المحاضرة العاشرة–إدارة المخاطر السيبرانية في المؤسسات:

مقدمة:

أصبحت المؤسسات المعاصرة، بمختلف أنواعها(اقتصادية، إدارية، إعلامية، تعليمية وأمنية)، تعتمد اعتمادا شبه كلي على النظم المعلوماتية، والشبكات الرقمية، وتكنولوجيات الاتصال الحديثة في تسيير أعمالها وتحقيق أهدافها الاستراتيجية. هذا التحول الرقمي المتسارع، ورغم ما يوفره من فرص كبيرة لتحسين الأداء، رفع الإنتاجية، وتسهيل الاتصال التنظيمي، إلا أنه في المقابل أفرز جملة من المخاطر والتهديدات السيبرانية التي تمس جوهر عمل المؤسسة، واستمراريتها، وسمعتها.

من هنا تبرز أهمية إدارة المخاطر السيبرانية كمدخل استراتيجي لا يقتصر فقط على الجوانب التقنية، بل يتعداها ليشمل الأبعاد التنظيمية، الاتصالية، القانونية، والأخلاقية.

فالمخاطر السيبرانية لم تعد شأنا تقنيا محضا يخص خبراء تكنولوجيا المعلومات فقط، وإنما أصبحت قضية تنظيمية واتصالية بامتياز، تتطلب مشاركة الإدارة العليا، ومسؤولي الاتصال، والموارد البشرية، إضافة إلى المستخدمين.

تهدف هذه المحاضرة إلى تقديم رؤية أكاديمية شاملة حول إدارة المخاطر السيبرانية في المؤسسات، مع التركيز على بعدها التنظيمي والاتصالي.

أولا–الإطار المفاهيمي لإدارة المخاطر السيبرانية:

1– مفهوم المخاطر السيبرانية:

تشير المخاطر السيبرانية إلى احتمال تعرض أنظمة المعلومات، الشبكاتن البيانات، أو البنى التحتية الرقمية للمؤسسة إلى تهديدات إلكترونية قد تؤدي إلى خسائر مادية، معنوية، قانونية أو تنظيمية.

وتتمثل هذه المخاطر في:

- اختراق الأنظمة المعلوماتية.
- تسريب أو سرقة البيانات.
- تعطيل الخدمات الرقمية.
- التلاعب بالمعلومات.
- المساس بسمعة المؤسسة وثقة جمهورها.

2- مفهوم إدارة المخاطر السيبرانية:

إدارة المخاطر السيبرانية هي عملية منهجية مستمرة تهدف إلى التعرف على المخاطر الرقمية، تحليلها، تقييمها، ثم وضع استراتيجيات للتقليل من آثارها أوتفاديها، مع ضمان استمرارية نشاط المؤسسة وتحقيق أهدافها. وهي لا تقتصر على الحلول التقنية، بل تشمل:

- السياسات التنظيمية.
- الاتصال الداخلي والخارجي.
- التكوين والتوعية.
- الالتزام القانوني والأخلاقي.

3- الفرق بين الأمن السيبراني وإدارة المخاطر السيبرانية:

- الأمن السيبراني: يركز على حماية الأنظمة والشبكات من الهجمات.
- إدارة المخاطر السيبرانية: أوسع نطاقا إذ تهتم بتحديد المخاطر المحتملة، تقييم احتمالات وقوعها وتأثيراتها، ثم اتخاذ قرارات استراتيجية بشأن كيفية التعامل معها.

ثانيا-أنواع المخاطر السيبرانية في المؤسسات:

1- المخاطر التقنية: تشمل:

- ✓ البرمجيات الخبيثة.
- ✓ هجمات الفدية.
- ✓ هجمات حجب الخدمة.
- ✓ الثغرات التقنية في الأنظمة.

2- المخاطر البشرية: تعد من أخطر أنواع المخاطر، وتشمل:

- الأخطاء غير المقصودة للموظفين.
- ضعف الوعي الأمني.
- الهندسة الاجتماعية والتصيد الاحتيالي.
- إساءة استخدام الصلاحيات.

3- المخاطر التنظيمية:

- غياب سياسات أمن معلومات واضحة.
- ضعف التنسيق بين الأقسام.
- سوء الاتصال الداخلي في حالات الأزمات.
- غياب ثقافة الأمن السيبراني.

4- المخاطر القانونية:

- انتهاك قوانين حماية البيانات.
- فقدان ثقة الشركاء والعملاء.
- التعرض لعقوبات قانونية.

- تشويه صورة المؤسسة إعلاميا.

ثالثا–مراحل إدارة المخاطر السيبرانية في المؤسسات:

1– **تحديد المخاطر**: تتم هذه المرحلة عبر:

- جرد الأصول الرقمية (البيانات، الأنظمة، الشبكات).
- تحديد نقاط الضعف.
- تحليل البيئة الداخلية والخارجية.

2– تحليل المخاطر: يتم فيها:

- دراسة احتمالية وقوع الخطر.
- تقدير حجم الأثر المحتمل (مالي، تنظيمي، اتصالي).
- تحديد الفئات الأكثر تأثرا داخل المؤسسة.

3– تقييم المخاطر:

- تصنيف المخاطر حسب الأولوية.
- تحديد المخاطر المقبولة وغير المقبولة.
- دعم عملية اتخاذ القرار الإداري.

4– معالجة المخاطر: تشمل

- ✓ تجنب المخاطر.
- ✓ تقليل المخاطر.
- ✓ نقل المخاطر (التأمين مثلا)
- ✓ قبول المخاطر ضمن حدود مدروسة.

5- المتابعة والتقييم المستمر:

- مراقبة التهديدات الجديدة.
- مراجعة السياسات والإجراءات.
- تحديث خطط الاستجابة.

رابعا-دور الاتصال التنظيمي في إدارة المخاطر السيبرانية:

1- **الاتصال الداخلي:** من خلال:

- نشر ثقافة الأمن السيبراني.
- توعية الموظفين بالمخاطر.
- تحسين تدفق المعلومات أثناء الأزمات.
- تقليل الإشاعات وسوء الفهم.

2- الاتصال الخارجي: ويتجلى في:

- إدارة الاتصال مع الجمهور في حال وقوع هجوم.
- الحفاظ على سمعة المؤسسة.
- الشفافية المدروسة في الأزمات السيبرانية.

3- الاتصال في إدارة الأزمات السيبرانية: ويتمثل في:

- إعداد خطط اتصال مسبقة.
- تحديد المتحدث الرسمي.
- تنسيق الرسائل الاتصالية.

خامسا–تحديات إدارة المخاطر السيبرانية في المؤسسات:

- التطور السريع للتهديدات.
- ضعف الموارد البشرية المؤهلة.
- مقاومة التغيير التنظيمي.
- ضعف التنسيق بين البعد التقني والاتصالي.

خاتمة:

تشكل إدارة المخاطر السيبرانية اليوم ركيزة أساسية لضمان استمرارية المؤسسات وحماية رأس مالها المعلوماتي والرمزي. ومن منظور الاتصال التنظيمي، لا يمكن تحقيق فعالية هذه الإدارة دون بناء ثقافة تنظيمية قائمة على الوعي، التواصل، والمسؤولية، بما يضمن مواجهة التهديدات السيبرانية بأقل الخسائر الممكنة.