
خدمات أكاديمية
كفاءات وطنية
معايير عالمية
دراسة
للاستشارات والدراسات والترجمة
UNIVERSITY
drasah1
www.drasah.com
00966555026526
00966560972772
info@drasah.com

خدماتنا

شركة دراسة
للاستشارات و الدراسات والترجمة

توفير المراجع العربية والأجنبية

التحليل الاحصائي وتفسير النتائج

الاستشارات الأكاديمية

جمع المادة العلمية

الترجمة المعتمدة

drasah1
info@drasah.com
00966555026526
00966560972772
drasah.com


دراسة
للاستشارات والدراسات والترجمة
تواصل معنا
00966555026526
00966560972772
متواجدون على مدار الســـاعة

التحول الرقمى فى مصر
هل يُلقي بمسئوليات جديدة على المراجع ؟

أستاذ دكتور
أحمد صلاح عطية
أستاذ المراجعة
كلية التجارة- جامعة الزقازيق

مجلة البحوث التجارية - كلية التجارة جامعة الزقازيق - المجلد الثالث والأربعون -يناير ٢٠٢١

ملخص :

تستهدف تلك الورقة البحثية ، إلقاء الضوء على مشكلة باتت تؤرق دول العالم أجمع الذى أضحى يسبح في مساحة لا نهائية من الفضاء السيبرانى ليعيش واقعا افتراضيا غاية فى التعقيد والتشابك ، وتحيط به المخاطر السيبرانية من كل جانب ، وهو مالفت نظر العديد من الباحثين والهيئات البحثية فى دول العالم المتقدم إلى المشاركة فى وضع ضوابط رقابية لضمان الأمن السيبرانى ، بما يوفر الحماية ضد الجرائم والانتهاكات الإلكترونية التى يمكنها إلحاق أضرار جسيمة على مستوى الدول أو منظمات الأعمال أو الأفراد .

على مستوى منظمات الأعمال ، يتركز نشاط المراجعة الداخلية فى تقييم والمساهمة فى تحسين أنظمة إدارة المخاطر والرقابة الداخلية والحوكمة ، وذلك من خلال اتباع أسلوب منهجى منظم وقائم على أساس المخاطر يستهدف فى الأساس خدمة الإدارة فى تحقيق أهدافها ، ومن هنا فإنه مع الدخول في بيئة التحول الرقمي إمتد نطاق نشاط المراجعة الداخلية لأعباء ومسئوليات جديدة باعتباره يمثل واحداً من أهم خطوط الدفاع عن المنظمة .

الكلمات المفتاحية : الأمن السيبرانى– التحول الرقمى– المراجعة الداخلية

مقدمة :

مع بدايات القرن الواحد والعشرين، تأكدت حقيقة النظر للمعلومات باعتبارها أصول Information Assets يتعين توفير الحماية لها ، باعتبار أن أي ضرر يصيبها ، يترتب عليه تداعيات خطيرة سواء على مستوى الدول أو المنظمات أو الأفراد ، وذلك في ظل هيمنة بيئة التحول الرقمي التي لم تعد خياراً ، بل أصبحت ضرورة ملحة للتطور ، وهو ما دعا المؤتمر السابع للشباب إلى إطلاق مبادرة "التحول الرقمي في مصر" مع تأكيد أن المبادرة تُعد مُتطلباً ضرورياً من متطلبات الأمن القومي المصري.[1]

الأمن السيبراني :

في بيئة التحول الرقمي يتم الاعتماد على الفضاء السيبراني Cyber Space كوسيط تعمل فيه كافة الشبكات والحاسبات والبرمجيات بالإضافة إلى حوسبة المعلومات ونقلها وتخزينها ، وذلك على مستوى العالم أجمع ، مما نتج عنه ارتفاع نسبة الإنتهاكات الإلكترونية التي يترتب عليها إلحاق الضرر بالعديد من الدول ومنظمات الأعمال والأفراد على مستوى العالم. وطبقا للمركز المصري للدراسات الاقتصادية ECES فقد تم تقدير الخسائر العالمية المتوقعة جراء تلك الانتهاكات بنحو 6 تريليون دولار مع حلول عام 2021 ، وهو مايُعد أكبر تحول للثروة في العالم من مجتمع الأعمال القانوني إلى مجتمع غير قانوني.[2]

