المملكة العربية السعودية
وزارة التعليم العالي
جامعة الملك سعود
كلية المعلمين
قسم الحاسب

Kingdom of Saudi Arabia
Ministry of Higher Education
King Saud University
Teacher's College
Computer Department

أمـن المعلومات

Information Security

المحاضرة الرابعة:.

الأحد 1430/1/1**هجري**

إعداد الأستاذ:.

عبدالله بن شائع بيهان

إدارة المخاطر Risks Management

ماهو الخطر؟

هي المشكلة التي يمكن أن تسبب فقدان بعض أو تهدد نجاح النظام ، ولكنها لم تحدث إلى الآن.

ماهي إدارة المخاطر؟

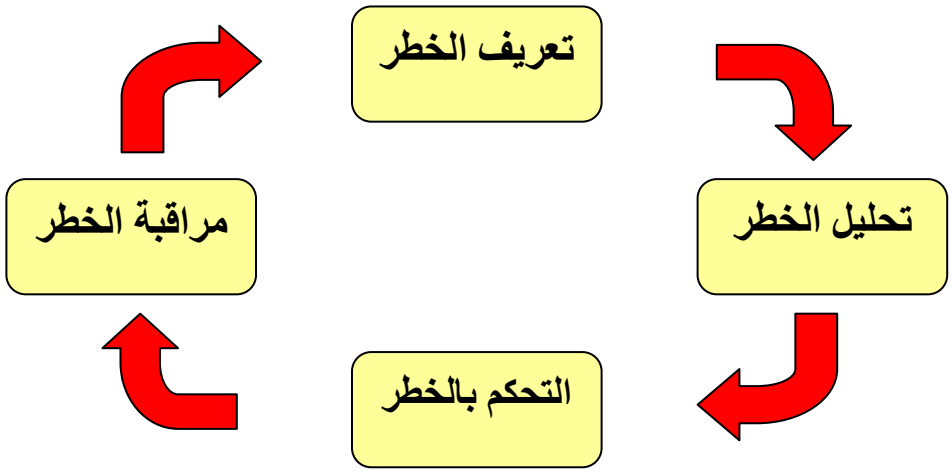
هو مجموعة من الأنشطة مع الأهداف الرئيسية لتحقيق أقصى قدر من النتائج الإيجابية للحالة وتقليل الآثار السلبية للحدث

ماهي إدارة المخاطر المعلوماتية؟

هي عملية تحديد المخاطر ، وتقييم مدى شدتها ووضع خطط لمواجهتها وذلك للوصول بالمخاطر إلى الحد المقبول وتنفيذ آليات للحفاظ على هذا المستوى .

ماهي مراحل إدارة الخطر؟

تمر إدارة الخطر بأربعة مراحل أساسية وهي:
تعريف الخطر - *تحليل الخطر* - *التحكم بالخطر* - *مراقبة الخطر*. وفيما يلي رسم توضيحي بالمراحل الأربعة.



1:تعريف الخطر :
تحديد وفهم المخاطر التي تواجه المنظمة أمر ضروري وذلك لكي نتمكن من تحديد القررات التي ستصدر عن سياسات أو أساليب تقديم الخدمات .

2: تحليل الخطر :

عندما يتم تحديد المخاطر يمكننا الأن البحث عن مسببات هذه المخاطر و عدد مرات حدوثها في فترة معينة (سنة مثلا) وشدة تأثيرها ومن ثم تحديد أفضل التقنيات للتحكم بها.

3: التحكم بالخطر:
هنا يتم التحكم بالمخاطر وذلك من خلال تطبيق عدد من الإجراءات والسياسات والتي من شأنها أن تقلل من حدوث الخطر وتبقيه في الحدود المقبولة وذلك حسب رؤية كل منظمة.

