أهمية العائد على الاستثمار الأمني في تقليل المخاطر

فيصل الهادي شهوب

المعهد العالي للعلوم والتقنية– غريان

Abstract:

In every public or private organization, each budget has to be justified and its effectiveness is often evaluated afterward. This valuation is named the return on investment or rate of return (ROI).This paper discussed Return on Investment measure that applies to every investment inside an organization, and also it is used as a measure of organization's performance, and it evinces that the typical approach for return on investment is not particularly for measuring security-related initiatives. Security is not mainly an investment that results in a profit, security is more about loss prevention. In other terms, when an organization investments in security, it does not expect to benefit, it expects to reduce the risks threating its assets. With this approach, the quantitative assessment of the return on security investment is done by calculating how much loss that an organization avoided to its investment. This paper has attempted to discuss some of critical points of calculating return on security investment . Especially, that the return on security on investment (ROSI) provides the basis for significant cost-benefit analysis of the risk reduction, and recently it has become a debatable topic due to growth of E-Business .Defining the value of security investments is challenging, however , it is clear that organizations will need to understand the variables that defines return on security investment. Finally, this paper clearly showed that the return on security investment can be used to convince decision-makers to invest in security to achieve a proper reasonable security level throughout organization.

الخلاصة :

في كل منظمة عامة أو خاصة اي استثمار في الميزانية يجب أن يكون له ما يبرره، وغالباً ما يتم تقييم فعالية هذا الاستثمار بعد ذلك، ويسمى هذا التقييم بالعائد على الاستثمار أو معدل العائد.ناقشت هذه الورقة العائد على الاستثمار الذي ينطبق على كل استثمار بداخل المؤسسة و يستخدم كمقياس لأداء المؤسسة، في حين أظهرت هذه الورقة أن هذا النهج النموذجي للعائد على الاستثمار لا يستخدم في قياس المبادرات المتصلة بالأمن. عموماً فالأمن ليس استثماراً يؤدي إلى الربح، لكنه يرتكز على منع الخسارة. وبعبارة أخرى عندما تستثمر مؤسسة ما في الأمن فإنها لا تتوقع ربحاً، و لكنها تتوقع أن تقلل من المخاطر التي تهدد أصولها. ومع هذا النهج يتم التقييم الكمي للعائد على الاستثمار الأمني وذلك من خلال حساب مقدار الخسارة التي سوف يتجنبها الاستثمار الخاص بالمؤسسة. وقد حاولت هذه الورقة مناقشة بعض النقاط المهمة لحساب العائد على الاستثمار الأمني. لاسيما أنه يوفر الأساس لتحليل التكاليف للحد من المخاطر، ومؤخراً أصبح هذا المقياس موضوع قابل للنقاش بسبب النمو الكبير للأعمال الإلكترونية، وكذلك صعوبة تحديد قيمة الاستثمار الأمني. ومع ذلك فإن من الواضح أن المؤسسات سوف تحتاج إلى فهم المتغيرات التي تحدد العائد على الاستثمار الأمني.وأخيراً أظهرت هذه الورقة بوضوح أن العائد على الاستثمار الأمني يمكن أن يستخدم لإقناع صانعي القرارات للاستثمار في الأمن لتحقيق نتيجة جيدة مما يجعل المستوى الأمني معقولاً في جميع أنحاء المؤسسة.

المقدمة :

أصبح الأمن في هذا الوقت من الأولويات في كل جوانب الحياة، وهذا يشمل كافة الأنشطة التجارية والحكومية، السؤال هنا كيف يمكن أن تصبح كل هذه الأنشطة والمؤسسات آمنة؟ وكيف يكون الأمن كافياً؟ وكيف تستطيع أي مؤسسة أن تعرف أنها قد وصلت إلى المستوى الأمني المقبول ؟ والأهم من ذلك ما هو المبلغ والوقت الكافي الذي يمكن أن يستثمر في مسألة الأمن؟

يمكن القول أن المسؤولين وصناع القرار بداخل المؤسسات أو الحكومات لا يهتمون ما إذا كانت التدابير الأمنية مثل الجدار الناري أو برامج مكافحة الفيروس وما الى ذلك من الوسائل والإجراءات الأمنية التي قد تحمي الخوادم والشبكات والأجهزة والموارد الخاصة بهم، لكنهم فقط يهتمون بمعرفة كم ستكلفهم قيمة هذه البرامج والمعدات والإجراءات الوقائية اللازمة لتطبيق هذه التدابير الأمنية، والأمر المهم الذي ينبغي عليهم معرفته هو كم سيكلفهم نقص الحماية على المعلومات السرية والموارد و إنتاجية مؤسساتهم إضافة على هذا كم سيكون التأثير سلبياً في حالة خرق أنظمتهم، ومن المهم أيضاً معرفة ماهي الحلول التي ستكون فعالة من حيث التكلفة وفعالية هذه الحلول فيما يخص الأداء والإنتاجية.