استدعى ماسبق، ضرورة توافر تشكيلة متنوعة من الضمانات الأمنية التي تتناسب وطبيعة البيئة الرقمية الجديدة، مما ترتب عليه ظهور اصطلاح " الأمن السيبراني " Cyber Security الذي يمكن تعريفه بأنه " كل الأنشطة أو العمليات أو الإجراءات التنظيمية اللازمة لضمان حماية المعلومات ونظم الإتصالات بجميع أشكالها من مختلف الإنتهاكات فضلا عن منع أو تقليل الآثار المالية المرتبطة بها."[3]

يعد الأمن السيبراني واحداً من المخاطر الأساسية التي تواجه العالم ، حيث لم تعد الهجمات السيبرانية نتاج عمل فردي أو مجموعة من القراصنة ، لكنها أصبحت تضم متخصصين في ذلك النوع من الجرائم ولديهم قدرات تعادل – إن لم تكن أفضل – من كيانات مؤسسية بدول العالم المختلفة ، ومن هنا لم يعد أمن المعلومات رفاهية بل قضية أمن قومي . وهو ما دعا أربع هيئات

مهنية كبرى إلى إصدار مجموعة من الأطر والمعايير التي تتعلق بالأمن السيبراني من زوايا مختلفة هي:[4]

1- جمعية المراجعة والرقابة على نظم المعلومات Information Systems Audit and Control Association (ISACA) التي طورت إطاراً لإدارة تكنولوجيا المعلومات لتمكين الإدارة من عبور الفجوة بين متطلبات الرقابة ، والمسائل الفنية ، ومخاطر الأعمال في وقت واحد، أطلق عليه Control Objectives for Information and Related Technology (COBIT).

2- المنظمة الدولية للمعايرة International Organization for Standardization (ISO) التي طورت سلسلة ISO 27000 وهي معايير تمكن المنظمة من تطبيق ضوابط رقابية تدعم مبادئ أمن المعلومات فيها .

3- معهد المحاسبين القانونيين الأمريكي The American Institute of Certified Public Accountants (AICPA) الذي طور إطاراً للتقرير عن إدارة المخاطر السيبرانية يوفر للمنظمة معلومات مناسبة ومفيدة حول درجة فعالية برامجها لإدارة المخاطر السيبرانية. ويطلق على الهيكل الرئيسي لهذا الإطار System and Organization Controls (SOC).

4- المعهد الوطني للمعايير وتكنولوجيا المعلومات National Institute of Standards and Technology (NIST) الذي أصدر إطاراً لتحسين البنية التحتية للأمن السيبراني مبني على المعايير والإرشادات والممارسات القائمة بهدف توجيه منظمات الأعمال لمحاولة خفض الآثار المحتملة للمخاطر السيبرانية .

يمكن النظر إلى الأمن السيبراني باعتباره جزءا لايتجزأ من استراتيجية أي منظمة ، وبالتالي يتوجب تخصيص موارد كافية تضمن تحقيق الأهداف المأمولة منه بنجاح. ومن أبرز أمثلة الاستثمارات التي تنفق عليه من تلك الموارد :[5]

* بناء بنية تحتية للأمن السيبراني تمنع حدوث الانتهاكات .
* وضع وإقرار الضوابط الرقابية اللازمة مع قابلية تعديلها أو تحديثها كلما حدث تغيير في بيئة التهديدات التي تواجه المنظمة .

