المحور 6: رأس المال الفكري في بيئة الأعمال الإلكترونية العربية

تنمية الموارد البشرية ودورها في تحقيق أمنية تكنولوجيا المعلومات المصرفية-رؤية مستقبلية-

من إعداد:

د/ بروش زين الدين: أستاذ محاضر" أ"، كلية العلوم الاقتصادية العلوم التجارية، وعلوم التسيير، جامعة فرحات عباس_سطيف_

البريد الالكتروني: zinberrouche@hotmail.com

أ/ محمد شايب: أستاذ مساعد "أ "، كلية العلوم الاقتصادية العلوم التجارية، وعلوم التسيير، جامعة فرحات عباس_سطيف_

البريد الالكتروني: MohammedChaib19@yahoo.fr

الملخص: ستواجه البنوك والمؤسسات المالية الجزائرية مخاطر جمة في سعيها لتبني النمط المالي والمصرفي الإلكتروني عند تقديمها لخدماتها للعملاء، وتحسبا منها للمخاطر والعوائق وللجرائم الإلكترونية المحتملة، وجب عليها تنمية مواردها البشرية وتدريبها بعناية وتدرّج، ووفق أخر ما توصلت إليه الاستراتيجيات والنظريات والتطبيقات العالمية للمعلوماتية بخصوص الحماية والوقاية من مختلف الأخطار الداخلية والخارجية الهادفة لحماية البيانات ذات الطابع الشخصي وكذا تأمين المعاملات الإلكترونية المصرفية والمحافظة على نظامها المعلوماتي.

Abstract: *The Algerian Banks and financial institutions will face serious risks as a result of the adoption of an electronic financial and banking system in the near future to offer its services to customers. TO meet the future challenges and risks such as the electronic crimes, it shall develop its human resources staff by training them carefully and gradually according to the latest theories and practices about the information safety and security and its prevention from the various internal and external threats. This protection shall make safe the personal data and secure the electronic banking transactions in order to maintain the stability of its information system .*

المقدمة:

يمكن للقطاع المصرفي أن يحقق نوعان من الثروة: الثروة المالية والمادية، أي رأس المال المادي، والثروة الفنية، أي رأس المال البشري[1]، وهذه الأخيرة تأتي من خلال المعرفة والتدريب للموظفين وللعملاء، فالبنوك تقاس بحجم ما لديها من خبراء وموظفين وإداريين وعملاء قادرين على تطوير النشاط المصرفي وانجاز الأعمال المالية التي تناط بهم بكل دقة ومهارة وإتقان.

يؤكد الخبراء اليوم على أهمية تأهيل الموارد البشرية البنكية لتتمكن من مكافحة الفساد المالي بمختلف أشكاله وذلك بتهيئة البيئة المصرفية لتنفيذ الإلتزامات والمعايير الدولية في مجال مكافحة الفساد المالي وبما يتماشى مع الإتفاقيات الدولية. فالتطورات التكنولوجية المتسارعة التي تشهدها الصناعة المصرفية أدت إلى بروز العديد من المخاطر التي وضعت كل من إدارة البنوك والجهات الرقابية أمام تحديات كبيرة للتعامل مع هذه المخاطر. ويتواصل الاهتمام بقضايا الجريمة في مجال الكمبيوتر والإنترنت والهاتف المحمول... ومختلف أنواع الجريمة الإلكترونية [2] في جميع النواحي الإقتصادية وخصوصا القطاع المصرفي والمالي.

مشكلة الدراسة: أمن المعلومات في البنك هو العلم الذي يعمل على توفير الحماية للمعلومات المصرفية من المخاطر التي تهددها أو الاعتداء عليها، وذلك من خلال الأدوات والوسائل اللازمة توفيرها لحماية المعلومات المالية المصرفية من المخاطر الداخلية والخارجية. أما تأهيل العنصر البشري في تكنولوجيا أمنية المعلومات المصرفية فيقصد به تنمية إمكانيات العنصر البشري، وما الذي ينبغي معرفته سواء بالنسبة للموظف أو الإداري وحتى العميل البنكي بخصوص هذه التقنيات، والمتعلقة بالحماية لأمنية تكنولوجيا الإعلام والاتصال المتبناة في البنوك.

---

[1] يقول **بيتر فرديناند دراكر *Peter Ferdinand Drucker*** وهو من مؤسسي علم الإدارة الحديثة: **"مازلنا حتى الأن في الشركات نضع الأهمية للنظام المؤسسي والخطط ونترك العنصر البشري"**، يعتبر دراكر من منظري الإدارة الأمريكان، من مواليد 19 نوفمبر 1909 بفينا بالنمسا وتوفي في كلارمون في كاليفورنيا بالولايات المتحدة الأمريكية في 11 نوفمبر 2005. لمزيد من المعلومات، أنظر لموسوعة الويكيبيديا الحرة:

http://fr.wikipedia.org/wiki/Peter_Drucker

[2] خصوص الجوانب التي تشملها الجريمة الإلكترونية فهي تشمل كل الجرائم والمخالفات التي تتم في الوضع العادي التقليدي ويمكن الشروع فيها وارتكابها من خلال الوسائط الإلكترونية،

مع تزايد حجم جرائم الإنترنت ومخاطر التكنولوجيا في البنوك[3]، تجد هذه الأخيرة نفسها أمام اشكالية تنمية مواردها البشرية، وموظفي تقنية وأمن المعلومات بشكل خاص على وسائل وأساليب وسياسات إدارة أمن المعلومات، إضافة إلى البرامج والتطبيقات المستخدمة في هذا المجال لإيجاد كفاءات مؤهلة تمتلك الوعي الأمني لضمان استمرارية الأعمال المصرفية، وتقليل المخاطر في استخدامات التقنية المعلوماتية.

أهداف البحث: يهدف هذا البحث إلى تحقيق مجموعة من الأهداف من أهمها ما يلي:

_التأكيد على أن حماية أمن المعلومات المصرفية هي حاجة ماسة وضرورية، لأن الحماية ليست فقط للبنوك وعملائها وإنما حماية للأمن الوطني والسياسي والاقتصادي والإجتماعي على الصعيد الوطني.

_التنويه بأهمية الموضوع فيما يخص عصرنة وتحديث النظام المصرفي الجزائري في ظل التحديات التي يواجها عند الانفتاح على الاقتصاد العالمي وما يترتب عن التحرير المالي.

_بيان الطبيعة المميزة لتنمية الموارد البشرية البنكية من تدريب وتعليم وتربية.

_تسليط الضوء على أهمية التنمية للموارد البشرية في أمنية تكنولوجيا المعلومات المصرفية.

_دور منظمات أمن المعلومات في تأهيل الكوادر البشرية البنكية في أمنية تكنولوجيا المعلومات المالية.

_موقع العنصر البشري البنكي في إطار الوقاية والحماية للمعلومات المالية المصرفية.

_تقديم التوصيات التي يمكن أن تساهم في تنمية البنوك الجزائرية لعنصرها البشري فيما يخص أمنية تكنولوجيات الإعلام والاتصال الحديثة.

المحور الأول: أهمية الإستثمار في رأس المال البشري في ظل اقتصاد المعرفة

إن أهم مظهر لاقتصاد المعرفة نظرية رأس المال البشري، التي تقوم على فرضية أساسية مفادها وجود اختلاف بين الأفراد فيم يتعلق بمقدار الإستثمار في مهاراتهم وخبراتهم وقدراتهم، بناء على ذلك فإن الفرد يعتبر أصلا من أصول المنظمة، إذ يمكن تحديد قيمته وتسييره كما تسير محفظة الموارد المالية[4].

---

[3] On parle en 2005, par exemple, de **42 milliards de dollars** de perte due à des vers voire des virus manipulés par la communauté des fameux « **hackers** ». Sécurité informatique dans le secteur bancaire: Une condition sine qua non, ***http://www.espacemanager.com/finance/securite-informatique-dans-le-secteur-bancaire-une-condition-sine-qua-non.html***

[4] حسين يرقى، **استراتيجية تنمية الموارد البشرية في المؤسسة الإقتصادية_حالة مؤسسة سوناطراك_**، مذكرة مقدمة كجزء من متطلبات الحصول على شهادة دكتوراه دولة في العلوم الإقتصادية، تخصص تسيير، جامعة الجزائر، الجزائر، 2007_2008. ص.167.

لذا يعتبر الاستثمار في رأس المال البشري خاصة في مجال تدريب الأفراد من الأمور الهامة لنجاح كل بنك وأيضا لتحقيق التنمية الإقتصادية.

أولا/ أهمية تنمية رأس البشري في ظل تكنولوجيات الإعلام والاتصال الحديثة:

إن من الأدق والأنفع أن نفكر في الأفراد من منظور جديد ليس بإعتبارهم أصولا ولكن كمستثمرين[5]، فلقد خلق النمو الهائل المتسارع في قطاع الخدمات القائمة على تكنولوجيا الإعلام والإتصال عبر بلدان العالم المتقدمة حاجة إلى الموظفين المؤهلين بمهارات هذه التكنولوجيا. وهنالك أيضاً طلب على زيادة قدرة هؤلاء المهنيين لتلبية المزيد المتزايد من الخدمات على الخط[6]. أو ما يسمى بالخدمات الإلكترونية اوالأفتراضية.