عند صرف مبالغ على منتجات أو خدمات أمنية، فإن صانعي القرار لدى المؤسسة يريدون معرفة أن التدابير الأمنية لها ما يبررها من الناحية المالية، وكذلك معرفة مقاييس الحماية وكمية الإنفاق عليها وما مدى التأثير الإيجابي على الإنتاجية وأداء المؤسسة، فمن غير المقبول تنفيذ إجراءات أمنية بتكلفة عالية تكون أكبر من الخطر المتوقع.

ومع التطور والتقدم والانفتاح الذي يشهده العالم اليوم، أصبحت المؤسسات وكذلك الحكومات تواجه الكثير من الصعوبات وتحيط بها الكثير من التهديدات والمخاطر المفاجئة، فكلما ازددنا تقدماً كلما ازدادت تلك المخاطر تعقيداً، بالتالي أصبحت الحماية من تلك المخاطر وتفادي الوقوع فيها مطلب أساسي يسعى الجميع لتحقيقه.

ومن أعظم المخاطر والتهديدات التي يشهدها عصرنا، هي تلك التي تهدد أمن المعلومات والحاسبات والشبكات لدى المؤسسات والحكومات.حيث تعددت هذه المخاطر وتنوعت أساليبها واختلفت دوافعها وأصبحت أي مؤسسة صغيرة كانت أم كبيرة تسعى للحفاظ على سرية المعلومات التي تملكها وسلامة أجهزتها وشبكاتها ومواردها، ولكن مع كثرة البرامج وتطورها أصبح اختراق الأجهزة والشبكات أو الحصول على المعلومات السرية أمراً يزداد سهولة في هذه الأيام.

في هذه المقالة سوف يتم مناقشة أولاً مقياس معدل الربح أو ما يعرف (بالعائد على الاستثمار)Return on Investment (ROI)ومعرفة أساسياته و كيفية حسابه وأهميته بالإضافة للعوامل التي يجب أن تؤخذ بعين الاعتبار عند حسابه، ومن ثم مناقشة نموذج حساب القيمة المالية للإنفاق على الإجراءات الأمنية (العائد الاستثماري الأمني) Return On Security Investment (ROSI)، واستعراض التقنيات اللازمة للحصول على البيانات الضرورية لهذا النموذج ملقياً بذلك الضوء على أهمية العائد الاستثماري الأمني، واتخاذ الوسائل الوقائية والدفاعية لتجنب تلك المخاطر وتقليل أضرارها، مستعرضاً بعض الأمثلة.

بداية يجب تعريف (العائد على الاستثمار) (ROI) بأنه مقياس معدل الربح والذي يشير إلى ما إذا كانت المؤسسة تستفيد من مواردها بطريقة فعالة، ويعرف أيضاً بمدى القدرة على الانتاج .[1]

وهو أيضاً مقياس الربح أو الخسارة باستثمار مؤسسة ما وغالباً ما يعبر عنه بنسبة الأرباح و ايضاً كفاءة وفعالية الاستثمارات الموجودة بداخل المؤسسة، وهو أحد أكثر النسب الربحية المستخدمة في المؤسسات وذلك بسبب مرونته.[2]

كذلك يعرف بأنه مقياس الأداء المستخدم لتقييم كفاءة الاستثمار أو لمقارنة كفاءة عدد من الاستثمارات المختلفة بداخل المؤسسة وأيضاً يقوم بحساب المبلغ العائد على الاستثمار بالنسبة لتكلفة الاستثمار نفسه.[3]

ويعرف أيضاً بأنه النسبة الربحية التي تحسب ارباح الاستثمار كنسبة مئوية من التكلفة الاصلية، ويمكن القول أنه يقيس مقدار المال الذي تم عليه الاستثمار كنسبة مئوية من سعر الشراء.[4]