* توفير نظم لفحص ومراجعة أمن المعلومات بالمنظمة أولا بأول بما يسمح بالكشف عن أية انتهاكات مع تحديد المسئولين عنها .
* تدبير آليات لتقليل حجم الدمار والخسائر المترتبة على حدوث انتهاكات كما في حالة عمل بوالص تأمين ضد القرصنة لدى شركات التأمين .
* تنفيذ برامج التدريب والتعليم والتوعية بالأمن السيبراني .

وعلى ذلك يمكن القول ، أن الأمن السيبراني يُعد بمثابة أحد الأبعاد الجديدة للأمن القومي بمشتملاته من دول ومنظمات أعمال وأفراد ، حيث أحدث تغييرا جوهريا في مفاهيم الصراع والقوة والتهديد كنتيجة للانتقال من عالم مادي إلى عالم افتراضي غاية في التعقيد والتشابك ، وبالتالي أصبح الاهتمام بالأمن السيبراني ضرورة حتمية في عالم التحول الرقمي الذي شرعت مصر أخيراً في قطع خطوات حثيثة في اللحاق به .

مراجعة الأمن السيبراني :

تستهدف مراجعة الأمن السيبراني توفير تقييمات Assessments أمام الإدارة لسياسات وإجراءات الأمن السيبراني للمنظمة، ودرجة تطبيقها عمليا بفعالية، بالإضافة إلى ذلك تكشف مراجعة الأمن السيبراني أوجه القصور في الرقابة الداخلية والتنظيمية التي يحتمل تعريضها المنظمة للخطر.

وتركز مراجعة الأمن السيبراني على معايير وإرشادات وإجراءات خاصة بالأمن السيبراني، فضلا عن التحقق من مدى الالتزام بتطبيق الضوابط الرقابية ، بجانب المراجعات التشغيلية الأخرى بما يحقق:[6]

* توفير الحماية للبيانات الحساسة وعالية الخطورة ، والملكيات الفكرية المختلفة .
* حماية الشبكات التي عن طريقها يتم الاتصال بالمصادر المتعددة للمعلومات والبيانات .
* إقرار مبدأ المسئولية والمحاسبة للأجهزة وما تحويها من معلومات وبيانات .
* التحقق من أن خطط المنظمة للحماية من المخاطر السيبرانية، تغطي كل السيناريوهات المختلفة حال التعرض لهجمات سيبرانية .

ويتنوع نطاق مراجعة الأمن السيبراني ليشمل:[7]

- سياسات أمن المعلومات المتعلقة بالشبكات وقاعدة البيانات والتطبيقات الموجودة حاليا .

- الضوابط الرقابية لأمن المعلومات.
- الضوابط السائدة لمنع فقدان البيانات، وللولوج إلى الشبكات التي يتم تطبيقها حاليا بالمنظمة.
- نظم الاكتشاف والمنع وردود الأفعال تجاه الانتهاكات .

يرتبط نجاح عملية مراجعة الأمن السيبراني بمساهمة ثلاثة أطراف: إدارة المنظمة، إدارة المخاطر، والمراجعة الداخلية. وينظر للثلاثة باعتبارهم خطوط دفاعية تسهم بكفاءة وفاعلية في تطبيق كافة الضوابط الرقابية في ظل بيئة التهديدات التي تواجه المنظمة نتيجة التحول الرقمي، يضاف إلى ذلك أن مراجعة الأمن السيبراني بهذه الكيفية تتم بمعرفة ثلاث وظائف مستقلة مما يعني زيادة فرص الكشف عن الثغرات الأمنية ، وأوجه الضعف الرقابية.[8]

المراجعة الداخلية :

طبقا لما ورد بالمعيار رقم 2100 من معايير الأداء المهني الصادرة عن معهد المراجعين الداخليين الأمريكي IIA ، يقوم نشاط المراجعة الداخلية بتقييم والمساهمة في تحسين أنظمة إدارة المخاطر ، والرقابة الداخلية ، والحوكمة ، وذلك من خلال اتباع أسلوب منهجي منظم وقائم على أساس المخاطر.[9] وهو مايعني أنها تستهدف أساسا خدمة الإدارة في تحقيق أهدافها باعتبارها إحدى أهم آليات النظام الرقابي بالمنظمة ، والذي على أساسه يتم تطبيق مبادئ الحوكمة.