ثانيا/ اقتصاد المعرفة وأهمية تكوين المختصين في المعلومات المصرفية

إن الأصول التقليدية_رأس المال المادي_ لم ولن تختفي ولكن في ضوء ما بلغته المعرفة من أهمية كونها تضيف قيمة للعمل المصرفي فمن المحتم أن تصبح المعرفة أصلا متزايد الأهمية بالنسبة للمنظمات خاصة البنوك إن لم تكن أهم أصولها على الإطلاق[7] وهذا يتطلب دورا جديدا ورؤيا مستقبلية لهم في عصر إدارة المعرفة واقتصاد المعرفة.

ومن خلال هذه الأدوار يمكن استنتاج المهارات الأساسية التي لها علاقة بإدارة المعرفة ولابد إن يمتلكها المختصين في المعلومات في عصر مجتمع المعلومات، وهي[8]: التعليم التنظيمي، إدارة الوثائق والتكنولوجيا. حيث على المختصين في المعلومات المصرفية أن يكونوا قادرين على امتلاك القدرة على التعلم الذاتى، والتنمية الذاتية، والتحكم الذاتي. وهو ما يتطلب إعادة النظر للبنك كمؤسسة مقرضة إلى الرغبة في تصميم بيئة عمل مريحة تناسب عمليات تبادل المعلومات واقتسامها بين الموظفين فيها، وبعبارة أخرى، ينبغي على كل مختص في المعلومات المصرفية أن يشارك الآخرين فيتعلم المعارف الشائعة وتنظيمها، ومن ثم تتاح له القدرة على التطوير المستمر استجابة لمتطلبات التحول نحو التعامل مع البيئة الرقمية والإلكترونية.

المحور الثاني: تنمية الموارد البشرية البنكية:

على الرغم من قدم ممارسات تنمية الموارد البشرية، إلا أن اهتمام المُنظِّرين الإقتصاديين والإداريين بدأ يتجه إليه كحقلٍ علمي في سنة 1958 ؛ حيث أصبح مصطلح تنمية الموارد البشرية ***Human Resource Development)*** أكثر تداولا في كتاباتم. ويشير أدب التسيير والإدارة إلى أن مفهوم تنمية الموارد البشرية بمضمونه المعاصر لم ينطلق ويصبح مصطلحًا واسع الإنتشار إلا مع الكاتب والمفكر الأمريكي ليونارد نادلر

---

[5] توماس أ. ستيوارت، **ثورة المعرفة_رأس المال الفكري_ ومؤسسة القرن الحادي والعشرين**، ترجمة علاء أحمد صلاح، الدار الدولية للإستثمارات الثقافية، القاهرة، مصر، 2004، ص. 393

[6] كمبا هارول إسلام، **تنمية رأس المال البشري لمبادرات تقديم الخدمات على الخط في أقل البلدان نمواً**_ تحديات وفرص_، ***http://www.ituglobalsymposium2008.info/Doc.26-Baharl%20Islam-India-A.W11.doc***

[7] توماس أ. ستيوارت، مرجع سابق، ص,31. بتصرف.

[8] المرجع السابق.

Leonard Nadler[9] بعد عشر سنواتٍ من التاريخ السابق[10]. البنوك وكغيرها من المنظمات تحاول بين الحين والأخر تنمية مواردها البشرية في ظل التغيرات التكنولوجية السريعة.

أولا/ مفهوم تنمية الموارد البشرية البنكية

إن تنمية الموارد البشرية هي تلك الجهود المخطَّطة والمنظمة المستمرة الهادفة إلى تحسين قدرات العنصر البشري في البنك، أي معارفهم ومهاراتهم واتجاهاتهم في سبيل تحسين سلوكهم وأدائهم الوظيفي، في وظائفهم الحالية وإعدادهم لوظائف أو مهام مستقبلية، أو تمكينهم من مواكبة نمو المؤسسة وتطورها، وذلك من خلال ثلاث وظائف رئيسية، هي التدريب والتعليم والتطوير.

ثانيا/ طبيعة وأبعاد تنمية الموارد البشرية في أمنية المعلومات المالية والمصرفية:

يمثل المثلث التالي ثالوث تنمية الموارد البشرية وهو: التربية، التعليم والتدريب[11]: فالتنمية عملية تحسين وانماء لقدرات العنصر البشري ووجهات نظرهم وصفاتهم الشخصية، بينما عملية التعليم تركز على اكساب معلومات عامة وواسعة وتركز عملية التدريب على اكساب مهارات وأساليب فنية وادارية محددة[12].

نركز بدرجة أقل على عملية التدريب أو التكوين في البنك على أمنية المعلومات المصرفية، هذه العملية تتطلب توفر حضور المكونين يشرف عليهم عدد من المكونين وضرورة توفر مجموعة من الوسائل المادية.

1/ماهية التدريب وأهميته: يتيح التدريب في أنه يتيح للموظف التأقلم مع التغيرات التي تحدث على مستوى العمل، نظرا لحالة التطور التي تمس أسلوب العمل) التقنيات والآلات (والتي تؤدي بدورها إلى تغيير طبيعة العمليات الإنتاجية، فضلا عن أن التدريب هو في حد ذاته صقل للمهارات والخبرات والمعلومات والمعارف[13]؛

إذن، التدريب في البنك هو عملية صقل وتنمية مهارات الموظفين في سياق معرفي ومنهجي علمي، أو في سياق منهجي وتطبيقي.

---

[9] يعتبر البروفيسور **ليونارد نادلو** كما يطلق عليه في الغرب، المهندس المعماري لفرع تنمية الموارد البشرية ***Architect of* HRD** ، إذ أنه من أوائل من حدد معالم هذا الحقل.

[10] حسين يرقى، مرجع سابق، ص. 89.

[11] هناك من يطلق على الثالوث: **التدريب**، **التعليم**، **التطوير** بالوظائف أساسية لتنمية الموارد البشرية.

[12] عبد المعطي محمد عساف، **التدريب وتنمية الموارد البشرية**،_ **الأسس والعمليات**_ دار زهران للنشر والتوزيع، عمان، الأردن، 2008، ص. 32.

[13] الداودي الشيخ، **تحليل أثر التدريب والتحفيز على تنمية الموارد البشرية في البلدان الإسلامية**، مجلة الباحث، مجلة دورية أكادمية متخصصة محكمة تعنى بالبحوث الإقتصادية، جامعة ورقلة، العدد 6، 2008، ص. 12.

وتظهر أهمية التدريب[14] للموظفين في البنك في الأسباب التالية[15]:

_أن الأفراد فور التحاقهم بالعمل يحتاجون إلى جرعات تدريبية من نوع خاص للقيام بأعباء الوظائف التي سيشغلونها للمرة الأولى.

_إن التطور التكنولوجي وما يترتب عليه من إدخال تكنولوجيا جديدة مستحدثة للإنتاج قد يتطلب إلغاء بعض الوظائف الحالية و إنشاء وظائف جديدة تتناسب مع التكنولوجيا الجديدة.

_إن إنشاء صناعات جديدة لم تكن موجودة من قبل قد يتطلب توفر مهارات معينة لا يمكن الحصول عليها عن طريق استخدام الأفراد الحاليين حتى ولو كانوا من الأفراد المهرة إلا إذا أعطوا تدريبا خاصا على تلك الأعمال الفنية الجديدة وطبيعي أن نوع التدريب ومدته يتوقفان على درجة المهارة المطلوبة في تلك الأعمال وعلى استعداد الأفراد الذين يتقرر تدريبهم لشغلها.

لذلك فإن نشاط التدريب يلقى اهتماما كبيرا في البنوك الحديثة نتيجة إدراك أهمية الدور الذي يعلبه التدريب في تحقيق الأهداف الإستراتيجية للبنك[16].

وتنقسم أساليب التدريب إلى ثلاثة أنواع: أساليب العرض: المحاضرة، التطبيق العلمي/ الإيضاحي. أساليب المشاركة: المناقشات، دراسة الحالة، لعب الأدوار، العصف الذهني، مجموعات المناقشة، الألعاب والقصة غير الكاملة. الأنشطة خارج قاعة التدريب: التكليفات، المشروعات، الزيارات الميدانية/ الرحلات.

---

[14] تتكون خطوات التدريب من أربع مراحل منطقية ومتتابعة:- **تحديد الإحتياجات التدريبية** في تحديد نوعية ومستوى البرامج التدريبية المطلوبة للموظفين، سواء كانت هذه البرامج تأهيلية للموظفين الجدد، أو تطويرية للمستمرين في أعمالهم ووظائفهم، -**تصميم البرامج التدريبية *Training Programs Design*** بحيث تحدد أهداف هذه البرامج من المعارف والمهارات والقيم المطلوب تحقيقها، وكذلك الأساليب التدريبية والتقويمية لهذه البرامج،- **تنفيذ برنامج التدريب**،- **تقييم البرامج التدريبية**، حيث بعد الإنتهاء من البرنامج لابد من تقييمه، أنظر:

_ بسمة أحمد ابراهيم أبو زيد، **واقع إدارة تنمية الموارد البشرية في المصارف العاملة في فلسطين وسبل تطويره**، رساله مقدمة استكمالا لمتطلبات الحصول على درجة الماجستير في إدارة الأعمال، غزة، فلسطين، 2008، ص. 31.