وغالباً ما يشار إليه في عالم الأسواق المالية بأنه أحد أشهر المصطلحات الاقتصادية، وأكثر المقاييس المالية المستعملة في عالم المال والاستثمار، و ايضاً مقياس مالي يستخدم لقياس الربحية من ناحية استثماري معين، أو المقارنة بين عدة خيارات استثمارية. ويقوم هذا المقياس بحساب حجم العائد من استثمار معين بالمقارنة مع كلفة هذا الاستثمار.[5]

وأيضاً يبين(ROI) للمستثمرين مدى كفاءة كل مبلغ يتم استثماره في أي مشروع داخل المؤسسة لتحقيق الربح، ولا تستخدم المؤسسات هذا المقياس فقط لقياس مدى أداء الاستثمار بل يُستخدم أيضاً لمقارنة أداء الاستثمارات المختلفة بجميع أنواعها وأحجامها.ويعتبر (ROI) عاملا أساسيا يأخذ بعين الاعتبار عندما تقرر أي مؤسسة أن تستثمر في تطوير تقنية جديدة أو تطوير تقنية موجودة.إذاً يمكن مقارنة كفاءة الاستثمار لأي مورد داخل المؤسسة، حيث أن هذا المقياس يحسب الأرباح والتكاليف المرتبطة بالاستثمار.

ويتم حساب هذا المقياس(ROI)بخصم كلفة الاستثمار من القيمة النهائية للاستثمار ثم قسمة الناتج على كلفة الاستثمار، ويتم التعبير عنه بنسبة مئوية. فعلى سبيل المثال، إذا كان العائد على الاستثمار هو 0.25 فإن العائد المحقق يبلغ 25% من الاستثمار الأولي.25% = ROI

ويمكن حساب العائد على الاستثمار Return on Investmentعن طريق المعادلة التالية :

$$ROI = \frac{\text{Expected Return} - \text{Cost Of Investment}}{\text{Cost Of Investment}}$$

ومن خلال هذه الصيغة يحسب العائد على الاستثمار بطرح العائد المتوقع من تكلفة الاستثمار ومن ثم تقسيمها على تكلفة الاستثمار.وبهذه الطريقة يمكن أن يكون حساب العائد الاستثمار متنوعاً، ولكن يمكن ان يكون معقداً بأن تقوم المؤسسة بتطبيق هذا المقياس على أكثر من استثمار لديها وهذا يعتمد على رغبة المؤسسة.

ومن المهم أن ندرك أنه لا توجد معادلة موحدة لعائد الاستثمار، أي أن الفكرة الأساسية تتمثل في أن الأرباح تكون كنسبة مئوية من قيمة الدخل ويقوم هذا المقياس بإظهار حجم الربح الصافي مقارنة بحجم الكلفة الإجمالية للاستثمار، فعندما يكون الناتج فوق 0 فإنه يعني أن العائد على الاستثمار إيجابي . ما يعني أن الاستثمار يدر ربحاً على المؤسسة، ولو كان الناتج أقل من 0 فإن العائد على

الاستثمار سيكون سلبياً، وبالتالي سوف تتكبد المؤسسة الخسارة من رأس المال المستثمر.

على سبيل المثال، لو كان العائد على الاستثمار يعادل5% فهذا يعني أن العائد يفوق كلفة الاستثمار بنسبة5%، أو بصيغة أخرى فإن ربحية الاستثمار هي5%، وعلى النقيض لو كان العائد على الاستثمار يعادل5%- فإن العائد على الاستثمار سلبي وبالتالي فإن الاستثمار لم يكن مربحاً ولكن قد حقق خسارة بنسبة5%.

سنفترض أن مؤسسة ما قررت القيام باستثمار في سوق الأسهم عن طريق شراء أسهم شركة صغيرة، بالرغم من أن هذه الخطوة قد تحمل مخاطرة كبيرة إلا أن هذه المؤسسة تعتقد أن أسهم الشركة سترتفع خلال الشهور المقبلة، وبالتالي قامت هذه المؤسسة بشراء 5000 سهم بقيمة 1 دولار لكل سهم، وبعد سنة ارتفع سعر أسهم الشركة كما توقعت هذه المؤسسة ووصلت إلى سعر 3.5+ دولار للسهم، عندها باعت هذه المؤسسة الأسهم وجنت الارباح.