وبناء على تقدير المخاطر ، تعمل المراجعة الداخلية على تقييم مدى كفاءة وفاعلية نظام الرقابة الداخلية ، كما تقوم أيضا بإبلاغ الإدارة بالتأكيدات حول النجاح أو الفشل في التعامل معه ، بالإضافة إلى دورها المتنامي في نشر ثقافة إدارة الخطر والأمن السيبراني بالمنظمة ، والذي بدوره يتوقف إلى حد كبير على فهم المراجع الداخلي لأبعاد دوره المتمثل في مساعدة المنظمة في تحقيق أغراضها ، وليس مجرد حصر المشكلات والتقرير عنها .

من نافلة القول ، أن كبر حجم الاستثمار في الأمن السيبراني في بيئة التحول الرقمي يستلزم بطبيعة الحال إضافة أعباء جديدة على عاتق المراجعين الداخليين .

بصورة عامة ، من المفترض الاستعانة بمراجع متخصص في تكنولوجيا المعلومات لفحص الضوابط الرقابية المتعلقة بالتكنولوجيا ، في حين تقوم المراجعة الداخلية بفحص الضوابط المالية والتشغيلية والالتزام فيما يعرف بالمراجعة المالية Financial Audit والمراجعة التشغيلية

Operational Audit ومراجعة الالتزام Compliance Audit. وبدخول عصر التحول الرقمي أضحت غالبية المنظمات تعتمد على تكنولوجيا المعلومات لميكنة عملياتها ، وبالتالي إضمحل الحد الفاصل بين دور مراجع تكنولوجيا المعلومات والمراجع الداخلي ، لدرجة إصدار معهد المراجعين الداخليين الأمريكي IIA إرشادات في يونيو 2020 بوجوب أن يتوافر لدى المراجعين الداخليين فهم أساسي لوظائف وعمليات تكنولوجيا المعلومات في المنظمات التي يعملون فيها.[10] وعلى ذلك أصبح مطلوبا من المراجعين الداخليين فهم بيئة الضوابط الرقابية في المنظمة، وذلك لتقديم تأكيدات للجنة المراجعة ومجلس الإدارة بما إذا كانت الضوابط المطبقة مناسبة لتحقيق الهدف منهما سواء فيما يتعلق بالحوكمة أو تقييم المخاطر السيبرانية أو إدارة خطر الأمن السيبراني. وهو ما دعا البعض إلى النظر للمراجعة الداخلية باعتبارها خط الدفاع الثالث عن المنظمة ضد التهديدات والمخاطر السيبرانية المختلفة.[11]

مسئوليات المراجعة الداخلية تجاه الأمن السيبراني للمنظمة :

قبل الاسترسال في عرض الأعباء المستجدة على عاتق المراجع الداخلي نتيجة الأخطار السيبرانية، يتعين الإشارة إلى مسألتين هامتين لهما ارتباط ببيئة التحول الرقمي هما : التفويض ، والتخطيط .

التفويض، حيث نادراً ما تعطي المنظمة تفويضاً كاملاً للمراجع الداخلي للولوج إلى كافة المعلومات والبيانات بسبب وجود مناطق أو مجالات ذات خصوصية يتعذر ولوج المراجع إليها بدون الحصول على تفويض خاص. وفي حالات أخرى ، يتعين النص داخل التعاقدات القانونية للمنظمة مع العملاء والموردين على بند خاص يعطي الحق للمراجع الداخلي في مراجعة حساباتهم حال قيامهم بالتوقيع والسماح من خلال أجهزة التليفونات المحمولة على سبيل المثال.[12]

