عنوان الدراسة: التخطيط الإستراتيجي لمواجهة تهديدات الإنترنت في المؤسسات الرقمية

إعداد: محمود عبد الرحمن كامل محمود معيد بقسم إدارة الأعمال بالكلية
إشراف: أ.د / فريد راغب النجار أستاذ إدارة الأعمال بالكلية
د/ أحمد عبد المنعم شفيق مدرس إدارة الأعمال بالكلية

ملخص الرسالة

هذه الرسالة دراسة ميدانية تركز بشكل أساسي علي قياس درجة تأثير تهديدات الإنترنت مثال (الاختراقات ، والبرمجيات الضارة، وهجمات عرقلة الخدمة، وسرقة واحتيال الهوية، واحتيال الإنترنت، والتجسس الصناعي، والمطاردة الإلكترونية، والتسكع الإلكتروني علي وظائف المؤسسات الرقمية الإلكترونية التي تشمل (التسويق ، الإنتاج والعمليات ، التمويل والاستثمار، والموارد البشرية) ، والتعرف علي دور التخطيط الإستراتيجي في الإستعداد لمواجهة هذه التهديدات في المؤسسات الرقمية محل الدراسة.

وقد تمثلت مشكلة الدراسة في مجموعة من التساؤلات التي تدور حول كيفية معالجة تهديدات وجرائم الإنترنت من خلال مدخل التخطيط الإستراتيجي للإستعداد لمواجهة التأثيرات السلبية لهذه التهديدات والجرائم، وقد استهدفت الدراسة قياس درجة تأثير تهديدات الإنترنت علي كل وظيفة من وظائف المؤسسات الرقمية محل الدراسة(شركات تكنولوجيا المعلومات وشركات التجارة الإلكترونية)،و التعرف علي مدي التباين بين أراء المديرين بهذه الشركات، وأيضا التباين بين أراء المديرين والخبراء حول درجة تأثير تهديدات الإنترنت علي وظائف المؤسسات الرقمية ، وأيضاً التعرف علي مدي ممارسة الشركات محل الدراسة لمدخل ومنهجية التخطيط الإستراتيجي للاستعداد لمواجهة هذه التهديدات.

وفي سبيل تحقيق ذلك بنيت الدراسة علي اختبار ثلاثة فروض رئيسة هي:

- هناك تباين بين أراء المديرين بالمؤسسات الرقمية محل الدراسة فيما يتعلق بتأثير تهديدات الإنترنت علي وظائف (التسويق ، الإنتاج والعمليات ، والتمويل والاستثمار، والموارد البشرية) .
- هناك تباين بين أراء المديرين والخبراء فيما يتعلق بتأثير تهديدات الإنترنت علي وظائف (التسويق ، الإنتاج والعمليات ، التمويل والاستثمار، الموارد البشرية) بالمؤسسات الرقمية.
- هناك تباين بين أراء المديرين بالمؤسسات الرقمية محل الدراسة فيما يتعلق بممارسة عملية التخطيط الإستراتيجي لمواجهة تهديدات الإنترنت.

وفي ضوء مشكلة الدراسة وأهدافها وفروضها تتكون الرسالة من قسمين ركز الأول علي الإطار الفكري والفلسفي للدراسة مستعرضاً أنواع تهديدات وجرائم الإنترنت وتأثيرها علي وظائف المؤسسات الرقمية بالإضافة إلي بعض تجارب الشركات والدول لمواجهة تهديدات الإنترنت فضلاً عن بعض النماذج والمداخل المطروحة لتحقيق أمن المعلومات ومن ثم المدخل المقترح (مدخل التخطيط الإستراتيجي) للإستعداد لمواجهة تهديدات الإنترنت، بينما تناول القسم الثاني الدراسة الميدانية واختبار الفروض ،فضلاً عن نتائج وتوصيات الدراسة.

ولغرض اختبار الفروض إعتمد الباحث علي البيانات الثانوية التي ساهمت في تكوين الإطار الفكري والفلسفي للدراسة ، بالإضافة إلي البيانات الأولية التي تم جمعها من خلال قائمتي إستبيان تم توجيه إحداها إلي المديرين بشركات تكنولوجيا المعلومات بالقرية الذكية بالقاهرة (٩٢ مفردة من ١٢٠ بنسبة ٧٦.٦٧%)، وشركات التجارة الإلكترونية (٦٩ مفردة من ١٠٠ بنسبة ٦٩%)، وتم توجيه الأخرى إلي مجموعة من الخبراء في مجالات علوم الحاسب والإتصالات والشبكات وأمن المعلومات (٥٠ مفردة)

وخلصت الدراسة إلي أن تأثير تهديدات الإنترنت علي وظائف المؤسسات الرقمية محل الدراسة كان تأثير منخفض وفقا لمقياس التأثير الخاص بالدراسة، كما تختلف درجات تأثير تهديدات الإنترنت علي كل وظيفة من وظائف الشركات محل الدراسة.كما أن مستويات ممارسة مجالات التخطيط الإستراتيجي لمواجهة تهديدات الإنترنت في شركات تكنولوجيا المعلومات كانت تفوق مثيلاتها في شركات التجارة الإلكترونية .

هذا وقد ثبتت صحة الفرض الأول جزئيا فيما يتعلق بوجود تباين بين أراء المديرين بالشركات محل الدراسة حول تأثير تهديدات الإنترنت علي وظيفتي التسويق والإعلان ، والتمويل والاستثمار، ولم تثبت صحة الفرض الأول جزئيا فيما يتعلق بوجود تباين بين أراء المديرين حول تأثير تهديدات الإنترنت علي وظيفتي الإنتاج والعمليات وإدارة الموارد البشرية.

كما ثبتت صحة الفرض الثاني القائل بوجود تباين بين أراء المديرين والخبراء حول تأثير تهديدات الإنترنت علي وظائف المؤسسات الرقمية.

كما ثبتت صحة الفرض الثالث القائل بأن هناك تباين بين أراء المديرين بالشركات محل الدراسة فيما يتعلق بممارسة التخطيط الإستراتيجي لمواجهة تهديدات الإنترنت.

وفي النهاية قدمت الدراسة مجموعة من التوصيات الموجهة للهيئات والأجهزة علي مستوي الدولة وأخري علي مستوي المؤسسات الرقمية والتي تعد بمثابة توجهات مستقبلية يأمل الباحث في الأخذ بها للتغلب علي تهديدات ومخاطر الإنترنت وتخفيف حدة آثارها السلبية.

كما فتحت الدراسة مجالات بحثية جديدة لاستكمال مسيرة البحث العلمي في مجالات أمن المعلومات والأعمال الإلكترونية.