وبالتالي يمكن حساب العائد على عملية الاستثمار التي قامت بها المؤسسة كالتالي : ($5.000 * 12=$17.500)

$$ROI = \frac{\$17.500 - \$5.000}{\$5.000} = 2.5$$

نستنتج من ذلك أن العائد على الاستثمار الذي حققته هذه المؤسسة هو 2.5 أو 250%وهذا يعني أن عملية الاستثمار كانت ناجحة جداً .وبصيغة أخرى يمكن القول أن المؤسسة ربحت 2.5 دولار على كل 1 دولار قامت باستثماره .

ولنفترض أن مؤسسة أخرى انفقت مبلغ مقداره 1000 دولار في الشهر على الدعايات الإلكترونية، وحصلت بالتالي على 1500 دولار كقيمة عوائد المبيعات نتيجة الدعايات الإلكترونية فعند حساب العائد على الاستثمار:

العائد على الاستثمار= (إجمالي إيرادات الاستثمار– إجمالي تكاليف الاستثمار) / إجمالي تكاليف الاستثمار العائد على الاستثمار=(1500 دولار–1000 دولار)/1000 دولار = 0.50 دولار. أي أنَّ كل دولار تنفقه المؤسسة في الحملات الإعلانية أي الدعاية الإلكترونية سيحصل مقابله على نصف دولار كعائد صافي.

ونستخلص من ذلك أنه يتم حساب العائد على الاستثمار(ROI) بنفس الطريقة مهما اختلفت أنواع العمليات الاستثمارية ومهما اختلفت أنواع الأسواق المالية، ويعتبر هذا المقياس الأكثر استعمالاً لدى المستثمرين لحساب الربح المحقق .

والجدير بالذكر ان الكثير من أسهم المؤسسات أعطت عائداً يتراوح ما بين 200% و500% خلال فترة نموها، ولكن بعد ذلك انهارت أسعار أسهمها، ولذلك يجب على صناع القرار لهذه المؤسسات أن لا يتخذوا و القرارات الاستثمارية بناءً على العائد الذي تحقق في الماضي.

لهذا يمكن القول أن كل مؤسسة عامة أو خاصة يجب ان تبرر كل استثمار لديها في الميزانية، وكثيراً ما يتم تقييم الفعالية لهذا الاستثمار بعد ذلك، وبما أن مفهوم حساب العائد على الاستثمار ينطبق على كل استثمار بداخل المؤسسة، وحيث أن تطبيق التدابير الأمنية ليس استثناءً إذاً فإن صناع القرار بداخل المؤسسات يريدون معرفة تأثير الأمن على هذه الاستثمارات.ومن أجل معرفة مقدار ما ينبغي أن تنفقه المؤسسات على التدابير الأمنية، فإنها تحتاج الى معرفة ما هي الحلول الأكثر فعالية من حيث التكلفة.لذا يجب أن يتوفر مقياس خاص للتدابير الأمنية وهو ما سوف تناقشه هذه الورقة.

حساب العائد على الاستثمار الأمني(ROSI) :

يجب على هذا المقياس أن يوفر إجابات لمجموعة من التساؤلات المالية الأساسية والأمنية وهي كالتالي :

- هل ستدفع المؤسسات الكثير من أجل التدابير الأمنية ؟

- ما هو الأثر المالي على الانتاجية في حالة انعدام الامن ؟
- متى يكون الاستثمار الأمني كافياً؟
- هل هذه التدابير الأمنية في صالح المؤسسة ؟

عموماً معظم التدابير الأمنية تتمحور حول منع الخسارة وتقليل المخاطر، وبعبارة أخرى عندما تستثمر أي مؤسسة في الأمن فأنها لا تتوقع فوائد بل أنها تقلل من المخاطر التي قد تهدد مواردها وأصولها.وتقدر الأضرار المحتملة بسبب حادث يمكن أن يحدث بعدة نقاط يجب أن تأخذ بعين الاعتبار :

- نطاق الحادث المحتمل (الإدارة والمواقع التي ستتأثر).
- تكلفة شراء المعدات و المواد التي تضررت من الحادث.
- تكلفة الموظفين لمعالجة هذا الحادث.