التخطيط ، حيث يعد تخطيط عملية المراجعة نقطة البداية للقيام بأي عملية مراجعة ، وفيما يتعلق بالأمن السيبراني صدرت إرشادات من معهد المراجعين الداخليين في مايو 2020 توصي بوضع خطة المراجعة على أساس تقييم المخاطر ، بما يعني وضع تخطيط شامل يستجيب للمخاطر المتغيرة مع التركيز على المخاطر ذات التأثير الأكبر على تحقيق المنظمة لأهدافها.[13] ويعني ذلك بطبيعة الحال ، ضرورة اهتمام المراجع الداخلي بالإلمام الكامل والفهم المستفيض لآثار وتداعيات

التهديدات والمخاطر السيبرانية التي تواجه المنظمة ، مع تضمين ذلك خطة المراجعة الداخلية المبنية على أساس المخاطر . وبناء عليه يتم إعداد خطة مراجعة سنوية يراعى فيها تحديد الأولويات والتوقيتات التي تتناسب مع ظروف ودورات النشاط بالمنظمة لتخفيض حدة الارتباك وكذا لزيادة فرص مشاركة أطراف هامة في عملية المراجعة مثل مسئولي تكنولوجيا المعلومات على سبيل المثال . بالتخطيط المناسب والجدول الزمني لأنشطة المراجعة ، يتم جمع الأدلة من خلال الكشف عن المناطق الخطرة ، والمخاطر المرتبطة بكل منها مع تجميع المعلومات الكافية .[14]

كما ألمحنا سابقا ، فإنه مع الدخول في عصر التحول الرقمي ، إمتد نطاق نشاط المراجعة الداخلية إلى مجال الأمن السيبراني مما نتج عنه بطبيعة الحال تحمل المراجع الداخلي لأعباء ومسئوليات جديدة باعتباره يمثل خط الدفاع الثالث عن المنظمة ضد أي أخطار سيبرانية . ويمكن عرض تلك المسئوليات في الآتي :

- مراجعة الضوابط الرقابية .
- التحقق من توافر الالتزام بالضوابط والاشتراطات الرقابية .
- مراجعة إدارة المخاطر بالمنظمة .
- مراجعة التعديلات والتحديثات الخاصة بالأمن السيبراني بالمنظمة .
- مراجعة ردود الأفعال تجاه الانتهاكات والهجمات السيبرانية .

وفيما يلي توضيح لكل منها :

مراجعة الضوابط الرقابية :

وهنا يتعين على المراجعة الداخلية واجب تقديم مراجعة مستقلة لاستراتيجية الأمن السيبراني بالمنظمة قبل وضع السياسات والإجراءات، بالإضافة لما تقوم به من فحص ومراجعة سياسات ومعايير وإجراءات الأمن السيبراني للتأكد من مناسبتها، وفعاليتها، وملاءمتها، وترابطها، بجانب التحقق من أن الضوابط الرقابية تغطي كافة النصوص الواردة في تلك السياسات والمعايير والإجراءات، كما تقوم أيضا بالتحقق من اكتمال عمليات التوثيق وتحديثها أولاً بأول. وطبقا لما ورد بالفقرة 2130من المعيار2100من معايير المراجعة الداخلية الصادر عن معهد المراجعين الداخليين الأمريكي IIA" يجب على نشاط المراجعة الداخلية تقييم مدى كفاية وفعالية الضوابط الرقابية في التعامل مع مخاطر المنظمة المتعلقة بالحوكمة والعمليات التشغيلية وأمن

المعلومات".[15] من ناحية أخرى، يتعين على المراجعين الداخليين تنمية وتوسيع معارفهم وقدراتهم الخاصة في مجال مراجعة أمن وتكنولوجيا المعلومات ، بما يساعدهم على تقديم توصيات ذات قيمة مضافة للإدارة .

