العنوان:	حال أمن المعلومات في المملكة العربية السعودية
المصدر:	مجلة دراسات المعلومات
الناشر:	جمعية المكتبات والمعلومات السعودية
المؤلف الرئيسي:	الغثبر، خالد بن سليمان
مؤلفين آخرين:	الصبيح، أمل ناصر(م. مشارك)
المجلد/العدد:	ع 14
محكمة:	نعم
التاريخ الميلادي:	2012
الشهر:	مايو
الصفحات:	189 - 205
رقم MD:	206878
نوع المحتوى:	بحوث ومقالات
قواعد المعلومات:	HumanIndex
مواضيع:	شبكات المعلومات، أمن المعلومات، تكنولوجيا المعلومات، السعودية، جرائم المعلومات، الحاسبات الإلكترونية، إدارة المخاطر، الوعي الأمني، الاختراقات الأمنية
رابط:	http://search.mandumah.com/Record/206878

حال أمن المعلومات في المملكة العربية السعودية

د. خالد بن سليمان الغثبر
مركز التميز لأمن المعلومات
جامعة الملك سعود

أ. أمل ناصر الصبيح
مركز التميز لأمن المعلومات
جامعة الملك سعود

الملخص:

تتسابق الجهات الحكومية والخاصة في المملكة العربية السعودية على الاستفادة من تقنية المعلومات لتقديم الخدمات الإلكترونية لتسهيل معاملات وخدمة المواطنين والعملاء، ولكن تواجه حلول تقنية المعلومات مخاطر أمنية قد تنتهي بسرقة المعلومات أو التخريب أو الاستغلال الخاطئ، فلابد من الاهتمام ببناء منظومة أمنية لحماية المعلومات والأنظمة من المخاطر المتزايدة. وخير بداية هي التشخيص السليم لحال أمن المعلومات في المملكة والتركيز على نقاط الضعف، وهذا ما نحاول توضيحه في هذه الورقة البحثية لدراسة حال تطبيق أمن المعلومات في المملكة العربية السعودية. هذا البحث هو امتداد لبحث سابق لدراسة حال تطبيق أمن المعلومات في المملكة العربية السعودية من خلال استبانة لمديري تقنية وأمن المعلومات في المنظمات السعودية خلال ورشة عمل خاصة قام بها مركز التميز لأمن المعلومات بجامعة الملك سعود في عام ٢٠١٠م. وفي هذا البحث طرح المركز الاستبانة نفسها على مديري تقنية وأمن المعلومات في المنظمات السعودية خلال ورشة عمل ثانية في عام ٢٠١١م (بعد مرور عام تقريباً). تبرز هذه الورقة البحثية أهم النتائج لاستبانة عام ٢٠١١م مع تبيين المقارنات بين الفترتين على سبيل التطور أو التأخر في بعض الجوانب الخاصة في أمن المعلومات.

١- مقدمة:

يعد تأثير تقنية المعلومات كبيراً على الاقتصاد والسياسة والثقافة، فقد أصبحت أهمية تقنية المعلومات أمرًا لا يخفى على الفرد أو المجتمع أو الحكومات أو الشركات، إن تقنية المعلومات كفيلة بزيادة إجمالي الناتج المحلي ومن ثم التوسع في القدرة الإنتاجية في قطاعات أخرى من ٥٠% إلى ٧٤% فهي تزيد من تنوع مصادر الدخل كما توفر الوظائف الجديدة ذات الرواتب العالية. فجميع هذه الفوائد الجمة المتعلقة بتقنية المعلومات جعلها تحوز على الاهتمام العالمي كقطاع هائل للاستثمار له الأولوية على غيره من القطاعات. فكثير من الدول النامية مثل الهند قد سجلت طفرة قياسية في اقتصادها خلال فترة زمنية قصيرة فقط بالاعتماد على صناعة تقنية المعلومات.

وبغض النظر عن تطورات صناعة تقنية المعلومات الحالية ومجالاتها الأكثر اتساعًا فإن هناك ما يهددها من جرائم المعلوماتية والتي تزداد تعقيدًا يومًا بعد يوم، فالعالم الرقمي المتسارع في النمو والذي يتغير ويتقلب بشكل سريع ومطرد يتعرض لمخاطر أمنية مستمرة مما ينتج عنه كثير من العواقب، وإن لم يتم علاج هذه المشكلات بالشكل الدقيق فستكون هناك معوقات كبيرة في تطبيق خدمات تقنية المعلومات، فأمن المعلومات اليوم لا يقتصر على برمجيات مكافحة الفيروسات وكلمات المرور، فالأمر يتجاوز ذلك بكثير، بالإضافة إلى ذلك فان أمن المعلومات هو جزء متمم للأمن القومي ولهذا فهناك طلب متزايد على الاستثمار في هذا المجال بدءاً من تثقيف المجتمع وتدريب المؤهلين من الأفراد وحتى بناء منتجات فاعلة وقادرة للاضطلاع بتلك المهام الحيوية.

من مراجعة المؤلفات المتعلقة بأمن المعلومات قد يبدو أن باحثي أمن المعلومات إما صبوا جل تركيزهم على الجوانب التقنية (معظم الوقت)، أو اعتمدوا نظريات وأطر من مجالات أخرى (وهو الأقل شيوعاً) مثل علم الاجتماع والفلسفة وعلم النفس والإدارة وربطها بأمن المعلومات لتوضيح الجوانب الإنسانية لمجال الأمن (٢). بعض النقاط ذات الصلة بهذا الطرح مذكورة في (٣-٧).

إن الوصول للمستوى المطلوب من أمن المعلومات يجعل من المهم معرفة وضعه القائم حاليًا. لهذا السبب يتم إجراء الاستقصاءات والدراسات. والحقيقة أن الدول النامية عانت من ندرة في الدراسات حول حالة أمن المعلومات لكن المشكلة تبدو أكثر تعقيدًا في الشرق الأوسط. فلا يوجد كثير من الذي سيستعرض تناول الوضع بالدراسة مع الإشارة للمملكة العربية السعودية حيث تناول أبو موسى التحكم في

إدارة تقنية المعلومات بالبحث (٧)، وتنفيذ (CoBIT) (٨) في حين قدم النذير إطاراً لفهم ثقافة أمن المعلومات في المملكة العربية السعودية(٩).