وبشكل واضح فأن المؤسسات أصبحت أكثر اعتماداً على التكنولوجيا مما جعل الحاجة الى التدابير الأمنية الكافية أمراً في غاية الأهمية، وهناك ثلاثة متغيرات مستخدمة في حساب (ROSI)العائد على الاستثمار الأمني وهي :التعرض للمخاطر، التخفيف من المخاطر، وتكاليف الحل. وبشكل أساسي فإن هذه المدخلات عرضة للعديد من الأخطاء وذلك لأنها تتطلب الكثير من الدقة. [6]

و لتحقيق العائد على الاستثمار الأمني المطلوب تستخدم المؤسسات حالياً مفاهيم معينة مثل توقعات الخسارة المفردة (SLE) وتوقعات الخسارة السنوية (ALE) ومعدل حدوث الخطر السنوي (ARO)، وهذا يساعد على قياس الآثار المترتبة إذا فقد أو أتلف أي أصل من أصول المؤسسة.

- **منهجية العائد على الاستثمار الأمني:**

تقييم العائد على الاستثمار الأمني يتم عن طريق تقييم مقدار الخسارة الذي يمكن أن يحدث مع الاستثمار، لذلك يجب مقارنة القيمة النقدية للاستثمار مع القيمة النقدية للحد من المخاطر، ويمكن تحديد هذه القيمة من خلال التقييم الكمي للمخاطر، وبالتالي يجب على المؤسسات معرفة المفاهيم التالية :

- **تقييم الخسارة المفردة :**

هو المبلغ المتوقع من المال الذي سيتم فقده عند حدوث الخطر، وفي هذا النهج يمكن اعتبار التكلفة الإجمالية للحادث انها تحدث مرة واحد فقط، وذلك لأن طبيعة الجرائم الالكترونية سوف تؤثر على جميع الأصول بداخل المؤسسة فعلى سبيل المثال: عند سرقة كمبيوتر محمول من داخل المؤسسة لن تكون الكلفة فقط استبدال هذا الكمبيوتر، بل ستؤدي الى فقدان الانتاجية وربما فقدان الملكية الفكرية اضافة الى احتمالية فقدان معلومات حساسة خاصة بالمؤسسة، لذلك ينبغي أن تشمل التكلفة الإجمالية لهذا الحادث :

تكلفة الخسارة المباشرة مثل (تعطل الموقع، استبدال الجهاز، معالجة فقدان البيانات .. الخ) وأيضاً تكلفة الخسارة غير المباشرة مثل (الوقت المستغرق للتحقيق في الحادث، التأثير على سمعة المؤسسة..الخ)

إذاً يمكن القول أن مؤسسة ما قد تقدر قيمة الكمبيوتر المفقود بقيمة 2,000$ في حين أن مؤسسة أخرى تتعامل بمعلومات حساسة أكثر فإنها سوف تقدر هذه الخسارة ب 100,000$ وذلك لأنها سوف تؤثر مثلاً على صورتها وميزتها التنافسية بين المؤسسات الأخرى. إذاً يمكن تقييم الخسارة المفردة SLE بطرق مختلفة، بالتالي سوف يكون حساب ال ROSI مختلفاً.

- **معدل حدوث الخطر السنوي :**

هو مقياس لاحتمال حدوث الخطر في السنة وتكون البيانات هنا تقريبية، ويمكن أن تعتمد على عوامل كثيرة مثل حدوث كوارث طبيعية مثل الفيضانات وارتفاع درجات الحرارة مما سوف يؤثر على أنظمة التشغيل، وأيضاً جرائم السطو على مواقع الأصول ...الخ .

وبطبيعة الحال فإن مقياس احتمال حدوث الخطر السنوي ARO يمكن أن يساعد على تقييم تكلفة انعدام الامن، واعتماداً على التدابير الأمنية الموجودة فإن

احتمال حدوث الخطر السنوي لهجوم البرامج الخبيثة مثلاً سوف ينخفض بشكل ملحوظ في وجود برامج مكافحة الفيروس.

- **معدل الخسارة السنوي:**

هو مقياس الخسارة النقدية السنوية التي يمكن توقعها من مخاطر محددة على أصل محدد، إذاً يمكن حساب مقياس الخسارة النقدية السنوية بطرح معدل الخسارة السنوي المتوقع من تقييم الخسارة المفردة، وذلك على النحو التالي :

$$ALE = ARO * SLE$$

ولحساب مقياس العائد على الاستثمار الأمني(ROSI)، يجب تقييم المخاطر الكمية وتكلفة تنفيذ التدابير لمكافحة المخاطر، اضافة إلى ذلك المقارنة بين توقعات الخسارة السنوية مع الخسارة المتوقعة.