التحقق من توافر الالتزام بالضوابط والاشتراطات الرقابية :

وهنا تقوم المراجعة الداخلية بالتحقق من أن الاستثمارات في الأمن السيبراني قد تم إنفاقها بحكمة في المكان المناسب وبالمبلغ المناسب، ويتم إنفاقها للمناطق الخطرة دون غيرها، وتقديم تأكيدات للجنة المراجعة ومجلس الإدارة بأن البنية التحتية الحالية كافية لتحقيق الأمن السيبراني للمنظمة في ظل الظروف القائمة. من ناحية ثانية يقع على عاتق المراجعة الداخلية مسئولية الحصول على تأكيدات من الإدارة بشأن :

- أن أصول معلومات وبيانات المنظمة قد تم تأمينها وحمايتها .
- أن كافة الأدوات والمعدات المشتراه كمستلزمات للأمن السيبراني هي ذاتها الأدوات والمعدات المطلوبة ، وأنه يتم استخدامها بالفعل وليس إيداعها المخازن .
- أن العاملين بالمنظمة قد تم تدريبهم ، وتعليمهم ، بما فيه الكفاية فيما يتعلق بالولوج للشبكة، والخروج منها ، والاسترجاع ، باعتبار أن التعليم والتدريب في هذه الحالة يسهم بشكل مباشر في خلق الوعي لدى الجميع بأمن المعلومات وأهميته .

مراجعة إدارة المخاطر بالمنظمة :

يقع على عاتق مجلس إدارة المنظمة مسئولية إدارة المخاطر التي تواجهها على النحو الذي يتفق وطبيعة نشاطها، وحجمها ، والسوق الذي تعمل فيه. وللمنظمة حرية تأسيس إدارة مستقلة طبقا لاحتياجاتها.[16] كما تقع عليه مسئولية وضع استراتيجية لتحديد المخاطر التي قد تواجه المنظمة، وكيفية التعامل معها، ومستوى المخاطر المقبول، وكذا اعتماد الأطر التنفيذية والإجراءات والقواعد اللازمة للتعامل مع كافة أنواع المخاطر ومن بينها بطبيعة الحال المخاطر السيبرانية.[17]

تتولى إدارة المراجعة الداخلية وضع نظم لتقييم إجراءات إدارة المخاطر في المنظمة ، على أن يتم وضع تلك النظم بناء على تصور ودراسة للمخاطر التي قد تواجهها المنظمة على أن يستعان في ذلك بآراء وتقارير مجلس الإدارة ومراقبي الحسابات، ويتم أيضا تحديث ومتابعة وتقييم تلك

المخاطر بشكل دوري.[18] وفي هذا المجال يتعين على المراجع الداخلي الحصول على عينات مختلفة من مناطق الخطر، ثم دراستها دراسة شاملة مستفيضة مع إمكانية الاستعانة ببيانات من خارج المنظمة .

من ناحية أخرى ، يمكن للمراجعين الداخليين إضافة قيمة للمنظمة من خلال تقييمهم لثقافة المنظمة Culture ولإدارة مخاطر السلوك داخل المنظمة Conduct Risk والتقرير عنها.[19]

وبذلك يقع على عاتق المراجعة الداخلية مسئولية الحصول على تأكيدات بشأن :

- أن إدارة المخاطر قد تعاملت مع جميع المخاطر دون استثناء .
- أن عملية تقييم وقياس المخاطر بما فيها المخاطر السيبرانية، قد تمت طبقا للاستراتيجية المعتمدة لتحديد المخاطر وحسب الأطر التنفيذية والإجراءات والقواعد اللازمة ، سواء من حيث الأدوات أو الطرق المستخدمة .
- أن التعامل مع المخاطر تم بصورة صحيحة وشرعية طبقا لمستوى الخطر المقبول.
- أن المنظمة تملك إطاراً لإدارة خطر السلوك يتناسب ومستوى فهم العاملين فيها وكذا يرقى لمستوى تطلعات وتوقعات المنظمة.