4: مراقبة الخطر:
هنا يتم مرقبة الخطر والتأكد من أن الإجراءات والسياسات المتخذة قد أدت الهدف المطلوب وفي حالة عدم تحقيقها لهدفها فإن الخطر يعاد مرة أخرى لمرحلة التعريف وهكذا حتى نصل إلى أن نحقق الحد المقبول لدى المنظمة.

لماذ نحتاج لإدارة المخاطر؟

1. تساعد على التخطيط الاستراتيجي.
2. التقليل من المفاجآت غير المتوقعة والمكلفة.
3. أكثر فعالية وكفاءة تخصيص الموارد.
4. الحصول على نتائج أفضل للمشاريع والبرامج.
5. المساعدة في تحديد الإحتياجات التأميرة بشكل واضح .
6. تزويد بمعلومات أفضل لإتخاذ القرار.
7. المساعد في مراجعة الحسابات.

ماهي أصناف المخاطر ؟
تصنف المخاطر من حيث مستوى الخطورة إلى ثلاثة أصناف وهي:
1 -مستوى منخفض (مخاطر معروفة التأثير).

2 -مستوى متوسط (مخاطر معروفة ولكن غير معروفة التأثير).
3 -مستوى عالي (مخاطر غير معروفة وغير معروفة التأثير).

ماهي أنواع الخطر؟

هناك العديد من التصنيفات للخطر ومنها على سبيل المثال لا الحصر،

1 -المخاطر المالية:
مثل الرهون العقارية ، الاستثمارات المالية في الاسواق المتذبذبة.

2 -المخاطر الصحية:
مثل الإصابة بالإعاقة أو الشلل .

3 -المخاطر البيئية:
مثل إنقراض نوع من الكائنات الحية البرية بسبب التلوثات الصناعية.

4 -المخاطر الأمنية:
مثل تسرب معلومات عسكرية حساسة بين الدول، إنتشار فايروس يعطل شبكة الإنترنت لعدد من الساعات.

5 -المخاطر التقنية:
المخاطر التي تنتج من سوء استخدامر المكونات المادية أو البرمجية والتي بدورها تؤثر على سلامة النظام في المنظمة.

6 -المخاطر البشرية:
وهي المخاطر المرتبة بالعنصر البشري كالسرقة و إنتحال الشخصية .

خطوات تحليل الخطر.

1 -إسناد قيمة لكل شئ من الممتكات (مادية مثل الأجهزة أو برمجية مثل الأنظمة والملفات) وذلك من خلال الإجابة على الأسئلة التالية أو معظمها لكل ممتلكة من ممتكلات المنظمة:

- ماهي أهمية هذه الممتلكة للمنظمة؟
- كم تكلفة صيانة هذه الممتلكة؟
- ماهي الفائدة التي تقدمها هذه الممتلكة للمنظمة؟
- ماهي تكلفة إعادة إنشاء أو إستعادة هذه الممتلكة؟
- كم هي تكلفة تطوير وتحديث هذه الممتلكة؟

2- تقدير الخسارة الفردية لمرة واحدة لكل ممتلكة
Single Loss Expectancy (SLE)
وطريقة حساب الخسارة الفردية من خلال ضرب قيمة الممتكلة بالنسبة المئوية للخسارة.
SLE = Asset Value x Exposure Factor (EF)
مثلاً يحث حريق لمكتب ، فقيمة المكتب = 10000$ ونسبة الخسارة عندما 50% علماً بأن معظم مكونات المكتب مقاومة للحريق.

إذن قيمة الممتلكة × نسبة الخسارة = 10000×0.5 = 5000$

إذن قيمة SLE=5000$.

3- تحديد عدد مرات حدوث الخطر في مدة معينة مثلا 12 شهر
Annualized Rate of Occurrence (ARO)

مثلاً يمكن أن يحدث حريق للمكتب 4 مرات في ال 12 شهر .
إذن ARO=4
قد يحصل الحريق مثلاً مرة كل سنة إذن ARO=1
قد يحصل الحريق مثلاً مرة كل عشر سنوات إذن ARO=0.1
قد يحصل الحريق مثلاً مرة كل مئة سنوات إذن ARO=0.01
وهكذا...