_محمد حسين سيد، **أهمية العنصر البشرى في تحقيق أهداف الشركات**، بحث مقدم إلى الأكاديمية العربية البريطانية للحصول على درجة الدكتوراه في إدارة الموارد البشرية تحت إشراف فريق التعليم عن بعد، دون سنة نشر، ص. 178. ***www.abahe.co.uk***

[15] منير نوري، **تسيير الموارد البشرية**، ديوان المطبوعات الجامعية، الجزائر، 2010، ص. 238-239. بتصرف.

[16] عادل محمد زايد، **ادارة الموارد البشرية_ رؤية استراتيجية_** كلية التجارة، جامعة القاهرة، 2003، ص. 284.

_**أنواع التدريب في أمنية المعلومات المصرفية**: هنا يمكن أن نطرح السؤال التالي: ماهي محددات اختيار البنك للتدريب داخل البنك(صنع مهارات) أو التدريب خارج البنك(شراء مهارات من سوق العمل) من أجل وقاية وحماية المعلومات المصرفية؟[17].

1. **التدريب الداخي**: يعرف على أنه الأنشطة التعليمية والمقدمة مسبقا من قبل ادارة الأفراد داخل البنك والتي تجذب فقط الافراد الذين يعملون بالبنك.

2. **التدريب الخارجي**: يعرف على أنه الأنشطة التدريبية التي يعدها وينظمها أفراد خارج البنك بخصوص كيفية تامين وحماية المعلومات المصرفية، مثلا: استشاريين، جهات متخصصة، منظمات أمن المعلومات...[18]

إن البرامج التدريبية والتي تخص أمنية المعلومات المالية والمصرفية تزيد من قدرات التحليلية للموظف وصقل مهاراتهم في العمل الجماعي عن طريق دراسة الحالات الواقعية والإنسجام مع المدربين الذين هم على مستوى عال من الإحتراف. كما يتم تصميم وتنفيذ العديد من البرامج المغلقة للبنوك والتي يتم تصميمها وفق احتياجات البنك، ويشارك في تقديم تلك البرامج بعض الموظفين بالبنك[19].

_**البرامج تدريبية والشهادات المعتمدة في أمن المعلومات**: تقدم على سبيل المثال: منظمة أمن المعلومات المذكورة سابقا برامج تدريبية وشهادات معتمدجة في أمن المعلومات منها[20]:

---

[17] راوية حسن، **مدخل استراتيجي لتخطيط وتنمية الموارد البشرية**، الدار الجامعية، الاسكندرية، مصر، 2002)، ص,285، بتصرف.

[18] مثلل: منظمة أمن المعلومات ***Information Systems Security Association*** أو ***ISSA*** وهي منظمة دولية غير هادفة للربح ومقرها الولايات المتحدة الأمريكية، كما أن المنظمة تعتبر أحد الأركان الرئيسية الراعية لشهادة خبير أمن المعلومات ***CISSP*** بالتعاون مع وزارة الدفاع الأمريكية وجامعة كارنيجي وقد تم تأسيس المنظمة عام 1984 بالولايات المتحدة الأمريكية ثم تأسيس العديد من الفروع حول العالم. **وتضم المنظمة أكثر من 13000 عضو محترفا في أمن المعلومات وأكثر من 140 فرعا حول العالم** . ***https://www.issa.org/***

[19] محمد البلتاجي، **دور المعاهد المصرفية في تأهيل العاملين في المؤسسات المالية الإسلامية**، المؤتمر الخامس للهيئات الشرعية للمؤسسات المالية الإسلامية، هيئة الحاسبة والمراجعة، البحرين، يومي 19 و20 نوفمبر 2005. ص. 20.

[20] منظمة أمن المعلومات، ***http://www.issa-eg.org/index.php?option=com_content&view=category&id=43&Itemid=54***

- Ø ***Certified Information Security Practitioner***: شهادة ممارس أمن المعلومات أو *CISP* هي المستوى الأول من شهادات ودبلومات أمن المعلومات المتخصصة التي تقدمها منظمة أمن المعلومات بالتعاون مع أكاديمية *ASKPC* ببريطانيا وأيضا معهد مهندسي الإليكترونيات بالولايات المتحدة *IEEE* وهو المدخل الرئيسي لعلم أمن المعلومات، البرنامج التدريبي عبارة عن ملفات توضيحية مصورة وفيديو مفصل وكتيبات متخصصة.
- Ø ***Certified Information Security Expert*** : دبلوم خبير أمن نظم المعلومات هو برنامج تدريبي وشهادة متقدمة في أمن نظم المعلومات تقدمها منظمة أمن المعلومات بالتعاون مع أكاديمية *ASKPC* ببريطانيا ومعهد مهندسي الإليكترونيات *IEEE* بالولايات المتحدة الأمريكية الدبلوم يشمل المادة العلمية لشهادة خبير أمن الشبكات *Network Security Professional* وأمن المواقع *Web Security Professional* وهذا البرنامج والشهادات معتمدة من معهد مهندسي الإليكترونيات والكهرباء *IEEE* بالولايات المتحدة الأمريكية ومنظمة أمن المعلومات ISSA.
- Ø ***Certified Cyber Crime Investigator***: محقق الجرائم الإلكترونية أو *Cybercrime Investigator* هو تخصص جديد ومتقدم تقدمه منظمة أمن المعلومات *ISSA* بالتعاون مع أكاديمية *ASKPC* ببريطانيا ومعهد مهندسي الإليكترونيات والكهرباء *IEEE* بالولايات المتحدة الأمريكية.
- Ø ***Information Systems Security Professional***: إن منظمة أمن المعلومات *ISSA* من أحد المؤسسين والرعاة لشهادة *CISSP* العالمية، لهذا فهي تقدم تدريب خاص لهذه الشهادة وأيضا شهادة اتمام للبرنامج من *ISSA* بعدد ساعات معتمدة .*CPE* إلا أنه للحصول على شهادة *CISSP* العالمية لابد من التسجيل في اختبار الشهادة عبر منظمة *ISC2* فهي الجهة التي تتولي الإختبارات واصدار شهادات *CISSP* .

2_**ماهية التعلم**: هو العملية التي ينتج عنها ازدياد القدرة على الأداء ومع ذلك ينبغي تهيئة البيئة التي يكون فيها الأفراد مستعدين وقادرين على استخدام هذه القدرة الأكبر[21].

فالإداري أو المعلم في البنك، وفيما يخص أمنية المعلومات المصرفية ليس الهدف تحويله الى أخصائي في تنمية الموارد البشرية وإنما عليه تعريف الموظفين بأن لديهم طرقا كثيرة لمساعدتهم على التعلم في سياق وظيفتهم الأمنية بخصوص المعلومات المصرفية ومسؤولياتهم القائمة.

[21] جنيفر جوي ماثيور، **تنمية الموارد البشرية**، ترجمة علا أحمد صلاح، (مجموعة النيل العربية، القاهرة، مصر، 2008)، ص.387.

ويدرك جيدا المكون أو المدرب أو المتدخل أنه لابد من توفر رغبة خاصة لدى الموظفين في استعاب محتوى برامج أمنية المعلومات المصرفية أو ما يقصد به دافع التعلم، هذا الأخير يتأثر بالمتغيرات الشخصية والموقفية، فهو يتحدد بالعلاقة بين التعلم للبرامج كمحتوى والنتائج التي يمكن أن يؤدي اليها.

3_ماهية التربية: ينبغي على العنصر البشري في البنك أن يلتزم بمعايير وقواعد وآداب المهنة في آداء جميع الأعمال بمهنية كاملة وبشكل أخلاقي والحفاظ على أعلى المعايير في المحافظة على سرية وحماية المعلومات الشخصية والحساسة، كما لابد من تحري الدقة والصدق في التعامل داخل البنك ويلتزم أيضا بأن لا يقوم بأية أعمال تنافي أخلاقيات المهنة المصرفية أو قد تشكل تضاربا للمصالح أو تضر بسمعة البنك أو مهنة أمن المعلومات، كما لابد من الإلتزام بالمحافظة على خصوصية الآخرين وعدم التعرض لسمعة الآخرين أو أي عميل للبنك.

تعد الجوانب الأخلاقية من أهم المجالات التي يجب غرسها في العاملين بالبنوك وذلك عن طريق الإهتمام بالبرامج التدريبية التي تحث العاملين على الإهتمام بحسن المعاملة وإتقان العمل والالتزام بتعاليم الإسلام[22]. لأن الخطر المعلوماتي يمكن أن يتسبب به الموظف عن قصد كما سنرى في المحاور الآتية.

يمكن القول في نهاية هذا المحور أن المكون (المتدخل) والمتكون (المشارك) في البنك يمثل البعد البشري لعملية التكوين بحيث تتم هذه العملية بفضلهم ومن أجلهم[23] من أجل تنمية للموراد البشرية البنكية في اطار بعد تدريبي، تعليمي وأخلاقي، لتبقى الأهية القصوى للبعد الاخير لأن الأبحاث تشير إلى أن اكبر الأخطار التي تهدد منظومة أمن المعلومات قد تأتي من داخل المنظومة وليس من خارجها.