ومن خلال تعريف العائد على الاستثمار ROI سابقاً في هذه الورقة فإننا نقول إن (ROSI) العائد على عملية الاستثمار الأمنية وهو مقياس لتطبيق حل أمني فعال سيؤدي الى خفض توقعات الخسارة السنوية ALE، فكلما كان العائد على الاستثمار الأمني أكثر فعالية كلما قل معدل توقعات الخسارة السنوية.

$$ROSI = \frac{\text{Monetary loss reduction} - \text{Cost Of Solution}}{\text{Cost Of Solution}}$$

و يمكن تحديد هذا الانخفاض في الخسائر النقدية (Monetary loss reduction) من خلال تحديدها بفارق توقعات الخسارة السنوية دون الحل الأمني، مقابل معدل الخسارة السنوي المعدل mALE لتنفيذ التدابير الأمنية.

$$ROSI = \frac{(ALE - mALE) - \text{Cost Of Solution}}{\text{Cost Of Solution}}$$

و هذا ما يعادل أيضاً نسبة التخفيف من الحل المطبق على توقعات الخسارة السنوية ALE

$$ROSI = \frac{ALE * Mitigation\ Ration - \ Cost\ Of\ Solution}{Cost\ Of\ Solution}$$

مثال :

تدرس مؤسسة ما الاستثمار في برنامج مكافحة الفيروس، لأنها كل سنة تعاني من حوالي 5 هجمات فيروس ARO=5، وتقدر هذه المؤسسة أن كل هجوم يكلف حوالي 15,000$ فقدان للبيانات والإنتاجية 15,000$، و من المتوقع أن يقوم برنامج مكافحة الفيروسات بحظر 80% من الهجمات (نسبة التخفيف 80%)، والتكاليف السنوية تكون 15,000$، بحيث تكلف رسوم التراخيص 15,000 $ و 10,000$ رسوم تدريب وتركيب وصيانة وما إلى ذلك.

يتم حساب العائد على الاستثمار الأمنيROSI على النحو التالي وفق المعادلة السابقة:

$$ROSI = \frac{(5 * 15{,}000) * 0.8 - \ 25{,}000}{25{,}000} = 140\%$$ وفقاً

لحساب العائد على الاستثمار الأمني فإن تطبيق برنامج مكافحة الفيروس هو حل فعال من حيث التكلفة.

وعموماً فأن قياس العائد على الاستثمار الأمني أمر صعب لأنه أقرب أن يكون وثيقة أمنية، و هو يعتبر استثمار لحدث قد يحدث أو لا يحدث. من أجل ذلك يجب على مدير أمن المعلومات بداخل أي مؤسسة أن يعرف متى يستعمل هذا المقياس (ROSI). فعلى سبيل المثال: إذا تمكنت برامج مكافحة الفيروس من إيقاف عدد 10 فيروسات وعدد من البرامج الخبيثة من اختراق شبكة الحواسيب داخل مؤسسة ما، ففي هذه الحالة لا يمكن قياس العائد على الاستثمار الأمني من حيث تنفيذ المنتج.لأنه من الممكن لبرنامج مكافحة الفيروس إيقاف هذه الفيروسات أو البرامج الخبيثة، لكن يمكن أن يكون عدد منها غير ضار، لذا ينبغي حسابها على أساس المخاطر التي سوف تعالجها.[6]