هذا البحث هو امتداد لبحث سابق (١) لدراسة حالة تطبيق أمن المعلومات في المملكة العربية السعودية من خلال استبانة لمديري تقنية وأمن المعلومات في المنظمات السعودية خلال ورشة عمل خاصة قام بها مركز التميز لأمن المعلومات بجامعة الملك سعود في عام ٢٠١٠م. وفي هذا البحث طرح المركز الاستبانة نفسها على مديري تقنية وأمن المعلومات في المنظمات السعودية خلال ورشة عمل ثانية في عام ٢٠١١م (بعد مرور عام تقريباً). تبرز هذه الورقة البحثية أهم النتائج لاستبانة عام ٢٠١١م مع تبيين المقارنات بين الفترتين على سبيل التطور أو التأخر في بعض الجوانب الخاصة في أمن المعلومات. تغطي هذه الدراسة الجوانب التقنية المتعلقة بأمن المعلومات وإدارة المخاطر وإدارة تأمين المعلومات. أما نتائجها فتقدم فحصاً متعمقاً لمستوى أمن المعلومات في مختلف القطاعات حالياً بحيث يمكن الاستفادة منها في تحقيق فهم أفضل لأدق تفاصيل أمن المعلومات في المملكة. كما تعتبر النتائج مفيدة لواضعي سياسات أمن المعلومات داخل المنظمات الحكومية ومنظمات القطاع الخاص. أيضًا، تتسم الدراسات العلمية التي أجريت حول أمن المعلومات بقلة العدد وخاصة ما يتعلق منها بالشرق الأوسط والمملكة العربية السعودية، لذلك تتمثل القيمة الثمينة لنتائج هذه الدراسة في تحسين فهم باحثي أمن المعلومات حول حالة هذا المجال في المنطقة عمومًا والمملكة العربية السعودية على وجه الخصوص.

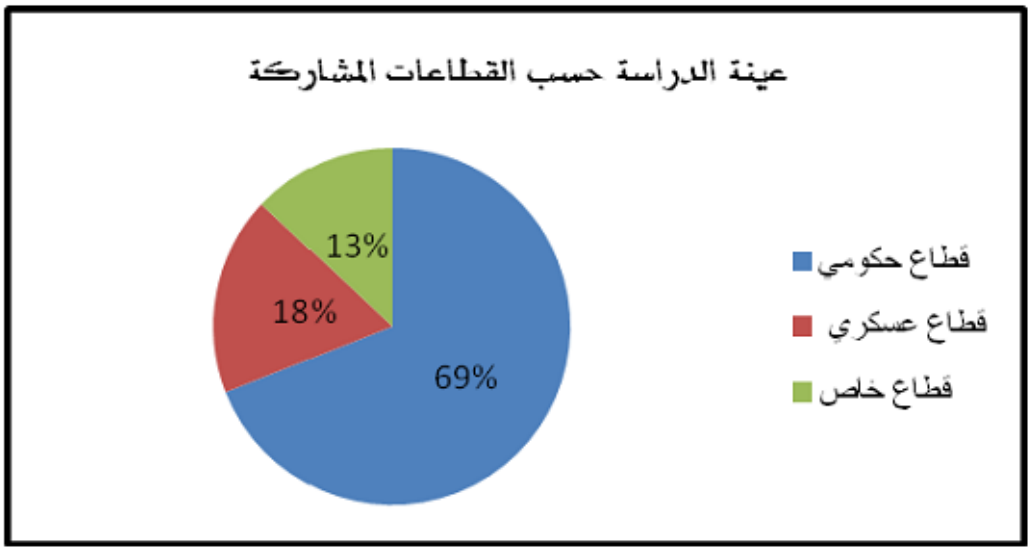
ولدراسة حالة أمن المعلومات في المنظمات السعودية سيتناول هذا البحث ما يلي: الجزء الأول سيتطرق إلى منهج البحث. يليها الجزء الثاني الذي سيستعرض بعض النتائج المختارة إلى جانب مناقشتها لتعكس حالة أمن المعلومات في المملكة العربية السعودية. وفي الجزء الأخير سيختم البحث بذكر بعض التوصيات.

٢- منهج البحث وعينة الدراسة:

منهج البحث المستخدم في الدراسة الشكل رقم (٣). وقد اتبع في غالبيته نمط الأسئلة الاختيارية إما إجابة واحدة أو عدة إجابات، وأيضًا نمط الأسئلة المفتوحة لطلب معلومات إضافية، وتدور أسئلة الاستبانة حول عدة مجالات منها سياسات أمن المعلومات ومعاييره، إدارة المخاطر، الوعي الأمني، مخاوف ومشاكل أمن المعلومات والهجمات الفعلية.

وجهت دعوة لمختلف القطاعات للمشاركة في مؤتمر لمناقشة أمن المعلومات في المنظمات السعودية شارك فيها أكثر من ١٠٠ شخص من قطاعات حكومية وعسكرية وخاصة مختلفة، وكان من بين الحضور مديرون تنفيذيون ومديرون تقنية المعلومات. وقد وزعت الاستبانة على هامش الورشة وطلب من الحضور تعبئتها وبلغ مجموع الردود السليمة ٧٩ استبانة.

وقد كانت تركيبة المشاركين تضم ٤٤% من قسم أمن المعلومات و ٥٠% من قسم تقنية المعلومات في حين أن ٦% من الإدارات الأخرى، إضافة لذلك أن ٣٧% من بين المشاركين هم مديرون في تقنية المعلومات أو أمن المعلومات. وكان المشاركون ينتمون إلى قطاعات مختلفة حيث النسبة الأعلى منهم يعملون في القطاع الحكومي غير العسكري، يليه القطاع العسكري، وأخيرا القطاع الخاص ويوضح الشكل (١) توزيع عينة الدراسة بناء على القطاعات.