المحور الثالث: تكوين العنصر البشري في ماهية تكنولوجيا أمنية المعلومات المصرفية:

أي خلل أمني أو جريمة إلكترونية[24] مهما كانت درجتها ستؤثر سلباً على العلاقة بين البنك وعملائه. لهذا يعمل المكون على أن تكون المهارات الأمنية جزءا من العمليات التشغيلية والتقنية، ووفق أساليب تدريب المختلفة، والتي يقصد بها الطريقة (الكيفية) التي يتم من خلالها عرض المادة التدريبية التي تخص كيفية التعامل مع التكنولوجيا المصرفية بأمنية كبيرة، وتقديم تدريب متخصص في مجال التوعية الأمنية ومبادئ أمن المعلومات المصرفية للموظفين.

---

[22] محمد البلتاجي، مرجع سابق، ص. 13.

[23] عبد الكريم بوحفص، **التكوين الاستراتيجي لتنمية الموارد البشرية**، (ديوان المطبوعات الجامعية، الجزائر، 2010)، ص. 192

[24] تجدر الإشارة أن اتفاقية بودابيست (2001) لمكافحة **الجريمة الإلكترونية**، تعتبر الأداة الدولية الوحيدة الملزمة بشأن الجرائم الإلكترونية. وتعد هذه الإتفاقية المصادق عليها من قبل48 دولة، بمثابة الخطوط التوجيهية لكل البلدان، والتي تقر تشريعا شاملا للجريمة المعلوماتية. كما أنها توفر إطارا للتعاون الدولي ضد جرائم الإنترنت.

أولا/ مفهوم أمن المعلومات المصرفية والمالية: يمكن تفسير مصطلح أمن المعلومات[25] من ثلاثة زوايا[26]:

1 _ **من زاوية أكاديمية:** هو العلم الذي يبحث في نظريات وإستراتيجيات توفير الحماية للمعلومات من المخاطر التي تهددها ومن أنشطة الإعتداء عليها.

2 _ **من زاوية تقنية:** هو الوسائل والأدوات والإجراءات اللازم توفيرها لضمان حماية المعلومات المصرفية من الأخطار الداخلية والخارجية.

3 _ **من زاوية قانونية:** أمن المعلومات المصرفية هو هدف وغرض تشريعات حماية المعلومات من الأنشطة غير المشروعة وغير القانونية التي تستهدف المعلومات ونظمها(جرائم الكمبيوتر والإنترنت).

ثانيا/ أهداف أمنية المعلومات: إن أغراض أبحاث وإستراتيجيات ووسائل أمن المعلومات – سواء من الناحية التقنية أو الأدائية - وكذا هدف التدابير التشريعية في هذا الحقل، ضمان توفر العناصر التالية لأية معلومات يراد توفير الحماية الكافية لها[27]:

1. **السرية أو الموثوقية *CONFIDENTIALITY***: وتعني التأكد من أن المعلومات لا تكشف ولا يطلع عليها من قبل أشخاص غير مخولين بذلك.
2. **التكاملية وسلامة المحتوى *INTEGRITY***: التأكد من أن محتوى المعلومات صحيح ولم يتم تعديله أوالعبث به، وبشكل خاص لن يتم تدمير المحتوى أو تغيره أو العبث به في أية مرحلة من مراحل المعالجة أو التبادل سواء في مرحلة التعامل الداخلي مع المعلومات أو عن طريق تدخل غير مشروع.

---

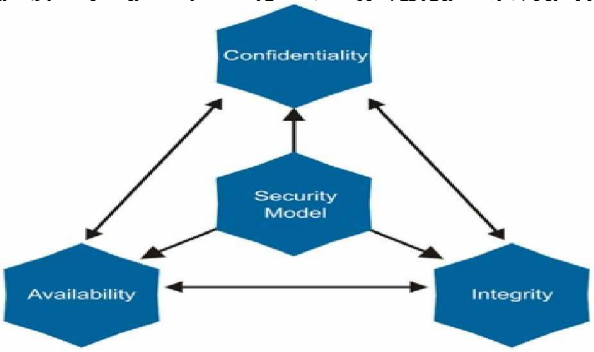
[25] إن استخدام اصطلاح **أمن المعلومات *Information Security*** وإن كان استخداما قديما سابقا لولادة وسائل تكنولوجيا المعلومات، إلا أنه وجد استخدامه الشائع بل والفعلي، في نطاق أنشطة معالجة ونقل البيانات بواسطة وسائل الحوسبة والإتصال. وله مواقع متخصصة على شبكة الإنترنت نذكر منها: ***http://www.itsecurity.be***

[26] عائض المري، **أمن المعلومات، ماهيتها هناصرها واستراتيجيتها**، معلومات قانونية، الدراسات والإستشارات القانونية، 6 نوفمبر 2011.أنظر الموقع الإلكتروني التالي: ***http://www.dralmarri.com/show.asp?field=res_a&id=205***

[27] المرجع السابق.

3. **توفر المعلومات أو الخدمة** ***AVAILABILITY*** : التأكد من استمرار عمل النظام المعلوماتي واستمرار القدرة على التفاعل مع المعلومات وتقديم الخدمة لمواقع المعلوماتية، وأن مستخدم المعلومات لن يتعرض إلى منع استخدامه لها أو دخوله اليها [28].

الشكل رقم (1): [illegible] المصرفية



المصدر: من إعداد الباحث

وهناك من يضيف من الكتاب في مجال الإلكترونية[29].

4. **إثبات التصرفات للقائمين بها** ***NON-REPUDIATION***: ويقصد به ضمان عدم انكار الشخص الذي قام بتصرف ما متصل بالمعلومات أو مواقعها إنكار أنه هو الذي قام بهذا التصرف، بحيث تتوفر قدرة إثبات أن تصرفا ما قد تم من شخص ما في وقت معين.

ثالثا/ أهم المخاطر والإعتداءات في بيئة المعلومات المصرفية:

تطال المخاطر والإعتداءات في بيئة المعلومات المصرفية أربعة مواطن أساسية هي مكونات تقنية المعلومات في أحدث تجلياتها:

1_**الأجهزة**: وهي كافة المعدات والأدوات المادية التي تتكون منها النظم، كالشاشات والطابعات ومكوناتها الداخلية ووسائط التخزين المادية وغيرها.

2_**البرامج**: وهي الأوامر المرتبة في نسق معين لإنجاز الأعمال، وهي إما مستقلة عن النظام أو مخزنة فيه

3_**المعطيات أو البيانات**: وتشمل كافة البيانات[30] المدخلة والمعلومات المستخرجة عقب معالجتها، وتمتد بمعناها الواسع للبرمجيات المخزنة داخل النظم. والمعطيات قد تكون في طور الإدخال أو الإخراج أو التخزين أو التبادل بين النظم عبر الشبكات، وقد تخزن داخل النظم أو على وسائط التخزين خارجه.

---

[28] إذا عملت المصارف في حقل البنوك الإلكترونية أو الخدمات المصرفية الإلكترونية عن بعد، كان عنصر عدم الإنكار بنفس أهمية بقية العناصر. ونجد ان **مواقع الإنترنت** مثلا تتطلب ايلاء عنصر الاستمرارية الاهتمام الأكبر، في حين أن **مواقع التجارة الإلكترونية** من بين مواقع الإنترنت تتطلب الحرص على توفير عناصر الحماية الأربعة بنفس القدر والأهمية.

[29] ***On Peut Résumer en 4 Lettres « DICA » (Disponibilité, Intégrité, Confidentialité et Auditabilité).***

4_**الإتصالات:** وتشمل شبكات الإتصال[31] التي تربط أجهزة التقنية بعضها بعض محليا ونطاقيا ودوليا، وتتيح فرصة اختراق النظم عبرها كما أنها بذاتها محل للإعتداء وموطن من مواطن الخطر الحقيقي.

المحور الرابع: منطلقات واستراتيجيات تأهيل العنصر البشري في أمنية تكنولوجيا المعلومات المصرفية:

على إدارة أمنية المعلومات وضع خطة طارئة للمحافظة على أمن المعلومات المصرفية وإجراء تجارب وتمرينات(تدريبات) عملية ضمانا لنجاح الخطة عند تعرض المعلومات المصرفية إلى الأخطار والتهديدات المحتملة وإحباط محاولات التجسس والإحتيال.

أولا/ منطلقات خطة حماية المعلومات: إن ضمان عناصر أمن المعلومات كلها أو بعضها يعتمد على المعلومات محل الحماية واستخداماتها وعلى الخدمات المتصلة بها، فليس كل المعلومات المصرفية تتطلب السرية وضمان عدم الإفشاء، وليس كل المعلومات في البنك واحدة بذات الأهمية من حيث الوصول لها أو ضمان عدم العبث بها، لهذا تنطلق خطط أمن المعلومات المصرفية من الإجابة عن سلسلة تساؤلات متتالية:

التساؤل الأول: ما الذي نريد أن نحميه؟ وإجابة هذا التساؤل تحدد تصنيف البيانات والمعلومات من حيث أهمية الحماية، إذ تصنف المعلومات تبعا لكل حالة على حدة، من معلومات لا تتطلب الحماية، الى معلومات تتطلب حماية قصوى.

التساؤل الثاني: ماهي مواطن الحماية؟

_**أمن الاتصالات:** ويراد بأمن الإتصالات حماية المعلومات خلال عملية تبادل البيانات من نظام إلى أخر.