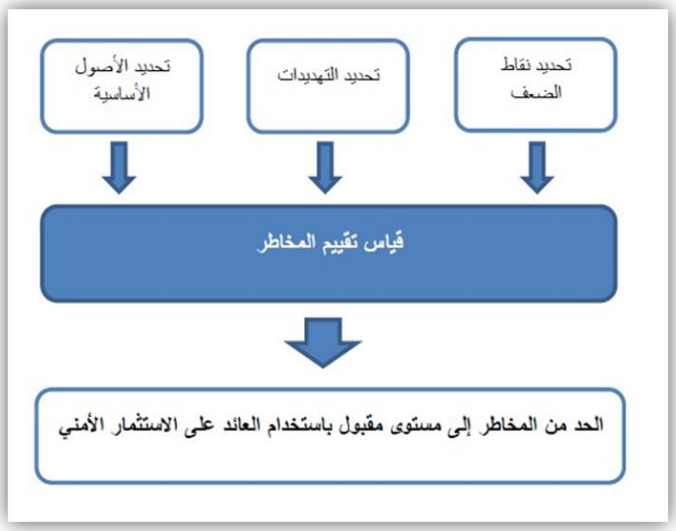
وينبغي أن تكون المخاطر النقطة المحورية عند تقييم العائد على الاستثمار الأمني، ومن أجل فهم المخاطر بشكل جيد تحتاج المؤسسة إلى تقييم و تقدير الخسارة المتوقعة، أي أن المؤسسة يمكن أن تستخدم أساليب تقييم إدارة المخاطر لديها، وبالتالي تحديد نوع من الضوابط التي قد تكون مطلوبة لمعالجة المخاطر ويمكن أن تضاف تكلفة هذه الضوابط إلى التكلفة الإجمالية للاستثمار. وهكذا فإن المؤسسة سوف تركز على المخاطر بدلاً من التركيز على المنتجات الأمنية، وأن تقدر كمية الأموال التي يتم توفيرها من الخسائر والتي قد لا تحدث أبداً[7].

ومن الصعب تقدير حوادث الجرائم الإلكترونية ومعدلات حدوثها سنوياً، ويمكن أن تكون التقريبات الناتجة عالية ومختلفة من بيئة إلى أخرى، لذلك فإن دقة البيانات الإحصائية المستخدمة في حساب (ROSI) ضرورية. ومع ذلك يصعب العثور على البيانات المهمة الخاصة بالحوادث الأمنية، نظراً لأن المؤسسات كثيراً ما تتردد في تقديم بيانات عن الحوادث الأمنية التي تحدث.[8]

أنشأت شركة Intel نموذجاً خاصاً لتحديد العائد على الاستثمار الأمني، ولقد نشرت تقريراً أوضحت فيه انها قادرة على توفير 18 مليون دولار سنوياً لتجنبها العديد من الخسائر المتوقعة . وهذا الأمر يوضح أهمية حساب (ROSI)، و قد أشارت أيضاً أن مؤسسة Intel بعد استخدامها لمقياس (ROSI) قد وفرت مستوى دقة أعلى من الوسائل الاخرى المتاحة لديها، و قد ساعد هذا المقياس على الحد من الخسائر وتحسين تخصيص الموارد وتحديد أفضل المنتجات الأمنية، وكذلك مقارنة البرامج الأمنية بالبرامج الغير أمنية وبالتالي اتخاذ القرارات المناسبة.

كما أن مؤسسة Intel تتبعت عدداً من الحوادث قبل وبعد تنفيذ التدابير الأمنية بالإضافة إلى القيمة المالية المقدرة للحادث، ومع ذلك لاحظت Intel أن البيانات القديمة للحوادث لا تعكس التغييرات التكنولوجية في المستقبل، مما يجعل هذا عيباً في نموذج ROSI، و لكنها شجعت كل موظفيها على دعم نموذج ROSI والتعرف عليه.[9]

و يوفر أيضاً موقع Security Now برامج وتطبيقات للمؤسسات لتحديد تكاليف تأمين نقاط الضعف وكذلك حساب مقياس ROSI. [10]



الشكل رقم (1)

وبناءً على الشكل رقم (1) يكمن السبب في تنفيذ التدابير الأمنية في حماية الأصول. وتعتبر الأصول أي شيء يحتوي على قيمة؛ على سبيل المثال، قواعد البيانات ،الخوادم التي تستضيف قاعدة البيانات والشبكات التي توفر الاتصال بالخادم في شركات شبكات اتصال وأيضاً الاصول الأخرى –مثل المعلومات الحساسة أو الشخصية أو السمعة.

ونقاط الضعف هي عبارة عن خلل في التدابير الامنية التي تتخذها المؤسسات لتأمين الأصول. حيث ان نقاط الضعف قد تلحق الضرر بأصول أي مؤسسة . وتتواجد في أنظمة التشغيل أو التطبيقات أو المعدات التي تستخدمها. على سبيل المثال، في حال لم تقم بتشغيل برامج مكافحة الفيروسات ومكافحة البرامج الضارة، فإن الاجهزة أو الشبكات الخاصة بالمؤسسة تكون عرضة للفيروسات. وعلى نحو مماثل، إذا لم يتم تحديث أنظمة التشغيل أو برامج التطبيق بشكل روتيني، سوف تكون المؤسسة عرضة لمشاكل البرمجيات.

