أمن المعلومات و تقنيتها
أمن المعلومات، لماذا؟

د. خالد بن سليمان الغثبر*

لا يجهل كثير من مسئولي تقنية المعلومات أهمية أمن المعلومات، خاصة مع تطبيق تقنيات المعلومات المختلفة في عالم يعتمد يوماً بعد يوم عليها في حياته اليومية. كذلك لا تكاد تمر مدة قصيرة إلا و يتصدر الأخبار الرئيسية خبر انتشار فيروس حاسوبي فتّاك و كأنه فيروس بيولوجي. و لا ننسى أخبار الجرائم المعلوماتية من سرقة أسرار أو تحويل من حسابات بنكية أو إفساد معلومات أو تعطيل موقع منظمة على الانترنت أو السيطرة عليه.

يمكن القول بأن هناك ثلاثة أنماط لمديري تقنية المعلومات في القطاعين الحكومي و الخاص فيما يتعلق بتطبيق مفهوم أمن المعلومات و هم على النحو الآتي:

أولهما: مدير غير مكترث بكل هذا، و يعده إما تضخيماً للواقع الأمني المعلوماتي و استنزافا للموارد البشرية و المادية في استثمارات خاسرة لا تدر مردوداً ملموساً أو أن ذلك المدير لا يرى منظمته هدفاً لأولئك المخترقين و لا يعلم (أو يتجاهل) أن الفيروسات و بعض البرامج الخبيثة لا تفرق بين وزارة أو بنك و أن ٨٠% من المخترقين و المخربين من داخل المنظمة و ليس من خارجها.

ثانيهما: مدير متحمس جداً لأمن المعلومات و يطالب باقتناء آخر التقنيات الحديثة لمواجهة تلك الهجمات الالكترونية بدون دراسة واقعيه لوضع منظمته و أولوياتها و قد ينفق لحماية معلومات أكثر من قيمة تلك المعلومات!

ثالثهما: مدير يعي أهمية أمن المعلومات و في الوقت نفسه يعي أهداف المنظمة و توجهاتها و يحاول خلق معادله للاستفادة من مفهوم أمن المعلومات فيما يتعلق بتحقيق أهداف المنظمة، و هذا النوع هو الأمثل مع قلته.

يواجه مديري تقنية المعلومات معوقاتٌ عديدة عند الرغبة في تطبيق مفهوم أمن المعلومات في منظماتهم، لعل من أهمها إقناع الإدارة العليا و تخصيص الميزانية المطلوبة مع الطاقات البشرية المؤهلة لتطبيق مفهوم أمن المعلومات بالشكل المطلوب بلا إفراط أو تفريط كما في حالة النمطين الأولين السابقين الذكر لمديري تقنية المعلومات.

لعل ما يجهله بعض مدراء تقنية المعلومات و كثير من الإدارات العليا هو طبيعة أمن المعلومات. إن بعض تقنيات المعلومات توفر عائداً مجزياً للاستثمار بها لما تقدمه من تقليل للوقت و الجهد المطلوب لتنفيذ العمليات المختلفة. فمثلاً نظام المحاسبة يقلل الكثير من الوقت و الأخطاء و الموارد البشرية مما يعود على المنظمة بتقليل المصروفات. و كذلك يقدم المتجر الإلكتروني على الانترنت بوابة أخرى للبيع و التسويق و رافداً مالياً للمنظمة. أما أمن المعلومات فهو بالمفهوم السطحي لدى كثير من الناس مصروفات من غير عوائد مالية و لا يمكن حساب العائد على الاستثمار بشكل دقيق و عادل فيما يختص في أمن المعلومات. إن هذا المفهوم الخاطئ و المقتصر على حساب الإيرادات المباشرة المتوقعة لكل استثمار حدّ من تطبيق أمن المعلومات و سبّب الكثير من العناء لمديري تقنية أمن المعلومات لإقناع الإدارة العليا بضرورة تبني الاستثمار في أمن المعلومات.

عند النظر في مفهوم أمن المعلومات من منظور آخر يمكن القول إن لأمن المعلومات فوائد عدة، لنأخذ بعض الأمثلة:

أولاً: ما المردود المالي لنظام التكييف أو الأبواب و الأقفال؟ عندما تقتنع بتلك الأنظمة و أهميتها فأنت مقتنع بأمن المعلومات.

ثانياً: ما المردود المباشر لوزارة الدفاع في معظم الدول؟ عندما تقتنع بأهميتها فأنت مقتنع بأمن المعلومات.

ثالثاً: ما المردود المباشر للجودة؟ عندما تقتنع بأهميتها فأنت مقتنع بأمن المعلومات.