_**أمن الكمبيوتر:** ويراد به حماية المعلومات داخل النظام بكافة أنواعها وانماطها كحماية نظام التشغيل وحماية برامج التطبيقات وحماية برامج إدارة البيانات وحماية قواعد البيانات بأنواعها المختلفة.

ولا يتحقق أمن المعلومات دون توفير الحماية المتكاملة لهذين القطاعين عبر معايير أمنية تكفل توفير هذه الحماية، ومن خلال مستويات أمن متعددة ومختلفة من حيث الطبيعة.

---

[30] فالبيانات هي المادة الخام الأساسية التي سيقوم الحاسب بتنفيذ تعليمات البرنامج التطبيقي عليها حرفيا للحصول على المعلومات المصرفية، أنظر:

_ أحمد علي حسين، **نظم المعلومات المحاسبية، – الإطار الفكري و النظم التطبيقية**، (الدار الجامعية، الإسكندرية، ج م ع، 2004)، ص. 24.

[31] **شبكات الإتصال:** أو شبكات اتصال البيانات، والتي تصل بين مجموعات حواسيب مرتبطة ببعضها البعض أو مع الوحدات التكنولوجية الأخرى كالطابعات و غيرها. وهذه الشبكات أنواع: _شبكات الإتصال المحلي ***Réseaux Locaux*** على صعيد المنظمة._ شبكات الإتصال الموسع ***Réseaux Etendus*** على الصعيد الوطني و الدولي. أنظر:

_ Marie–Hélène Delmonde et Autres, **Management des Systèmes d'Informations**, (Dunod, Paris, France, 2003), P. 59.

التساؤل الثالث: ماهي أنماط ومستويات الحماية؟ البرامج التدريبية من مهامها التعريف بأنواع الحماية المطلوبة من الموظف أن يعرفها ويتدرب عليها[32]:

1 - **الحماية المادية:** وتشمل كافة الوسائل التي تمنع الوصول إلى نظم المعلومات وقواعدها كالأقفال والحواجز والغرف المحصنة وغيرها من وسائل الحماية المادية التي تمنع الوصول الى الاجهزة الحساسة.

2- **الحماية الشخصية:** وهي تتعلق بالموظفين العاملين على النظام التقني المعني من حيث توفير وسائل التعريف الخاصة بكل منهم وتحقيق التدريب والتأهيل للمتعاملين بوسائل الأمن الى جانب الوعي بمسائل الأمن ومخاطر الإعتداء على المعلومات.

3- **الحماية الإدارية:** ويراد بها سيطرة جهة الإدارة على ادارة النظم المعلومات وقواعدها مثل التحكم بالبرمجيات الخارجية أو الأجنبية عن المنشأة، ومسائل التحقيق بإخلالات الأمن، ومسائل الإشراف والمتابعة لأنشطة الرقابة اضافة إلى القيام بأنشطة الرقابة ضمن المستويات العليا ومن ضمنها مسائل التحكم بالإشتراكات الخارجية.

4- **الحماية الإعلامية- المعرفية:** كالسيطرة على إعادة انتاج المعلومات وعلى عملية إتلاف مصادر المعلومات الحساسة عند اتخاذ القرار بعدم استخدامها.

التساؤل الرابع: ما هي المخاطر التي تتطلب الحماية؟ تصنيف هذه المخاطر ضمن قوائم تبعا لأساس التصنيف، فتصنف كمخاطر من حيث مصدرها ومن حيث وسائل تنفيذها، ومن حيث غرض المتسببين بهذه المخاطر، ومن حيث أثرها على نظام الحماية وعلى المعلومات محل الحماية. وهو ما سنقف عليه وبشكل أخر في العنصر الموالي.

ثانيا/ تحليل العوامل المهددة لأمن الأنظمة الآلية للمعلومات

تعمل الإدارة المختصة في أمن المعلومات بتوضيح المخاطر للموظف التي يمكن أن يكون سببا في وقوعا وهذا لتجنبها مستقبلا، من بين العوامل المتسببة في الخطر في البنوك والمؤسسات المالية ما يلي33:

1_**أفعال المتعاملين(الأفراد)غير مقصودة:** تكون في الغالب نتيجة ضغط شديد في العمل أو ضعف في القدرات الذاتية في الإنضباط والإهتمام لدى المستخدمين[34] مثل: إرسال تقارير بالخطأ، وضع كلمة السر في

[32] عائض المري، مرجع سابق، ص, 1,

[33] أحمد عوض حاج علي وعبد الأمير خلف حسين، **أمنية المعلومات وتقنيات التشفير**، (دار الحامد للنشر، عمان، الأردن، 2005)، ص.20-22.

المكان يسهل معرفتها، نسيان إغلاق الشاشات فتبقى مفتوحة وعارضة لبيانات غير مسموح بعرضها أو نتيجة مشاكل أو عطل في الأجهزة والبرامج... أما تغيير البيانات فأهم مسبباته هو الخطأ غير المقصود عند إدخال وتعديل البيانات التأمينية.

2_**أفعال المتعاملين المقصودة**: مثل معالجة محرفة، أو تشغيل محرف للبرنامج، إطلاع الآخرين على بيانات هامة، نقل بعض البرامج والبيانات الخاصة، تدمير أو تزييف برنامج أو معلومة أو إحداث عطل[35] أو غير ذلك من الأفعال المقصودة، ويطلق على هذه الأخطار الناتجة عن مستخدمي النظام يوميا بإسم أخطار مرتبطة بالإستغلال ***les Risques Liés à l'Exploitation*** [36].

عند تحليل الدوافع التي تؤدي إلى خيانة الموظفين مع النظام تجدها تتدرج من الخيانة العظمى بدافع اعتقادي أو سياسي أو مادي إلى خدمة بنك أخرى منافس بدافع مادي أو انتقامي إلى خدمة أفراد بتمليكهم معلومات عن أفراد آخرين منافسين بدافع مادي أو دافع صداقة أو خدمات ذوي القربى أو أصدقاء بتحسين بيانات تخصهم إلى الإنتقام من زملاء أو غيرهم بدوافع وهو أدنى درجة من حيث الخطورة.

3_**الإعتداء الخارجي**: نعني بالاعتداء الخارجي أن يتمكن أشخاص من غير المتعاملين مع النظام البنكي من الإطلاع أو تغيير أو مسح أو سرقة بعض أوكل معلومات النظام. تنشأ هذه المخاطر من عدم التأمين الكافي للنظم مما يجعلها عرضة لعمليات الهاكرز ***Hacker***. الإعتداء على المواقع الإلكترونية بالدخول غير المشروع، سواء نتج عنه تدمير هذه المواقع أو شغلها أو إتلاف ما تحويه من قواعد بيانات أو معلومات، بل مجرد الدخول غير المشروع عدته بعض الأنظمة الدولية مخالفة توجب الجزاء. وقد يكون الإعتداء على الشبكة المعلوماتية بإيقافها أو تعطيلها أو تدمير أو مسح البرامج أو البيانات الموجودة أو المستخدمة فيها أو حذفها أو تسريبها أو إتلافها أو تعديلها.

---

[34] كما أن الإعتداء خصوصية الفرد عند معالجة بياناته إلكترونياً وذلك بتغيير الغرض الذي من أجله جمعت البيانات أو قيام غير المختص بالإطلاع عليها يعد صورة حديثة في الإعتداء الإلكتروني تطلب تدخل المنظم بوضع ما يحمي خصوصية الأفراد عند معالجة بياناتهم.

[35] العطل (***Panne***): خطأ يحدث في المعدات يجعلها لا تعمل بصورة صحيحة، وهناك العطل التدريجي والعطل الخفيف، كما توجد عدة تقنيات في التعامل مع الأعطاب في الأجهزة مثل التنبؤ بالخطأ، تسجيل الخطأ، معدل الفشل ***Failure Rate*** لمزيد من المعلومات، أنظر:

- تيسير الكيلاني، **معجم الكيلاني لمصطلحات الكمبيوتر والإنترنت**، (مكتبة لبنان ناشرون، بيروت، لبنان، 2004). ص. 286 – 287.

[36] Michelle Lafitte, **Les Systèmes d'Information dans les Etablissements Financières**, (Presses de Jouve, Paris, France, 2000), P. 230.

يسمى كذلك هذا الإعتداء بالإختراق والذي يتمثل في عبث بعض الأشخاص الخارجين بالأنظمة المصرفية[37]، ووفقا لتصنيف البنك المركزي للمخاطر التي تتعرض لها البنوك والمؤسسات المالية نتيجة استخدام التكنولوجيا والتي تتمثل في: مخاطر التشغيل، مخاطر السمعة والمخاطر القانونية[38].

4_**الكوارث الطبيعية والحريق**: ربما تكون أقل خطورة وأيسر، حيث المرونة في الخزن وإمكانية وجود نسخ مسندة للبرامج والبيانات في أماكن بعيدة ومتعددة، وكذلك ما تسببه الذبذبات الكهربائية العالية من أخطار نتيجة للأعطاب المفاجئة في نظام الكهرباء.

على العموم، يمكن حصر العوامل التي تؤدي الى المخاطر والناتجة عن المعلوماتية في عوامل بشرية، مادية، وعوامل خارجية[39].