الخسارة السنوية للممتلكة Annualized Loss Expectancy (ALE)

ALE = SLE x Annualized Rate of Occurrence (ARO)

إذن الخسارة السنوية للمكتب المحترق = 20000$ = 4 x 5000$
ملاحظة: لكي نتمكن من حماية المكتب من الحريق يتوجب علينا شراء أداءة تحكم قيمتها تكون أقل أو تساوي 20000$ ولا تزيد عن هذا المبلغ وإلا فلا فائدة من شراء أداة التحكم لأنها أغلى من الخسارة المتوقعة.

4- تقليل أو نقل أو قبول الخطر.
لكل خطر يمكن إختيار أحد الإختيارات الثلاث:
إما تقليل الخطر:

وذلك من خلال اخذ الإحتياطات ووضع الخطط والاستراتيجيات لتقليل تأثير الخطر.

أو نقل الخطر:
وذلك من خلال التأمين بحيث تتحمل جهة أخرى الخطر مقابل مبلغ مالي.

او القبول بالخطر:
وذلك عندما لا يمكن دفع المال لمواجهة الخطر أو أنا الخطر لا يمكن مواجته فبالتالي يجب التعايش مع الخطر .

تطبيق عملي

No	Threat	Cost per Incident	Frequency of Occurrence	Cost of Control	Type of Control	ALE(Prior)	SLE	ARO	ALE(Post)	CBA	Worth the Cost
1	Programmer mistakes	$5,000	1 per month	$20,000	Training	$260,000	$5,000	12	$60,000	$180,000	yes
2	Loss of intellectual property	$75,000	1 per 2 years	$15,000	Firewall/IDS	$75,000	$75,000	0.5	$37,500	$22,500	yes
3	Software priacy	$500	1 per month	$30,000	Firewall/IDS	$26,000	$500	12	$6,000	($10,000)	no
4	Theft of information (hacker)	$2,500	1 per 6 months	$15,000	Firewall/IDS	$10,000	$2,500	2	$5,000	($10,000)	no
5	Theft of information (employee)	$5,000	1 per year	$15,000	Physical Security	$10,000	$5,000	1	$5,000	($10,000)	no
6	Web defacement	$500	1 per quarter	$10,000	Firewall	$6,000	$500	4	$2,000	($6,000)	no
7	Theft of equipment	$5,000	1 per 2 years	$15,000	Physical Security	$5,000	$5,000	0.5	$2,500	($12,500)	no
8	Viruses,Worm, Trojan horses	$1,500	1 per month	$15,000	Anti-virus	$78,000	$1,500	12	$18,000	$45,000	yes
9	Denial-of-service attacks	$2,500	1 per 6 months	$10,000	Firewall	$10,000	$2,500	2	$5,000	($5,000)	no
10	Earthquake	$250,000	1 per 20 years	$5,000	Insuance /backups	$12,500	$250,000	0.05	$12,500	($5,000)	no
11	Flood	$50,000	1 per 10 years	$10,000	Insuance /backups	$25,000	$50,000	0.1	$5,000	$10,000	yes
12	Fire	$100,000	1 per 10 years	$10,000	Insuance /backups	$50,000	$100,000	0.1	$10,000	$30,000	yes
-	Total						$497,500		$168,500		

CBA هو مؤشر يبن لنا هل الأداة التي شراءها لتقليل الخطر مجدية من الناحية الإقتصادية أم لا. وذلك من خلال المعادلة التالية:
الخسارة السنوية قبل شراء الأداة (ALE(prior – قيمة الأداةCost of Control – الخسارة السنوية بعد شراء الأداة (ALE(post.

فإذا كانت النتيجة موجبة فهذا يعني أن الاداة مناسبة. اما إذا كانت النتيجة سالبة فهذا يعني أن الأداة غير مناسبة.

The End