الشكل رقم (١) توزيع عينة الدراسة حسب القطاعات المشاركة.

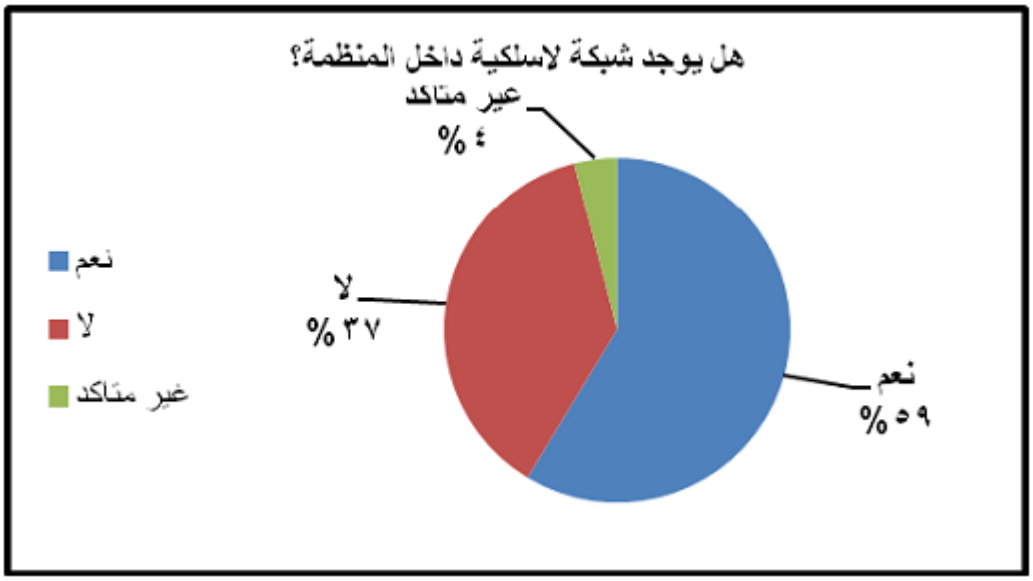
٣- النتائج والمناقشات:

في هذا الجزء سنعرض نتائج الاستبانة موزعة على سبعة أقسام وسنعقد مقارنة بين نتائج هذه الدراسة مع نتائج لدراسة سابقة أجريت العام الماضي. وعلى الرغم من شمولية الاستبانة لم يجر ذكر النتائج كافة للاختصار، بل جرى انتقاء نتائج مختارة في المجالات ذات الصلة بحيث ترسم صورة شاملة للوضع بأكمله. وتحقيقاً لهذه الغاية استخلصت النتائج من مجالات الوصول إلى الشبكة، وسياسات أمن المعلومات ومعاييره، وإدارة المخاطر، والوعي الأمني، ومخاوف ومشاكل أمن المعلومات والهجمات الفعلية.

٣,١ الوصول إلى الشبكة:

لا يخفى على الجميع فوائد الشبكات اللاسلكية في ربط كثير من الحواسيب والأجهزة المحمولة والهاتفية بطريقة مرنة وميسرة مقارنة بالشبكات السلكية، إلا أن تلك التقنيات لا تخلو من المخاطر الأمنية مثل الاختراقات والتصنت وغيرها. لذا يجب على المنظمات الحرص في تطبيق تلك الشبكات بشكل آمن ومراجعة تلك التطبيقات بشكل دوري لمنع الاختراقات والتسريبات. وقد بين نتائج الاستبانة أن ٣٧% من المنظمات لا يوجد بها شبكة لاسلكية كما يشير إليه الشكل رقم (٢)، أما بقية المنظمات التي تمتلك شبكة لاسلكية فإن ٧٤% منهم يطبق قواعد صارمة بحيث لا يستخدم الشبكة إلا موظفو المنظمة فقط.

وبالنظر إلى كل قطاع على حدة بينت النتائج الواردة في الجدول رقم (١) أن نسبة من لديه شبكة لاسلكية في القطاع الحكومي ويطبق قوانين صارمة قد انخفضت من ٩٢% في عام ٢٠١٠ إلى ٧٤% هذا العام. ونجد أيضاً أن جميع من لديه شبكة لاسلكية في القطاع العسكري والقطاع الخاص يطبق قوانين صارمة للوصول إلى الشبكة بنسبة ١٠٠% وبمقارنتها مع الدراسة السابقة التي أجريت عام ٢٠١٠م نلاحظ ارتفاع عدد المنظمات المهتمة بمنع دخول غير المصرح لهم إلى الشبكة بشكل كبير، وتعتبر هذه النتائج مؤشراً جيدًا على وعي تلك المنظمات بأهمية تأمين شبكاتهم اللاسلكية.



الشكل رقم (٢) وجود شبكة لاسلكية في المنظمات السعودية

الجدول رقم (١) التحكم في الوصول لشبكات اللاسلكية داخل المنظمات في العامين ٢٠١٠م، ٢٠١١م

نوع المنظمة	تطبيق قواعد صارمة للدخول على الشبكة اللاسلكية عام ٢٠١٠م	تطبيق قواعد صارمة للدخول على الشبكة اللاسلكية عام ٢٠١١
قطاع حكومي	%٩٢	%٧٦
قطاع عسكري	%٥٠	%١٠٠
قطاع خاص	%٦٢	%١٠٠

٣,٢ سياسات أمن المعلومات:

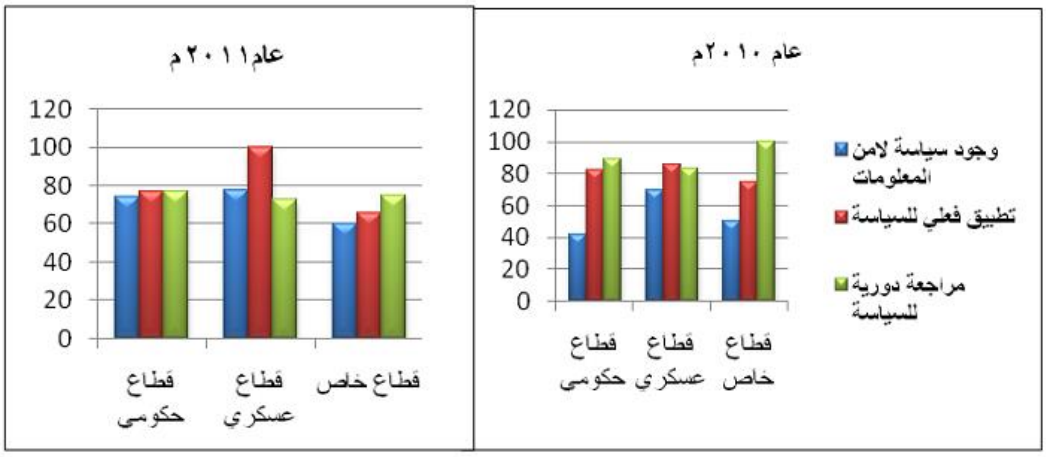
لا يمكن تأمين وحماية الأنظمة الحاسوبية بأدوات وبرمجيات فقط، فتطبيق أمن المعلومات بشكل كامل يتطلب بالإضافة إلى ذلك الاهتمام بالجانب البشري، وكذلك سن السياسات والإجراءات الأمنية للتعامل مع المعلومات وتلك المعدات والبرمجيات والمستخدمين بشكل منظم ومدروس. بمعنى أن أي إخفاق في سن تلك السياسات والإجراءات ينعكس بالسلب على أمن المعلومات في المنظمات. وقد أظهرت الدراسة ارتفاع نسبة المنظمات المهتمة بامتلاك سياسات أمن المعلومات، ففي الدراسة السابقة التي أجريت عام ٢٠١٠م كانت نسبة من يمتلك سياسة لأمن المعلومات هو نصف المنظمات المشاركة، أما في الدراسة

الحالية فقد أظهرت النتائج أن ثلاثة أرباع المنظمات المشاركة تمتلك سياسة لأمن المعلومات. إذا نظرنا إلى كل قطاع على حدة نجد أن النسبة الأعلى كانت من نصيب القطاع العسكري، حيث بلغت ٧٨%، يليها القطاع الحكومي بنسبة ٧٤%، وأخيرًا القطاع الخاص بنسبة ٦٠%.

بالنظر إلى التطبيق الفعلي للسياسة بينت النتائج للدراسة الحالية وجود انخفاض في نسبة المنظمات الذين يطبقون السياسات الأمنية للمعلومات بشكل فعلي هذا العام عنه في العام الماضي حيث بلغت نسبتهم هذا العام ٧٨% مقارنة بـ ٨٦% العام الماضي، وبالنظر إلى القطاعات المختلفة نجد أن كافة القطاعات العسكرية المشاركة و٧٧% من القطاع الحكومي و٦٦% من القطاع الخاص الذي لديه سياسات لأمن المعلومات يقوم بالفعل بتنفيذها.

وأما ما يخص مراجعة وتحديث السياسات الأمنية وجد هذا العام أن٥٥% من المنظمات مهتمة بمراجعة وتحديث السياسات الأمنية، وقد انخفضت عن العام الماضي بأكثر من الثلث تقريبا (٣٧%). وإذا نظرنا إلى القطاعات المختلفة نجد أن ٧٧% من القطاع الحكومي، و٧٣% من القطاع العسكري، و٧٥% من القطاع الخاص الذي يمتلك سياسات أمنية يقوم بمراجعتها وتحديثها بشكل مستمر.

وبشكل عام زادت عدد المنظمات التي تمتلك سياسة أمنية ولكن قل عدد من يقوم بمراجعها وتحديثها في عام ٢٠١١م عنه في ٢٠١٠م، الشكل رقم (٣)



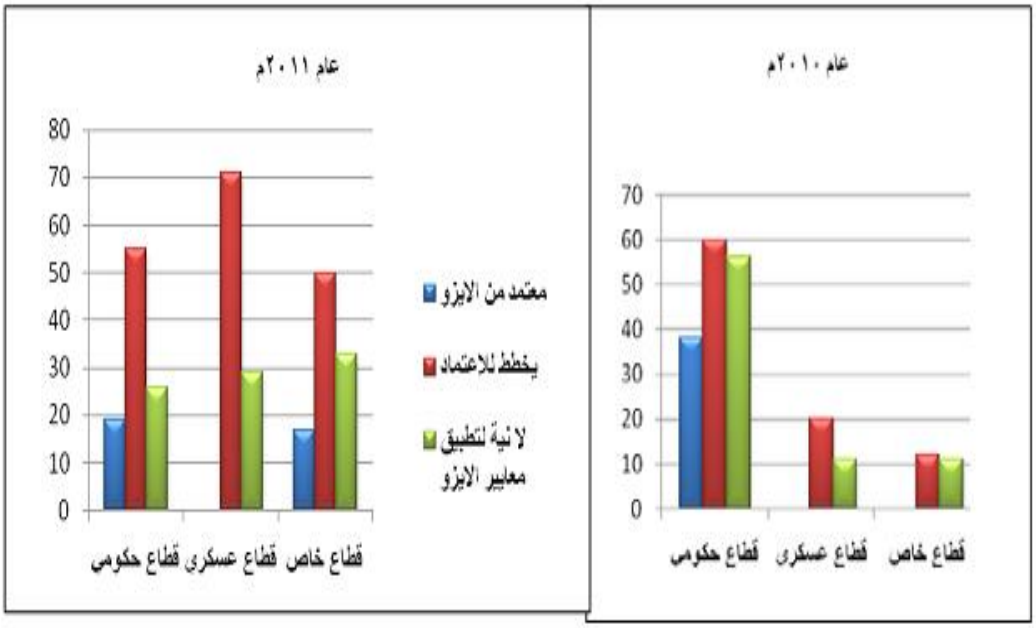
الشكل رقم (٣) وجود سياسات أمن المعلومات وتطبيقها ومراجعتها في المنظمات السعودية بين العامين ٢٠١٠م، ٢٠١١م

٣,٣ شهادات أمن المعلومات ومعاييره:

تسعى المنظمات إلى تطبيق المعايير الدولية في أمن المعلومات لعدة أغراض منها لوجود متطلبات من الشركاء أو لطمأنة العملاء أو أصحاب القرار. وهي طريقة إيجابية في تطبيق الحد الأدنى المتعارف عليه دولياً؛ لأن السعي إلى تطبيق نظام آمن وكامل هي عملية غير منتهية في عالم ملئ بالمخاطر المتجددة.