5_**تدمير أنظمة المعلومات الخاصة بشركات المالية**: لتدمير نظام معلومات سواء كليا أو جزئيا لابد من إختراقه أولا، ولكي تتم عملية الإختراق لابد من وضع برنامج يتم تصميمه خصيصا لهذه العملية، ويعتبر برنامج حصان طروادة ***Trojan Horse***40 من البرامج الخطيرة التي تستخدم في عمليات اختراق نظام المعلومات الخاص بشركات التأمين أو المؤسسات المالية الأخرى، وتكمن خطورة هذا البرنامج في كونه يتيح للمخترق أن يحصل على كلمة السر***Pass Word*** للدخول في هذا النظام[41]، إضافة إلى هذه البرامج هناك الفيروسات ***Virus*** والفيروس هو: "برنامج صغير طور خصيصا لتنفيذ أعمال تخريبية على الحاسب الآلي، يحتوي هذا النوع من البرامج على أوامر تخريبية معينة في نص الشفرة التي كتب بها"[42]،

أو هو عبارة "عن برنامج له أهداف تدميرية يهدف إلى إحداث ضرر جسيمة بنظام الكومبيوتر أومكوناته"[43]. إذن الفيروس عبارة عن برنامج خارجي مكتوب بإحدى لغات البرمجة، صنع عمدا من قبل المبرمجين، وهو قادر على التناسخ والإنتشار، ويستطيع الدخول إلى البرامج المصرفية بغرض تغيير خصائصها أو إزالتها أو تعديلها أو تخريبها وما شابهها من عمليات.

---

[37] مفتاح صالح ومعارفي دليلة، **البنوك الإلكترونية**، مداخلة ضمن المؤتمر العلمي الخامس بعنوان: نحو مناخ استثماري وأعمال مصرفية إلكترونية_ جامعة فيلادلفيا، عمان، الأردن، يومي 4 و5 يوليو 2007، ص. 5 .

[38] رافعة ابراهيم الحمداني، **أثر استخدام التكنولوجيا المصرفية في ظاهرة غسيل الأموال والجهود الدولية لمكافحتها**، المؤتمر العلمي الرابع، استراتيجيات الأعمال في مواجهة تحديات العولمة، جامعة فيلادلفيا، عمان، الأردن، يومي 14 و 15 مارس ، 2005، ص9.

[39] Michelle Lafitte, OP. Cit. P. 230

[40] Tout le monde ou presque et même les plus jeunes connaissent aujourd'hui les variétés de virus qui sont les plus fréquents sur cyber espace. Les « **Troyan Horses** », « **Spywares** », « **Malwares** », « **dialers** »

[41] منير وممدوح محمد الجنبيهي، **البنوك الإلكترونية**، (دار الفكر الجامعي، الإسكندرية، مصر، 2005) ص. 132.

[42] محمود الربيعي وآخرون، **المعجم الشامل لمصطلحات الحاسب الآلي والإنترنت**، (مكتبة العبيكان، الرياض، السعودية، 2001)، ص. 446

[43] علاء عبد الرزاق السالمي وحسين علاء عبد الرزاق السالمي، **تكنولوجيا المعلومات**، دار وائل للنشر والتوزيع، بيروت، لبنان، 2004)، ص.207.

ثالثا/ ادارة الخطر المعلوماتي ***Management de Risques Informatiques***

تعمل ادارة تقنية أمنية المعلومات على ادارة الخطر المعلوماتي لتجد نفسها تجيب على السؤال التالي:

التساؤل الرابع : ما العمل على عدم تحقق أي من المخاطر رغم وجود وسائل الحماية؟

وإجابة هذا التساؤل هو ما يعرف مخطط أو طريقة مواجهة الأخطار عند حصولها، فبشكل عام، الحماية المعلوماتية تستند على مبدأ أو طريقة *La Roue de la Deiming ou la Methode de PDCA* من أجل وضع خطة أو طريقة لإدارة مخاطر تكنولوجيا الإعلام والإتصال داخل البنك، ويستخدم هذا المبدأ على تحديد نهج لتنفيذ سياسة أمنية فعالة وإدراجه في سياق التحسين المستمر لضمان الهدوء والتطور يسيطر عليها نظام المعلومات البنكي كما يوضحه الشكل الموالي:

الشكل رقم(2): عمليات حماية النظام المعلوماتي المصرفي

Source : ***http://www.nbs-system.com/blog/introduction-a-la-securite-informatique.html***

من خلال الشكل يمكن القول أن أي خطر معلوماتي لابد من إدارته وفق أربعة خطوات:

_ تنفيذ عملية حماية المعلومات المصرفية يكون أولا من خلال تحديد السياسة الأمنية وتحديد هوية المخاطر ووضع أهداف السلامة.

_ ثم من الضروري وضع تدابير الأمن المحددة لتحقيق الأهداف التي تم وضعها مسبقا.

_ بعد التحقق من أن هذه التدابير تشمل القسم الأعظم من سلسلة أمن المعلومات وأمن النظام البنكي، لابد من المتابعة والمراقبة للتأكد من فعالية نظام الحماية الموضوع.

_ وأخيرا، تحليل النتائج وفقا لمستوى الأمن الذي يتحقق، وتحديد الموارد التي تتطلب تغييرات، ومن ثم متابعة تطور التهديدات الجديدة وتقديم تدابير السلامة.

في الأخير، يمكن القول بالفعل أن أمن المعلوماتية هو عملية تتطور بإستمرار. هذه العملية لتطوير نظام المعلومات في البنوك، سواء على مستوى التكنولوجيا المصرفية أو من الناحية التنظيمية للموارد المستخدمة لتشغيلها. وأثناء القيام بالبرامج التدريبية المهم أن تكون استجابة ما لتنمية للعنصر البشري ملائمة لموقع أو وضع معين وأيضا متى لا تكون كذلك. مع ضرورة أن تتوفر في اخصائي أمن المعلومات المدربين مهارات الإتصال، الإنصات، الإقناع، اللباقة، الثقة بالنفس، الهدوء، التواضع...[44].

المحور الخامس: موقع العنصر البشري البنكي في إطار الوقاية والحماية للمعلومات المالية المصرفية.

إن مهام المتصلين بنظام أمن المعلومات المصرفية تبدأ في الأساس من حسن إختيار الأفراد المؤهلين وعمق معارفهم النظرية والعملية، على أن يكون مدركا أن التأهيل العملي يتطلب تدريبا متواصلا ولا يقف عند حدود معرفة وخبرة هؤلاء لدى تعيينهم، وبشكل رئيس فإن المهام الإدارية أو التنظيمية تتكون من خمسة عناصر أو مجموعات رئيسة: تحليل المخاطر، وضع السياسة أو الإستراتيجية، وضع خطة الأمن، وضع البناء التقني الأمني– توظيف الأجهزة والمعدات والوسائل، وأخيرا تنفيذ الخطط والسياسات.

أولا/ المهام والواجبات الإدارية والشخصية *Administration and Personnel Responsibilities*

ومن المهم إدراك أن نجاح الواجبات الإدارية أو الجماعية للبنك يتوقف على إدراك كافة المعنيين في الإدارة(بمهامهم التقنية والإدارية والمالية) إستراتيجية وخطة وواجبات الأمن والتزام المؤسسة بإعتبار مسائل الأمن واحدا من الموضوعات التي يدركها الكافة ويتمكن الكل من التعامل مع ما يخص واجباتهم من بين عناصر الأمن.

وعلى المستوى الشخصي أو مستوى المستخدمين، فإن على الإدارة البنكية أن تضع التوجيهات الكافية لضمان وعي عام ودقيق بمسائل الأمن، بل المطلوب بناء ثقافة الأمن لدى العاملين والتي تتوزع بين وجوب مراعاة أخلاقيات استخدام التقنية وبين الإجراءات المتطلبة من الكل لدى ملاحظة أي خلل، وعلى ادارة البنك

تحديد للمستخدمين ما يتعين عليهم القيام به والأهم ما يحظر عليهم القيام به عند استخدامهم للوسائل التقنية المختلفة.

---

[44] عبد الكريم بوحفص، مرجع سابق، ص. 192 .

ثانيا/ ضوابط أمن المعلومات في البنوك والمؤسسات المالية

على الإدارة في البنوك والمؤسسات المالية تعريف موظفيها ببعض الضوابط للتخفيف من المخاطر، من خلال تنفيذ واحد أو أكثر من ثلاثة أنواع مختلفة من الضوابط[45]:

1_**الضوابط الإدارية**: أو الرقابة الإدارية (وتسمى أيضا الضوابط الإجرائية) تمثل في السياسات والإجراءات والمعايير والمبادئ التوجيهية. فالرقابة الإدارية تشكل إطارا لإدارة الأعمال التجارية في المؤسسات المالية وإدارة الأفراد. إنها إطلاع الموظفين على كيفية العمل وكيفية تشغيل العمليات المالية اليومية. ومن الأمثلة الأخرى على الضوابط الإدارية في البنوك والمؤسسات المالية: السياسة الأمنية، سياسة كلمة السر، سياسات التوظيف، والسياسات التأديبية.

2_**الضوابط التقنية**: وتسمى أيضا الضوابط المنطقية، وهي استخدام البرمجيات والبيانات لرصد ومراقبة الوصول إلى نظم المعلومات والمحوسبة. على سبيل المثال: كلمات السر، والجدران النارية، وكشف التسلل، قوائم التحكم بالولوج، وتشفير البيانات والضوابط المنطقية.

