتحليلها جيدا لتحديد إشارات الضعف.
اليقظة الشاملة **(استراتيجية أو تكتيكية)** **Veille globale** ↓	– إتباع نهج أكثر شمولية: جمع مختلف اليقظة والاندماج في مستوى الاستراتيجية.
الذكاء الاقتصادي	– يتضمن عملية حماية تراث المؤسسة. – يتضمن عمليات الضغط والتأثير. – يفترض ثقافة جماعية للمعلومات. – يدمج مجموعة واسعة من المعنيين في المؤسسة.