اتضح من نتائج هذه الدراسة بعد استثناء تلك المنظمات التي كانت إجاباتها "غير متأكد" أن نسبة المنظمات المعتمدة من الأيزو ٢٧٠٠١ بلغت ١٦% ضمن القطاعين الحكومي والخاص فقط، بينما لا يوجد في القطاع العسكري من هو معتمد من الايزو. وبينت نتائج الاستبانة أيضاً أن ٥٧% من المنظمات تخطط لتطبيق معايير الأيزو خلال السنة القادمة، في حين أن ٢٧% من المنظمات لا نية لها بتطبيق تلك المعايير. وهذه النتائج بدت مقاربة لنتائج العام ٢٠١٠م، حيث بلغت نسبة المنظمات المعتمدة من الايزو ١٩% ومن يفكر جديًا بتطبيق معايير الأيزو خلال السنة القادمة ٦٠%، وأخيراً كانت نسبة المنظمات التي لا نية لها بتطبيق معايير الايزو ٢١%.

وبالنظر إلى اعتماد القطاعات المختلفة لمعايير الأيزو كما يشير إليه الشكل رقم (٤) نجد أن أفضل المؤشرات جاءت في صالح القطاع الحكومي للعامين ٢٠١٠م و٢٠١١م يليه القطاع الخاص بينما لا يزال القطاع العسكري غير معتمد من الأيزو.

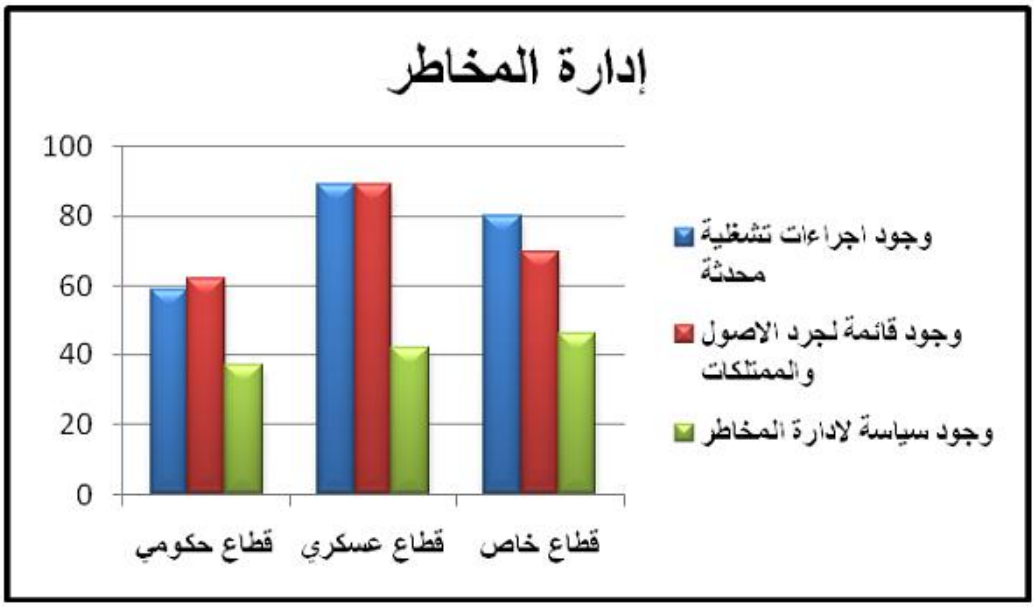


الشكل رقم (٤) حالة شهادات الأيزو ٢٧٠٠٠ في المنظمات السعودية

٣,٤ إدارة المخاطر:

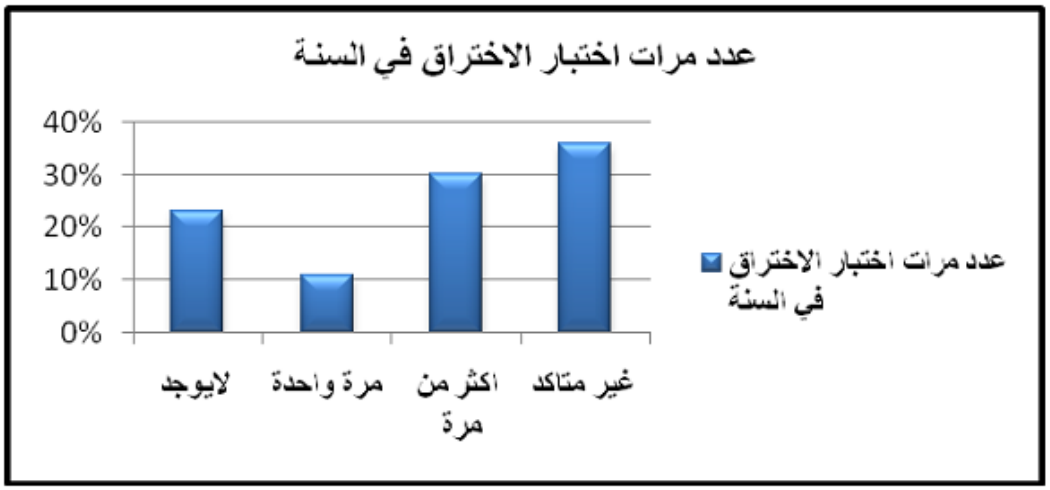
لا يمكن حماية البيضة في صندوق أمانات إلا إذا كانت من ذهب. وكذلك المعلومات والأنظمة، لابد من دراسة أهمية تلك المعلومات والأنظمة والمخاطر والتهديدات التي قد تأثر عليها قبل الشروع في تحديد نوع وتكلفة أنظمة الحماية عليها. وهذا ما يسمى بإدارة المخاطر والتعامل معها، وذلك للتركيز على المعلومات والأنظمة ذات المخاطر العالية والسبب هو أن المنظمات لا تملك الموارد المالية والبشرية والتقنية لحماية المعلومات والأنظمة كافة بالمستوى نفسه. تبين نتائج هذه الدراسة أن نحو ٤١% من المنظمات تمتلك سياسة لتقييم المخاطر، وأن ٧١% من المنظمات لديها قائمة جرد محدثة للممتلكات والأصول من برامج وأجهزة، أيضاً تمتلك ٨٣% من المنظمات إجراءات تشغيلية محدثة كالنسخ الاحتياطية ومعالجة تعطل النظام.