3_**الضوابط المادية**: تتمثل رصد ومراقبة البيئة في مكان العمل ومرافق المعلوماتية. بالإضافة الى مراقبة الدخول والخروج من وإلى مصالح البنك. على سبيل المثال: الأبواب والأقفال، والتدفئة وتكييف الهواء والدخان وأجهزة إنذار الحريق ونظم إخماد الحريق، وكاميرات المراقبة، ووضع المتاريس، وحراس الأمن، وتأمين الكابلات، وما إلى ذلك فصل الشبكة، ومكان العمل في مجالات وظيفية هي أيضا الضوابط المادية.

رقابة هامة من المنطقي أن لا يتم التغاضي عنها كثير من الأحيان هو مبدأ الإمتيازات الأقل. هذا المبدأ يتمثل في أن الفرد أو برنامج أو عملية في النظام لا يتم منح أي امتيازات الوصول أكثر من ضرورية لأداء المهمة.

ثالثا/ بعض أساليب نظم الرقابة الداخلية في البنوك والمؤسسات المالية

تقوم إدارة الموارد البشرية في ظل المخاطر الجمة التي تحدثها تكنولوجيا الإعلام والإتصال بتدريب وتعليم موظفيها واكسابهم مهارات عدة تخص استخدامهم للطرق وأساليب عديدة من أجل أمنية المعلومات المصرفية، من أمثلتها مايلي:

[45] لمزيد من المعلومات أنظر الموقع الإلكتروني التالي: http://ar.wikipedia.org/wiki/sécurité_de_l'information

1_**إستخدام وسائل تعريف المستخدم:** ويتم استخدامها لحماية النظام من أخطار التدخل الغير الشرعي بإنتحال صفة شخص مصرح له بإستخدام النظام، وتستخدم للحماية من هذه الأخطار ما يلي[46]:

2_**كلمات السر:** حيث تحرص البنوك على وضع كلمات المرور الخاصة بالمستخدمين ومنع القراصنة من الإستيلاء عليها.

3_**التعريف باستخدام الخصائص البيولوجية:** وذلك بالإعتماد على الصفات البيولوجية لشخص المستخدم مثل: طول الجسم، بصمة الأصبع أو بصمة الصوت...

5_**التوقيعات الرقمية والإلكترونية *Electronic Digital Signature*** : هو وسيلة من وسائل تشفير البيانات يستخدم للتأكد من أن الرسالة قد جاءت من مصدرها دون تعرضها لأي تغير أثناء عملية النقل. ويمكن للمرسل استخدام المفتاح الخاص لتوقيع الوثيقة إلكترونيا، أما من طرف المستقبل، فيتم التحقق من صحة التوقيع عن طريق إستخدام المفتاح المناسب[47].

تستخدم هذه التوقيعات للتأكد من أن الرسالة قد جاءت من مصدرها دون تعرضها لأي تغيير أثناء عملية النقل، وبإستخدام التوقيع الرقمي يتم تأمين سلامة الرسالة والتحقق من صحتها، كما أنه من فوائد هذا التوقيع أيضا أنه يمنع المرسل من التذكر للمعلومات التي أرسلها[48].

6_**جدران النار *Fire Walls*:** جدار الحماية عبارة عن مجموعة من الأنظمة توفر وسيلة أمنية بين الأنترنت وشبكة البنك الداخلية حيث تجبر عمليات الدخول إلى الشبكة الداخلية والخروج منها للمرور عبر هذا الجدار الذي يتصدى لجميع محاولات الدخول للشبكة بدون صفة[49]. ويسمح بالمرور للمصرح له فقط كما هو معرف بسياسة الأمن المحلية[50].

هي أدوات تقع على طرف شبكة الإنترنت الخاصة بالمنظمة، تعمل كمنفذ للإنترنت وتعمل على تحقيق الرقابة على المعلومات من وإلى الشبكة، كما يوجد نوعين من الجدران النارية[51]:

_جدران الحماية بالفلترة للرسائل(حزم ***Paquets***).

---

[46] أمين السيد أحمد لطفي، **مراجعة وتدقيق نظم المعلومات**، (الدار الجامعية، الإسكندرية، مصر، 2005)، ص. 771_ 773.

[47] Mohamed Louadi, **Introduction aux Technologies de l'Information et de la Communication**, Centre de Publication Universitaire, P. 398.

[48] منير وممدوح محمد الجنبيهي، مرجع سابق، ص. 22.

[49] محمود محمد أبو فروة، **الخدمات البنكية الإلكترونية عبر الإنترنت** ، (دار الثقافة للنشر والتوزيع، عمان، الأردن، 2009)، ص.93_94.

[50] جاري شنايدر، **التجارة الإلكترونية**، تعريب سرور علي ابراهيم سرور، (دار المريخ لنشر، الرياض، المملكة العربية السعودية، 2008)، ص. 575.

[51] Mélissa Saadoun, **Technologies de l'Information et Management**, (Hermès Sciences Publications, Paris, France, 2001), P. 41.

_جداران الحماية للتطبيقات(جسر التطبيقات ***Passerelle d'Application***).

7_ **الرقابة على الأمن**: بمعنى القيام بمراجعة دورية ضمن نظم الرقابة الداخلية على أمن المعلومات التي تطبقها المعلومة بغرض الكشف عن نقاط الضعف والعمل على علاجها.

الخاتمة: ينظر في الوقت الحاضر إلى تنمية الموارد البشرية في البنوك بأبعادها الثلاثة على أنها عملية استراتيجية، تأخذ شكل نظام فرعي مكون من أجزاء متكاملة، وتعمل ضمن نظام واستراتيجية أكبر هي استراتيجية البنك وضمن إطار ودور تسيير الموارد البشرية فيها.

إن أمن المعلومات يحتاج إلى استراتيجية قوية بهدف حماية البنية التحتية والتصدي للتهديدات، وتحقيقاً لذلك تدقق إدارة النك في اختيار الكوادر الجيدة بين أفضل المتقدمين بالبنك والسعي إلى زيادة فعالية الكوادر القائمة وإعدادهم إعداداً كافياً بما يتمشى وسياسة أمنية معلوماته المصرفية وإدخاله لأساليب التقنية الحديثة وتطوير خدماته.

البنوك الجزائرية وكباقي البنوك العالمية عليها تكييف مواردها البشرية وتكوين المختصين في أمن المعلومات المصرفية بمتطلبات العمل المصرفي الإلكتروني، وهو النمط التغييري الذي تفرضه الحاجات الجديدة للقوى العاملة حاضرا ومستقبلا، وحاجة هذه القوى إلى التعليم المستمر. وأن أمن المعلومات وعملية التأهيل وتنمية الموارد البشرية لا تخص الموظف البنكي وفقط وأنما كذلك العملاء الذين يتعامل معهم البنك، لأن الثغرة الأمنية يمكن أن يتسبب في وقعها عملاء البنك أنفسهم وليس موظفوه.

في الأخير ويمكن القول أن تنمية الموارد البشرية في البنوك والمؤسسات المالية في مجال التكنولوجيا المالية يعتبر خطوة أساسية لمكافحة الجريمة الإلكترونية مستقبلا وحفاظا على أمنية تكنولوجيا المعلومات المالية في القطاع المالي والمصرفي الجزائري.

التوصيات: نبرز في نهاية هذه الأوراق عددا من التوصيات لإدارات البنوك الجزائرية المهمة في هذا المجال كون أن المعايير العالمية والإتفاقيات الدولية تشدد على أهمية توعية وتدريب العاملين في مجال أمن المعلومات او الذين يتعاملون مع المعلومات بجميع أشكالها:

_ أهمية التركيز على البعد الأخلاقي كأهم بعد من أبعاد التنمية البشرية البنكية في مجال أمن المعلومات لهذا فإن برامج التوعية الأمنية والأخلاقية هي من أهم وأكثر الخطوات فاعلية لتقليل أو تحجيم الأخطار الداخلية والتي تمثل اكثر من 90% من مشكلات أمن المعلومات طبقا للإحصائيات العالمية.

_على إدارات البنوك الجزائرية إتاحة فرص المشاركة للعنصر البشري في المؤتمرات والندوات العلمية والعربية والعالمية المتخصصة في أمنية تكنولوجيا المعلومات المصرفية والمالية.

_تكوين المختصين في المعلومات المصرفية والمالية بمتطلبات المجتمع الرقمي والعمل المصرفي الإلكتروني، وهو النمط التغييري الذي تفرضه الحاجات الجديدة للقوى العاملة حاضرا ومستقبلا، وحاجة هذه القوى إلى التعليم المستمر.

_العناية المالية والمادية بوظيفة البحث والتطوير في البنوك وبأقسام تكنولوجيات الإعلام والاتصال أو بمصالح أنظمة المعلوماتية، وكذلك التكوين المهني والمستمر للموظفين لضمان التجديد والتحديث انسجاما لإجراءات المتخذة لحماية المعلومات المصرفية .

_إن مشكلة أمن المعلومات المصرفية والمالية مشكلة عالمية، لذا وجب على البنوك الجزائرية الإستفادة من تجارب الآخرين الأخرى وإنشاء إطار موحد لحماية المعلومات.