وقد يكون التهديد لإيذاء أحد الأصول أو التسبب في عدم توفرها. وتعتبر أخطاء الموظفين والظواهر الطبيعية تهديدات أيضاً. وقد يتسبب هذا التهديد بتعطيل خدمة شبكة الإنترنت أو البريد الإلكتروني، أو فقدان معلومات حساسة أو الكشف غير المقصود عنها، حيث أن تحديد التهديدات أمر مهم إلا أنه جانب في غاية التعقيد.

والمخاطر يمكن أن تكون متنوعة، فقد تكون غير متوقعة وفجائية، مثل الناجمة عن الحرائق أو الناجمة عن أعطال فنية مرتبطة بأعطال قد تطال الأجهزة أو لعدم توافر الصيانة المناسبة، كما قد تكون نتيجة لعوامل إدارية تعود إلى أخطاء ونواقص مرتكبة على صعيد إدارة المؤسسة، إضافة الى مسائل مهنية ومدى كفاءة وإنتاجية وخبرة الموظفين،... وغيرها الكثير.

إذاً يمكن تعريفها على أنها عبارة عن أشياء قد تحدث أو لا تحدث في المستقبل، وقد يترتب عنها في حال حصولها آثارا على المشروع أو المؤسسة. لذا يجب أن تكون هناك عملية متواصلة من المتابعة الدقيقة والرصد والتحليل لأي مخاطر محتملة قد تنشأ، وبشكل أساسي يجب على كل مؤسسة أن تدرك أن يكون حساب العائد على الاستثمار الامني هو الهدف الأساسي لديها، عندها لن يكون هناك احتمال للخوف أو عدم اليقين والشك لدى صناع القرار، وبالعكس فإن صانعي القرار بداخل أي مؤسسة سيكونون أكثر حماساً إذا كان المشروع يضمن زيادة في الإيرادات وعلاوة على ذلك تنفيذ الحلول الأمنية تكون في وقت مبكر، والنقطة الجوهرية هي أن الانخفاض في المخاطر بالمؤسسة والتي تكون أكبر من كلفة هذه التدابير الأمنية.ولهذا فإن تقييم الاستثمارات الأمنية هي عملية أساسية ينبغي على المؤسسات المشاركة فيها، وهذا التقييم يعمل كوسيط بين القرارات المتعلقة بالتمويل وتنفيذ القرارات الأمنية .[11].

إذاً فإن العائد على الاستثمار الامني يعتبر كأداة يمكن استخدامها من قبل المتخصصين في مجال الامن (المعلومات–الشبكات.. الخ) وأيضاً يمكن لهذا المقياس أن يزود كلاً من رجال الاعمال وموظفي أمن المعلومات وصانعي القرارات

بوجهة نظر واضحة عن قيمة ومنافع أي مبادرة أمنية يُرغب في تنفيذها ، لاسيما أن الحوادث الامنية يمكن أن تفقد أي مؤسسة إنتاجيتها وبالتالي سوف تأثر على أدائها.

المراجع :

[1]http://www.businessdictionary.com/definition/return-on-investment-ROI.html .

[2]http://www.investinganswers.com/financial-dictionary/technical-analysis/return-investment-roi-1100.

[3]http://www.investopedia.com/terms/r/returnoninvestment.asp [4]http://www.myaccountingcourse.com/financial-ratios/return-on-investment .

[5]https://www.netotrade.ae/learn/trading-academy/forex-trading-basics/calculate-roi.

[6]http://www.computerweekly.com/tip/Return-on-security-investments-Measurement-guidelines.

[7]https://www.enisa.europa.eu/publications/introduction-to-return-on-security-investment/at_download/fullReport.

[8]http://www.infosecisland.com/blogview/14644-Calculating-the-Return-on-Security-Investment-ROSI.html.

[9]http://uwcisa.uwaterloo.ca/biblio2/topic/Karen_Cheng_Final_Paper__ROSI.pdf.

[10]https://www.securitynow.com .

[11]https://ai2-s2-_pdfs.s3.amazonaws.com/3f84/55ec9ee0e16a4fb50a903262bdd1c3d639d3.pdf.