مراجعة التعديلات والتحديثات الخاصة بالأمن السيبراني بالمنظمة :

تتسم بيئة التحول الرقمي بالتغيير السريع في نظم تكنولوجيا المعلومات، وهو مايستلزم ضرورة قيام المنظمة من وقت لآخر بإدخال تعديلات على نظم الأمن السيبراني لديها مع عمل التحديثات الضرورية للضوابط العامة لتكنولوجيا المعلومات مثل ضوابط الدخول على البنية التحتية، والتطبيقات، والبيانات .

في هذا الشأن يتولى نشاط المراجعة الداخلية مهام توصيف وتحديد أي تعديلات أو تحديثات تمت في مجال الأمن السيبراني بالمنظمة، ومن ثم يقع على عاتقها المسئوليات التالية :

- التحقق من وجود واكتمال عملية إدخال التعديلات والتحديثات بالفعل .
- التحقق من أن التعديلات أو التحديثات قد طبقت على كافة أنحاء المنظمة .
- التحقق من الالتزام بالضوابط الخاصة بأهداف ومخاطر التعديلات أو التحديثات .
- الإلمام بالتغييرات التي تنال اللوائح ذات الصلة ، والمتطلبات الجديدة ، واتجاهات الصناعة أولا بأول ، والتحقق من تضمينها كافة الخطط والبرامج داخل المنظمة .

- تقديم تأكيدات بكل ماسبق لمجلس إدارة المنظمة بمعرفة لجنة المراجعة.

مراجعة ردود الأفعال تجاه الانتهاكات والهجمات السيبرانية :

مع حدوث جريمة سيبرانية بالمنظمة، فإن الأمر يتطلب بطبيعة الحال حدوث رد فعل أو استجابة من المنظمة تجاه تداعيات تلك الجريمة، وهو مايعد بمثابة " إدارة أزمة". ويتوقف النجاح في إدارة الأزمة على شرطين هامين: الأول : سرعة اكتشاف الجريمة، والاعتراف المبكر بها. فعلى سبيل المثال، ترتب على مرور مائة يوم حتى تم اتخاذ إجراءات كرد فعل نتيجة انتهاك بيانات شركة Starwood الأمريكية، أن زادت التكلفة على الشركة بمقدار (8192) ضعفا بالمقارنة بالتكلفة الأصلية عند وقوع الجريمة.[20]

الثاني : كيفية إدارة الأزمة الناتجة عن اكتشاف الجريمة في التوقيت الملائم، وبطرق مناسبة طبقا لما هو وارد بالسياسات والمعايير والإجراءات المنصوص عليها داخل المنظمة .

في هذا الشأن يتعين على نشاط المراجعة الداخلية :

- تقييم كيفية مواجهة الإدارة للأزمة المترتبة على الانتهاك السيبراني بما ينطوي عليه من خطط وعمليات وتكاليف .
- تقييم مدى توقيت ومناسبة رد فعل الإدارة تجاه الجريمة، ومقارنة ذلك بردود الفعل الخاصة بالهجمات السيبرانية السابقة إن وجدت .
- مطابقة مدى ملاءمة الحلول الفنية المتخذة من قبل الإدارة تجاه الانتهاك بما هو وارد بالسياسات والمعايير والإجراءات الأمنية، وليس طبقا للحكم الشخصي للمراجع .
- تقديم تأكيدات بكل ماسبق لمجلس إدارة المنظمة بمعرفة لجنة المراجعة.

الهوامش

1- المؤتمر السابع للشباب (2019)، المنعقد بالعاصمة الإدارية الجديدة خلال شهر أغسطس بحضور السيد / رئيس الجمهورية .

2- المركز المصري للدراسات الاقتصادية (2019)، ندوة "على أعتاب التغيير : التجارة والتنمية في عصر المعلومات"، القاهرة، 2019/12/23 :

available at:www.eces.org.eg (accessed 7 january 2020) .