رابعاً: التقليل من المخاطر يقلل من تعرض المنظمة للخسائر المالية و المادية و كذلك يحافظ على سمعة المنظمة في السوق أو عند عملائها، و أمن المعلومات من أفضل ما يمكن الاستثمار فيه لتقليل المخاطر.

خامساً: عندما يكون مبدأ المراقبة و المحاسبة مطبقاً في المنظمة فإن المسئول يحاول قدر جهده توفير السبل المناسبة و تطبيقها لإظهار ذلك لمرؤوسيه (و محاسبيه) باهتمامه بتقليل المخاطر، و هنا يكون أمن المعلومات ضرورة ملّحه كأداة من أدوات المحافظة على حماية المعلومات و تقنياتها لخدمة المنظمة و أعمالها المتعلقة بها.

لنقف قليلاً عند بعض الإحصائيات الاقتصادية و نرى ما الأنسب في موضوع تطبيق أمن لمعلومات و تبنيه، هل تتبناه المنظمة أو لا؟

لتطبيق مفهوم أمن المعلومات بالشكل المناسب فعليك الاستثمار (مصروفات) بتقنيات متعددة(مثل أنظمة جدر حماية، مكافح الفيروسات، كاشف الاختراقات، تشفير المعلومات، التحقق من الهوية و غيرها من الأنظمة و معظمها عالية التكلفة) و كذلك عليك بالاستثمار بالكوادر البشرية المتخصصة و تدريبه على الجديد من التقنيات و كذلك المتابعة الدقيقة و الدورية لآخر المستجدات من مخاطر و تحديثات للأنظمة المطبقة في المنظمة و لا ننسى التوعية الشاملة لمنسوبي المنظمة و غيرها من المصاريف. نعم كل هذه المصاريف لا تقوم بتسريع عمل معين أو زيادة مبيعات بشكل مباشر بل بالعكس يعدّها البعض معوقات و تعقيداً لبعض الأعمال التي كانت تُنفذ بكل سهولة و يسر.

أتوقع أن النظرة السوداوية هذه تدعم النمط الأول من مدراء تقنية المعلومات و لكن لا تستعجل في القرار حتى ترى تكلفة ترك تطبيق أمن المعلومات.

هناك أكثر من ١٩,٦٠٠ عيب فني مسجل في مختلف التقنيات من عام ١٩٩٥م و حتى الربع الثاني من عام ٢٠٠٥م حسب تقرير (CERT)، وتجاوز عدد الفيروسات المعروفة حاجز ١٠٠,٠٠٠ في عام ٢٠٠٤م و هي في تزايد مطرد. يبلغ متوسط التكاليف الناجمة عن إصابة الفيروسات الحاسوبية للمنظمات الكبرى سنوياً ٦٧,٠٠٠ دولاراً أمريكيا(٢٥١,٠٠٠ريالاً سعودياً) فيما يبلغ متوسط الخسائر السنوية المسجلة لكل منظمة و الناتجة عن ضعف أمن المعلومات قرابة ١٣٠,٠٠٠,٠٠٠ دولاراً أمريكياً(٤٨٧,٥٠٠,٠٠٠ ريالاً سعودياً) حسب تقرير CSI/FBI لعام ٢٠٠٥م. يُتوقع تكلفة استعادة الأنظمة لما قبل الهجوم أو الاختراق قرابة ٢١٣,٠٠٠ دولاراً أمريكياً (٨٠٠,٠٠٠ ريالاً سعودياً) تتوزع التكلفة على الفريق التقني و تعطيل الموظفين و عمل المنظمة. كل هذه الإحصائيات و التكاليف ناجمة عن ضعف أو عدم وجود تطبيق لأمن المعلومات مع الأخذ بالاعتبار أن تلك الإحصائيات تمثل جزء يسيراً من الواقع نظراً لحساسية الموضوع و تحاشي المنظمات الإفصاح عن أي هجوم عليها لتلافي تشويه سمعتها و لا نغفل انه يصعُب تقدير الخسائر لكثير من الحالات و عدم معرفة المنظمات لبعض الهجمات فضلاً عن حصر الخسائر.

الآن و بعد معرفة تكاليف تجاهل أمن المعلومات، هل يسعك تجاهل أمن المعلومات؟ و لا تنس أن تجاهل أمن المعلومات يعرض تقنية المعلومات في المنظمة إلى خسائر كبيرة خاصاً إذا كانت أعمال المنظمة الرئيسية تعتمد عليها.

أخيرا، أتركك تراجع منظمتك، و تحسب أيهما أكثر كلفة تطبيق أمن المعلومات أم الخسائر التي قد تنجم عن الهجمات المتزايدة يومياً؟

استشاري أمن المعلومات - جامعة الملك سعود

CISSP, CISM, MCSE:Security, PMP, BS7799 LA
KSAKSU@GMAIL.COM