من الشكل رقم (٥) يعتبر القطاع العسكري من أفضل الفئات التي شملتها الدراسة في إدارة المخاطر من حيث تحديثها لقوائم جرد الأصول والممتلكات وامتلاكها إجراءات تشغيلية محدثة يليها القطاع الخاص، وأخيرًا القطاع الحكومي.



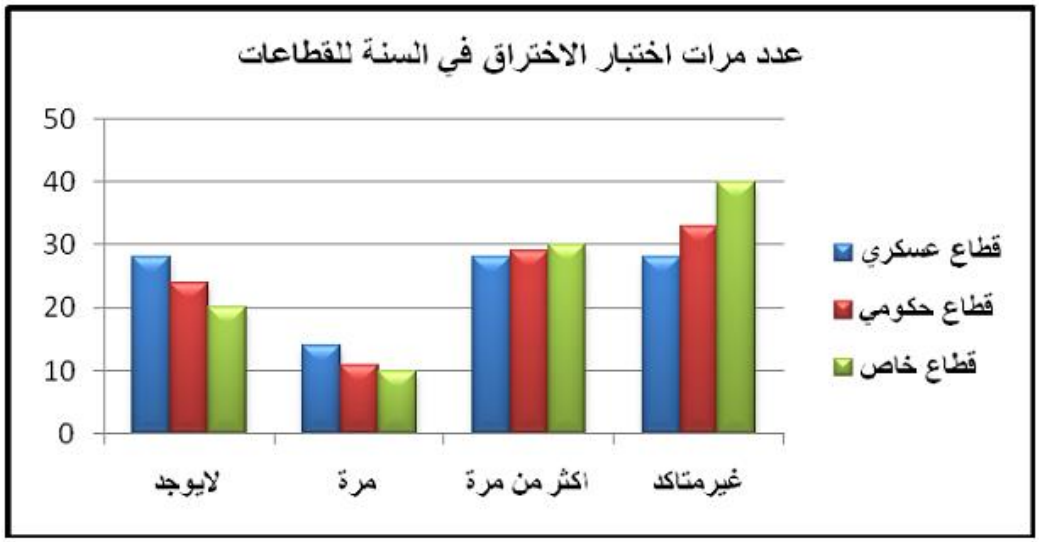
الشكل رقم (٥) حالة إدارة المخاطر في المنظمات السعودية بناءً على سياسة تقييم المخاطر وتحديث قائمة جرد الموجودات وإجراءات العمليات

أما بالنسبة لعدد المرات التي تقوم بها المنظمة لتقييم الثغرات الأمنية في شبكاتها واختبار إمكانية الاختراق فقد بينت نتائج الدراسة لعام ٢٠١١م كما يشير إليه الشكل رقم (٦) أن النسبة الكبرى والتي تعادل ٣٦% من المنظمات المشاركة غير متأكدة من عملية القيام بتقييم الثغرات في شبكاتهم تليها نسبة ٣٠% من المنظمات التي تقوم بعملية التقييم أكثر من مرة في السنة ويتراوح نسبة من يقوم بتقييم الثغرات مرة في السنة ١١% ومن لا يقوم به مطلقاً ٢٣%.



الشكل رقم (٦) عدد مرات اختبار الاختراق في المنظمات السعودية

وبالنظر إلى القطاعات المختلفة نجد أن النسب متقاربة في القيام بتقييم الثغرات الأمنية كما يشير إليه الشكل رقم (٧) وتتراوح ما بين ٢٨% إلى ٣٠% لتقييمها أكثر من مرة في السنة وما بين ١٠% إلى ١٤% لتقييمها مرة في السنة، أما عدم وجود عملية التقييم مطلقا نجد أن النسبة الكبرى كانت ٢٨% من القطاع العسكري. وبالمجمل نلاحظ تدني نسب الجهات التي تهتم بإدارة المخاطر وكذلك تقييم الثغرات الأمنية ونأمل بتحسن تلك النسب في الأعوام القليلة القادمة.



الشكل رقم (٧) عدد مرات اختبار الاختراق في كل فئة من عينة البحث

٣,٥ مخاوف ومشكلات أمن المعلومات:

يعرض الجدولان رقم (٢) (٣) أهم خمس أولويات في أمن المعلومات تهتم بها المنظمات المشاركة في الاستبانة وأشد خمس مخاوف تهدد أمن معلوماتها وقد احتلت برامج مكافحة الفيروسات أهم أولوية أمنية بينما عدم الالتزام بمعايير أمن المعلومات في المنظمة هو أشد المخاوف الأمنية السعودية.

بمقارنة أهم خمس أولويات أمن المعلومات في الدراسة الحالية مع الدراسة السابقة نجد أنها تشابهت في أربع أولويات هي وجود برامج مكافحة الفيروسات وجدار الحماية والوقاية من فقد البيانات والتحكم في الوصول للشبكة، واختلفت في عنصر واحد حيث استبدل عنصر كشف ومنع الاختراق في الدراسة السابقة بالتحقق من هوية المستخدم في الدراسة الحالية. أما بالنسبة لأشد خمس مخاوف فقد تشابهت في نقص الممارسات العملية الكافية لحماية البيانات وغياب الممارسات الجيدة في اختيار كلمة السر وعدم الالتزام بمعايير أمن المعلومات في المنظمة وظهرت مخاوف أخرى كقلة وجود العاملين المتخصصين في أمن المعلومات بالمنظمة وقلة الدعم المالي المخصص لأمن المعلومات.