3- في مواجهة الأخطار والتهديدات الإلكترونية ظهر اصطلاح "أمن المعلومات"، و/أو "أمن نظم تكنولوجيا المعلومات"، و/ أو "الأمن السيبراني"، إلا أن المصطلح الأخير هو الأكثر استخداما على مستوى الفضاء السيبراني. لمزيد من التفاصيل، يمكن الرجوع إلى :

Kissel, R. (2013), "Xploreterms : a glossary of common cybersecurity terminology", National Initiative for Cybersecurity Careers and Studies, available at : https://niccs.us-cert.gov/glossary (accessed 3 May 2020) .

4- Kahyauglu, Sezer B.,and Caliyurt, Kiymet, (2018),"Cyber security assurance process from the internal audit perspective", Managerial Auditing Journal, Vol.33 No.4,pp 360-376 .

5- Fitzgerald, Todd j.,(2017), "Auditing cyber security :evaluating risk and auditing controls", Information Systems Audit and Control Association (ISACA), available at :http://www.isaca.org/knowledge-center/research/researchdeliverables/pages/auditing-cyber-security.aspx (accessed 15 December, 2019)

6- The IIA"s Audit Executive Center,(2017)," What the board should expect from internal audit for optimal cyber risk protection," IIA, Tone at the Top, issue 82, June, pp.1-4 .

7- Information Systems Audit and Control Association,(2017), "Cyber Security Audit", ISACA, availableathttp://www.isaca.Org / knowledge

- certer/research/cybersecurityaudit_mis_eng_2017.pdf (accessed 19 January 2020)

8- Fitzgerald , Todd J.(2017), op .cit

9- The Institute of Internal Auditors (2017), "International Standards for The Professional Practice of Internal Auditing , " IIA , North America. available at :http://www.theiia.org/standards-guidance /mandatory – guidance/pages/standards.aspx (accessed 6 september 2020) .

10- The Institute of Internal Auditors (2020), The International Professional Practice Framework (IPPF), "IT Essentials for Internal Auditors,"IIA, june, available at : http://www.theiia.org/standards. guidance/recommended-guidance/pages/newly-released-ippf-guidance -aspx (accessed16 september 2020)

11- Fitzgerald ,Todd J.(2017) , op.cit .

12- Fitzgerald , Todd J.(2017) , op.cit .

13- The Institute of Internal Auditors (2020), The International Professional Practice Framework (IPPF), "Developing A Risk–Based Internal Audet Plan, "IIA, may. Available at :http://www.theiia. org/standards-guidance/recommended-guidance / pages/developing-a-risk-based-internal-audit-plan-aspx (accessed 14September 2020).

14- Fitzgerald, Todd J.(2017) , op.cit.

15- The Institute of Internal Auditors (2017) , " International Standards for The Professional Practice of Internal Auditing , op.cit.

16- Egyptian Financial supervisory Authority, Egyptian institute of Directors, (2016), "The Egyptian Corporate Governance code", Third Release, August, Available at, www.eiod.org (accessed 12 October 2020).

17- Ibid.

18- Ibid.

19- تم تعريف "ثقافة المنظمة" طبقا لإرشادات معهد المراجعين الداخليين الأمريكي بأنها "خليط من القيم Values، والاتجاهات Attitudes، وأنماط السلوك Patterns of behavior، تشكل فيما بينها شخصية خاصة للمنظمة . بينما "إدارة خطر السلوك" تعني قياس كيفية تعامل الأفراد مع مجموعة القيم المهنية والأخلاقية والاتجاهات وأنماط السلوك السائدة داخل المنظمة . للتفاصيل يمكن الرجوع إلى:

The Institute of Internal Auditors (2020), The International Professional Practice Framework (IPPF), "Auditing Conduct Risk," IIA, JUNE. Available at :http://www.theiia.org/standaeds-guidance/recommended-gudance/practice-guides/pages/auditing-conduct-risk-aspx (accessed 2 october 2020)

20- Werthein, Steven (2019), "Auditing for Cyber Security Risk," The CPA Journal, june .available at :https://www.cpajournal.com (accessed 5 October 2020).