_ضرورة اتحاد البنوك الجزائرية مع الكيانات الإقتصادية الهامة في محاولة منها للقيام ببناء حائط صد إلكتروني مضاد لما قد تتعرض له من هجمات ومحاولات اختراق وقرصنة من محترفي إرتكاب جرائم الإنترنت.

_أهمية عقود الشراكة مع مؤسسات الحماية والوقاية من مخاطر التكنولوجيا للحصول على برامج الحماية مثل شركة سيمانتيك المُتخصصة ببرامج الحماية من الفايروسات.

_تعزيز التكوين في المجالات القانونية والتشريعية والتقنية والعلمية، وتعزيز وتحسيس الفاعلين في المجتمع بأمن الأنظمة المعلوماتية وبالجرائم الإلكترونية خاصة العملاء.

_اعتماد وسائل الإعلام التي يمكن أن تساهم بدورها في هذه العملية، ولا سيما من خلال الأنشطة التحسيسية حول مخاطر هذا النوع من الجرائم.

_ضرورة إنشاء مراكز التدريب في مجال أمنية المعلومات المصرفية، تضم قاعات مهيأة بكافة الأجهزة التقنية التي تساعد المحاضر(القائم بالعملية التدريبية) على عرض مادته، ولوحات عرض الكترونية وعادية كما تضم مكتبة تحتوي على الكتب والدوريات التي لها علاقة بالمجال المصرفي والمالي الإلكتروني.

_على البنوك تحديث تكنولوجيا المعلومات وتطويرها دون توقف، لمواجهة التهديدات أو الحد منها، إذ إن الذين يمارسون عملية الإحتيال والتعدي والتجسس عبر وسائل اتصالهم يقومون بتطوير الأجهزة ولديهم عدد من الخبراء والفنيين.

_امكانية إشراك جهاز أمني متدرب ليس فقط أمنيا بل فنيا وإداريا وحسن اختيار المدربين في تقديمال برامج التدريبية مستمرة لموظي البنوك للتصدي لمحاولات الإضرار بأمن المعلومات المصرفية، وأن يكون هذا الجهاز قادر على رصد مواقع المجرمين والمتسللين.

قائمة المراجع باللغة العربية:

_ حسين يرقى، **استراتيجية تنمية الموارد البشرية في المؤسسة الإقتصادية،_حالة مؤسسة سوناطراك_**، مذكرة مقدمة كجزء من متطلبات الحصول على شهادة دكتوراه دولة في العلوم الإقتصادية، تخصص تسيير، جامعة الجزائر، الجزائر، 2007_2008.

_ توماس أ. ستيوارت، **ثورة المعرفة،_رأس المال الفكري_ ومؤسسة القرن الحادي والعشرين**، ترجمة علاء أحمد صلاح، الدار الدولية للإستثمارات الثقافية، القاهرة، مصر، 2004.

_ كمبا هارول إسلام، **تنمية رأس المال البشري لمبادرات تقديم الخدمات على الخط في أقل البلدان نمواً_ تحديات وفرص_**، http://www.ituglobalsymposium2008.info/Doc.26-Baharl%20Islam-India-A.W11.doc

_ عبد المعطي محمد عساف، **التدريب وتنمية الموارد البشرية،_ الأسس والعمليات_** دار زهران للنشر والتوزيع، عمان، الأردن، 2008.

_ الداودي الشيخ، **تحليل أثر التدريب والتحفيز على تنمية الموارد البشرية في البلدان الإسلامية**، مجلة الباحث، مجلة دورية أكادمية متخصصة محكمة تعنى بالبحوث الإقتصادية، جامعة ورقلة، العدد 6، 2008.

_ عبد الكريم بوحفص، **التكوين الاستراتيجي لتنمية الموارد البشرية**، ديوان المطبوعات الجامعية، الجزائر، 2010

_ بسمة أحمد ابراهيم أبو زيد، **واقع إدارة تنمية الموارد البشرية في المصارف العاملة في فلسطين وسبل تطويره**، رساله مقدمة استكمالا لمتطلبات الحصول على درجة الماجستير في إدارة الأعمال، غزة، فلسطين، 2008.

_ محمد حسين سيد، **أهمية العنصر البشرى في تحقيق أهداف الشركات**، بحث مقدم إلى الأكاديمية العربية البريطانية للحصول على درجة الدكتوراه في إدارة الموارد البشرية تحت إشراف فريق التعليم عن بعد، دون سنة نشر، www.abahe.co.uk

_ منير نوري، **تسيير الموارد البشرية**، ديوان المطبوعات الجامعية، الجزائر، 2010.

_ عادل محمد زايد، **ادارة الموارد البشرية،_ رؤية استراتيجية_** كلية التجارة، جامعة القاهرة، 2003.

_ محمد البلتاجي، **دور المعاهد المصرفية في تأهيل العاملين في المؤسسات المالية الإسلامية**، المؤتمر الخامس للهيئات الشرعية للمؤسسات المالية الإسلامية، هيئة الحاسبة والمراجعة، البحرين، يومي 19 و20 نوفمبر 2005.

_ جنيفر جوي ماثيور، **تنمية الموارد البشرية**، ترجمة علا أحمد صلاح، مجموعة النيل العربية، القاهرة، مصر، 2008.

_ عائض المري، **أمن المعلومات، ماهيتها هناصرها واستراتيجيتها**، معلومات قانونية، الدراسات والإستشارات القانونية، 6 نوفمبر 2011. أنظر الموقع الإلكتروني التالي: http://www.dralmarri.com/show.asp?field=res_a&id=205

_ أحمد علي حسين، **نظم المعلومات المحاسبية، – الإطار الفكري والنظم التطبيقية**، الدار الجامعية، الإسكندرية، ج م ع، 2004.

_ أحمد عوض حاج علي وعبد الأمير خلف حسين، **أمنية المعلومات وتقنيات التشفير**، دار الحامد للنشر، عمان، الأردن، 2005.

_ تيسير الكيلاني، **معجم الكيلاني لمصطلحات الكمبيوتر والإنترنت**، مكتبة لبنان ناشرون، بيروت، لبنان، 2004.

_ مفتاح صالح ومعارفي دليلة، **البنوك الإلكترونية**، مداخلة ضمن المؤتمر العلمي الخامس بعنوان: نحو مناخ استثماري وأعمال مصرفية إلكترونية_ جامعة فيلادلفيا، عمان، الأردن، يومي 4 و5 يوليو 2007.

_ رافعة ابراهيم الحمداني، **أثر استخدام التكنولوجيا المصرفية في ظاهرة غسيل الأموال والجهود الدولية لمكافحتها**، المؤتمر العلمي الرابع، استراتيجيات الأعمال في مواجهة تحديات العولمة، جامعة فيلادلفيا، عمان، الأردن، يومي 14 و15 مارس، 2005.

_ منير وممدوح محمد الجنبيهي، **البنوك الإلكترونية**، دار الفكر الجامعي، الإسكندرية، مصر، 2005.

_ محمود الربيعي وآخرون، **المعجم الشامل لمصطلحات الحاسب الآلي والإنترنت**، مكتبة العبيكان، الرياض، السعودية، 2001.

_ علاء عبد الرزاق السالمي وحسين علاء عبد الرزاق السالمي، **تكنولوجيا المعلومات**، دار وائل للنشر والتوزيع، بيروت، لبنان، 2004.

_ أمين السيد أحمد لطفي، **مراجعة وتدقيق نظم المعلومات**، الدار الجامعية، الإسكندرية، مصر، 2005.

_ محمود محمد أبو فروة، **الخدمات البنكية الإلكترونية عبر الإنترنت**، دار الثقافة للنشر والتوزيع، عمان، الأردن، 2009.

_ جاري شنايدر، **التجارة الإلكترونية**، تعريب سرور علي ابراهيم سرور، دار المريخ لنشر، الرياض، المملكة العربية السعودية، 2008 .

قائمة المراجع باللغة الفرنسية:

_Mélissa Saadoun, **Technologies de l'Information et Management**, Hermès Sciences Publications, Paris, France, 2001.

_Mohamed Louadi, **Introduction aux Technologies de l'Information et de la Communication** , Centre de Publication Universitaire.

_ Michelle Lafitte, **Les Systèmes d'Information dans les Etablissements Financières**, Presses de Jouve, Paris, France, 2000.

_ Marie–Hélène Delmonde et Autres, **Management des Systèmes d'Informations**, Dunod, Paris, France, 2003.

قائمة مواقع الإنترنت:

_***http://ar.wikipedia.org/wiki/sécurité_de_l'information*** **/ *voir le*** : 01_11_2011

_***http://www.nbs-system.com/blog/introduction-a-la-securite-informatique.html*** **/ *voir le*** : 28_10_2011

_***http://fr.wikipedia.org/wiki/Peter_Drucker*** **/ *voir le :*** 15_10-2011

_***http://www.espacemanager.com/finance/securite-informatique-dans-le-secteur-bancaire-une-condition-sine-qua-non.html*** **/ *voir le*** : 05_11_2011

_***https://www.issa.org/*** ***voir le*** : 08_11_2011

_***http://www.issa-eg.org/index.php?option=com_content&view=category&id=43&Itemid=54*** **/ *voir le 16_10_2011***