الجدول رقم (٢) أهم خمس أولويات في امن المعلومات داخل المنظمات السعودية

الدرجة	أولويات أمن المعلومات
الأول	برامج مكافحة الفيروسات
الثاني	جدار الحماية
الثالث	الوقاية من فقد البيانات
الرابع	التحقق من هوية المستخدم
الخامس	التحكم في الوصول للشبكة

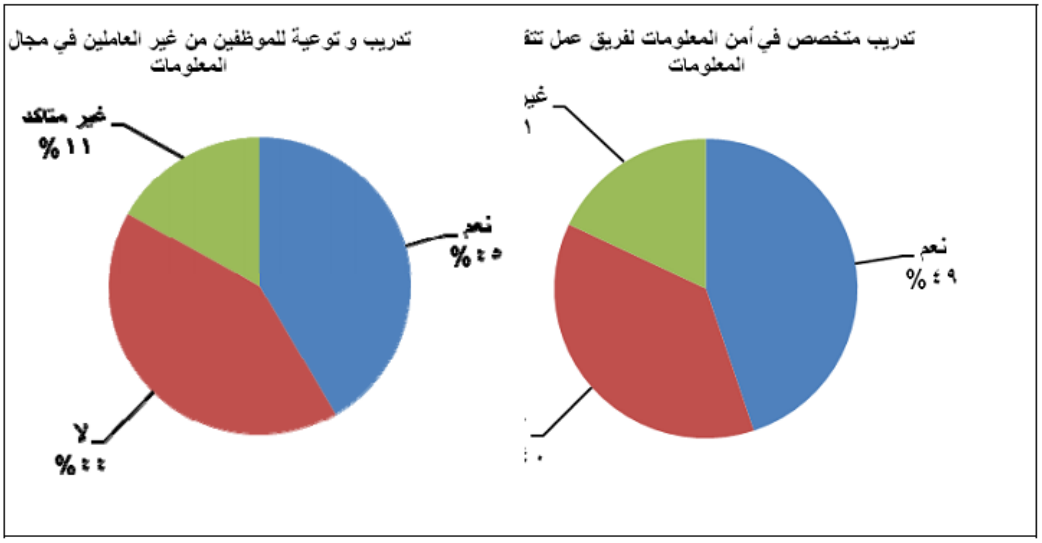
الجدول رقم (٣) أشد خمسة مخاوف في امن المعلومات داخل المنظمات السعودية

الدرجة	مخاوف أمن المعلومات
الأول	عدم الالتزام بمعايير أمن المعلومات في المنظمة
الثاني	قلة وجود العاملين المتخصصين في أمن المعلومات بالمنظمة
الثالث	نقص الممارسات العملية الكافية لحماية البيانات
الرابع	غياب الممارسات الجيدة في اختيار كلمة السر
الخامس	قلة الدعم المالي المخصص لأمن المعلومات

٣,٦ الوعي الأمني:

البشر هم الحلقة الأضعف في سلسلة أمن المعلومات، وعليه فإن من أولويات إدارات أمن المعلومات الاهتمام بتوعية وتثقيف المستخدمين للأنظمة بشكل دوري ومبتكر لتعريفهم بأهمية المعلومات والمخاطر التي تحدق بتلك المعلومات وكيفية الوقاية منها. ولكن مع الأسف هذا هو آخر ما تهتم به المنظمات للاعتقاد الخاطئ بأن أمن المعلومات يكمن في البرمجيات والمعدات فقط. وقد أظهرت النتائج الواردة في الشكل رقم (٨) أن ما يعادل نصف المنظمات المشاركة تقريبًا قدمت دورات في أمن المعلومات لموظفيها ليس في قطاع تقنية المعلومات فحسب إنما في القطاعات الأخرى المختلفة. وهذا مؤشر جيد

ويدل على حرص المنظمات السعودية لنشر الوعي الأمني بين موظفيها من خلال توفيرها لدورات تدريبية متخصصة وتوعوية أيضًا في أمن المعلومات.



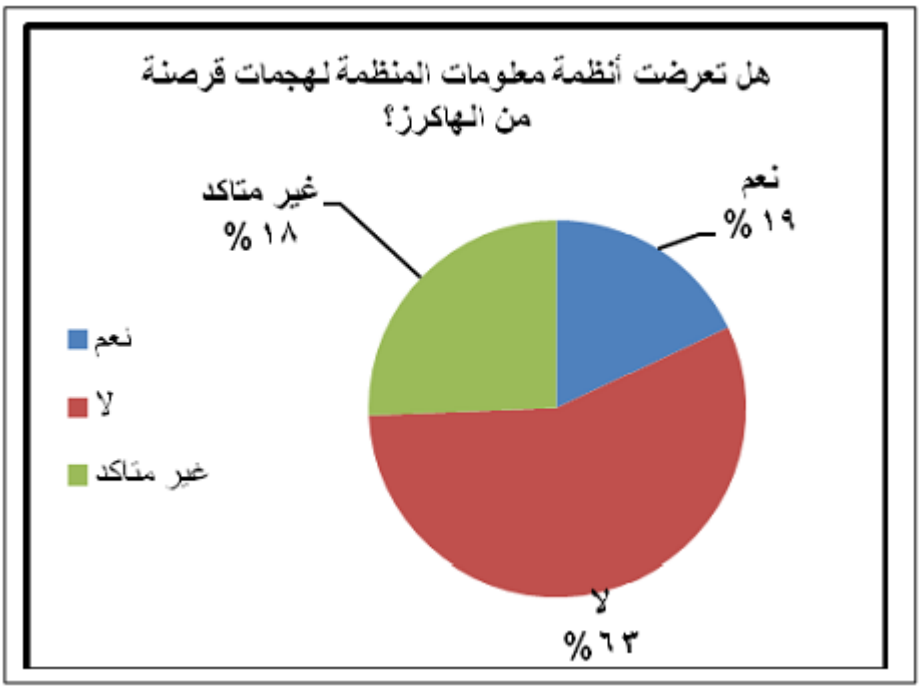
الشكل رقم (٨) التدريب المقدم للموظفين في المنظمات السعودية في أمن المعلومات

٣-٧ الاختراقات الأمنية الفعلية:

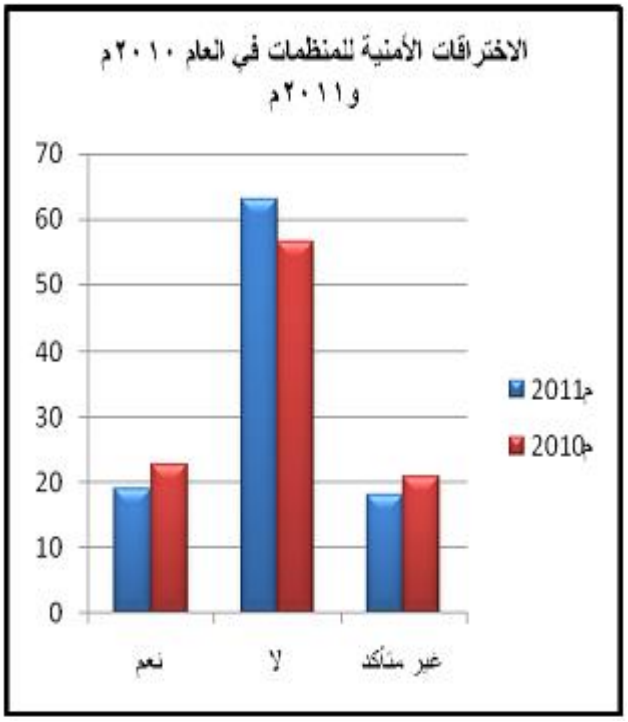
لا يخلو أكثر البرمجيات من ثغرات أمنية مكتشفة أو غير مكتشفة جراء أخطاء برمجية أو أخطاء في الإعدادات، وتستغل تلك الثغرات لاختراق تلك الأنظمة وسرقة المعلومات أو التحكم في تلك الأنظمة. وعلى المنظمات الاهتمام بكشف الثغرات بشكل دوري وسد الثغرات الأمنية في تلك البرمجيات لتفادي الاختراقات الأمنية.

بالنسبة للاختراقات الأمنية بينت نتائج الدراسة كما يشير إليه الشكل (٩) أن خمس المنظمات تقريبا تعرضت أنظمتها لهجمات القرصنة ونسبة ١٨% من المنظمات لم تكن متأكدة من تعرضها

للهجوم في حين أن نسبة ٦٣% ذكرت أن منظماتها لم تتعرض لأي هجوم. وبمقارنتها مع نتائج الدراسة السابقة نجد زيادة في نسبة المنظمات التي لم تتعرض لأي هجوم بنسبة ١١%، وانخفاض عدد من تعرض للهجوم بـ ٢٠% كما يشير إليه الشكل رقم (١٠).



الشكل رقم (٩) هجمات القرصنة الفعلية التي تعرضت لها المنظمات السعودية



الشكل رقم (١٠) مقارنة الهجمات القرصنة التي تعرضت لها المنظمات السعودية في العامين ٢٠١٠م و٢٠١١م

الخاتمة:

بشكل عام نرى ازدياد الاهتمام بأمن المعلومات بين المنظمات السعودية الحكومية والخاصة، إلا أنه دون المأمول حيث نجد ضعفًا في تطبيق معايير أمن المعلومات وكذلك إدارة المخاطر وتقييم الثغرات الأمنية. أيضًا نلاحظ ضعف في التدريب والتوعية في أمن المعلومات بالإضافة إلى ذلك نرى أهمية وجود توجه حكومي عالي المستوى لتطبيق أفضل لأمن المعلومات في المنظمات سواء الحكومية أو الخاصة التي تتعامل

مع بيانات المواطنين وذلك في عدة مجالات منها: تحديد الحد الأدنى من المعايير لتطبيق أمن المعلومات في المنظمات، دعم ميزانيات أمن المعلومات، وإيجاد برنامج وطني لتأهيل الكوادر الوطنية في أمن المعلومات.

المراجع

(1) K. Alghathbar, A .Mriza, and S. Nabi, "Information Assurance in Saudi Organizations - An Empirical Study," International Conference on Security Technology (SecTech 2010), December 13 ~ 15, 2010. Jeju Island, Korea.

(2) M. Summerfield, "Evolution of Deterrence Crime Theory," 2006. Available at http://mobile.associatedcontent.com/article/32600/evolution_of_deterrence_crime_theory.html. Last accessed May 08, 2010.

(3) D.W. Straub, "Effective IS Security: An Empirical Study," INFORMATION SYSTEMS RESEARCH, vol. 1, 1990, pp. 255-276.

(4) M.C. Stanfford and M. Warr, "A Reconceptualization of General and Specific Deterrence," Journal of Research in Crime and Delinquency, vol. 30, 1993, pp. 123-135.

(5) M. Siponen, "A conceptual foundation for organizational information security awareness," Information Management & Computer Security, vol. 8, 2000, pp. 31-41.

(6) L.N.K. Leonard, T.P. Cronan, and J. Kreie, "What influences IT ethical behavior intentions: planned behavior, reasoned action, perceived

importance, or individual characteristics?," Information and Management, vol. 42, 2004, pp. 143-158.

(7) A.A. Abu-Musa, "Exploring Information Technology Governance (ITG) in Developing Countries: An Empirical Study," International Journal of Digital Accounting Research, vol. 7, 2007, pp. 71-120.

(8) A.A. Abu-Musa, "Exploring the importance and implementation of COBIT processes in Saudi organizations: An empirical study," Information Management & Computer Security, vol. 17, 2009, pp. 73-95.

(9) M. Alnatheer and K. Nelson, "A proposed framework for understanding information security culture and practices in the Saudi context," Proceedings of the 7th Australian Information Security Management Conference, Perth, Australia: SECAU - Edith Cowan University, Australia, 2009, pp. 6-17.