

عنوان المشروع
(دراسة حالة)
سرقة بنك بنغلاديش المركزي
آثار الفشل في إدارة المخاطر أمام التهديدات السيبرانية

أسم الطالب
أحمد نور محمد عبد الشكور

مشروع تخرج- ١
كلية الإدارة- جامعة ميدأوشن

إشراف
د. منى مصطفى العشري
عضو هيئة التدريس- كلية الإدارة- جامعة ميدأوشن

جدول المحتويات

٢	١. الفصل الأول: الإطار العام للدراسة
٣	١,١. المقدمة:
٥	١,٢. مشكلة الدراسة
٥	١,٢,١. فجوات على المستوى النظري
٦	١,٢,٢. فجوات على المستوى التطبيقي
٧	١,٣. أهمية الدراسة
٧	١,٣,١. على المستوى النظري:
٨	١,٣,٢. على المستوى التطبيقي:
٩	١,٤. أسئلة الدراسة
١١	١,٥. أهداف الدراسة
١٣	١,٦. فرضيات الدراسة
١٤	١,٧. نموذج الدراسة
١٥	١,٨. منهجية الدراسة
١٧	١,٩. الدراسة الميدانية
١٨	١,١٠. مخطط المشروع المقترح
٢٠	قائمة المراجع

١. الفصل الأول: الإطار العام للدراسة

١,١ . المقدمة:

"الأمن هو عملية، وليس منتجًا." هذه الكلمات الشهيرة لبروس شناير، العارف في الأمان العالمي، توضح جوهر المشاكل التي تواجه المؤسسات المالية في زمن الرقمية. إن سرقة بنك بنجلاديش المركزي سنة ٢٠١٦ والتي تمثل واحدة من أكبر عمليات الاختيال الإلكتروني في التاريخ تكشف عن ضعف الأنظمة المالية العالمية بمواجهة التهديدات السيبرانية المتطورة. هذا الحادث سلط الضوء بشكل واضح على أهمية إدارة المخاطر بالبنوك خاصة في مجال الأمن السيبراني حيث أصبحت المؤسسات المالية سواء كانت بنوك تجارية أو مركزية هدف رئيسي للمجرمين الإلكترونيين،

في عالم يزداد فيه الاعتماد على التقنية، صار الحماية الرقمية حاجة ملحة، وليس فقط خيار. كما قال كيفين ميتنيك الهاكر المعروف الذي أصبح خبير أمني "أفضل طريقة للتوقع في المستقبل هي صنعه." وهذا ينطبق تماما على مجال الحماية الرقمية، حيث يجب أن تكون المؤسسات المالية سريعة في تطوير استراتيجيات امنية لمواكبة التهديدات المتغيرة دائماً، مع اعتبار أهمية إدارة المخاطر بشكل فعال.

إدارة المخاطر في البنك هي عمل مهم لضمان استقرارها واستمرارها. فالبنوك العادية، التي تتعامل بشكل مباشر مع الناس، تواجه عدة مخاطر مثل مخاطر الائتمان ومخاطر السوق ومخاطر العمل. مخاطر الائتمان تعني احتمال عدم قدرة الزبائن على دفع ديونهم، بينما مخاطر السوق تظهر من تغيرات أسعار الفائدة وأسعار العملات والأسهم. أما مخاطر العمل فاهي مرتبطة بفشل الأنظمة الداخلية وأخطأ البشر والكوارث الطبيعية.

لكن البنوك المركزية، التي تحمل واجب الحفاظ على ثبات النظام المالي، تواجه مخاطر زيادة تتعلق بالسياسة النقدية وأسعار الصرف. وتتضمن هذه المخاطر احتمال حدوث تضخم كبير أو هبوط قيمة العملة الوطنية أو عدم استقرار الأسواق المالية.

مع نمو التكنولوجيا المالية وظهور الخدمات البنكية عبر الإنترنت، ظهرت مخاطر جديدة تتعلق بالأمن الإلكتروني. فقد صارت البنوك عرضة للهجمات الرقمية التي تهدف لسرقة الأموال، واستهداف المعلومات الحساسة، وتعطيل العمليات البنكية. وفي هذا الصدد تبرز أهمية إدارة المخاطر في الأمن الإلكتروني كأمر هام للبنوك.

سرقة بنك بنجلاديش المركزي في ٢٠١٦، التي حصل فيها اختراق نظام سويفت للتحويلات المالية الدولية، هي مثال واضح على فشل إدارة المخاطر في الأمن السيبراني. هذه الحادثة كشفت عن نقاط ضعف خطيرة بخدمات البنك، بما فيه عدم وجود آليات كافية للحقائق من صحة المعاملات المالية وعدم وجود نظام جيد للكشف عن الاختراقات الأمنية.

هذه الدراسة ستركز على فحص دقيق لعملية سرقة المصرف، مع اهتمام خاص بتحديد نقاط الضعف في نظام الأمان الإنترنت للمصرف، وكيفية استغلالها من قبل اللصوص. كما ستبحث الدراسة في نتائج هذه السرقة على المصرف وعلى النظام المالي العالمي ككل؛ مع تسليط الضوء على دور فشل إدارة الأخطار في هذا السياق - سواء على مستوى المصرف المركزي أو البنوك التجارية التي تعمل معه.

تهدف هذه الدراسة إلى تقديم فهم كامل لعملية السرقة، واستخراج الدروس المستفادة منها وتقديم توصيات عملية لتعزيز الأمن في الإنترنت وإدارة المخاطر في المؤسسات المالية. وبهذا تستطيع المؤسسات المالية أن تأخذ خطوات مبكرة لحماية نفسها من الهجمات على الإنترنت القادمة وتحقيق الأمن المالي الدائم.

١,٢. مشكلة الدراسة

تكمن المشكلة البحثية الرئيسية في هذا البحث في تحديد العوامل التي ساهمت في فشل إدارة المخاطر في بنك بنغلاديش المركزي وكيف أدى ذلك إلى اختراق أمني كارثي. سنبحث في الأسئلة التالية:

- ما هي نقاط الضعف المحددة في أنظمة الأمن وإجراءات إدارة المخاطر التي استغلها المجرمون لتنفيذ السرقة؟
- كيف يمكن لبنك بنغلاديش أن يحسن من إدارة المخاطر وأمنه السيبراني لمنع وقوع حوادث مماثلة في المستقبل؟
- ما هي الدروس التي يمكن أن تتعلمها البنوك المركزية الأخرى من هذه الحالة لتقوية دفاعاتها ضد التهديدات السيبرانية؟

١,٢,١. فجوات على المستوى النظري

- **نقص في الأبحاث المتخصصة:** على الرغم من وجود العديد من الدراسات حول الأمن السيبراني وإدارة المخاطر في البنوك بشكل عام، إلا أن هناك نقصًا في الأبحاث التي تركز بشكل خاص على البنوك المركزية والتحديات الأمنية الفريدة التي تواجهها نظرًا لسرية إجراءات البنوك لا توجد كثير من الأبحاث أو الدراسات التي ترى وتروي ما بداخلها من إجراءات وعمليات.
- **الحاجة إلى نماذج نظرية محدثة:** النماذج النظرية الحالية لإدارة المخاطر قد لا تكون كافية للتعامل مع التهديدات السيبرانية المتطورة باستمرار. هناك حاجة إلى تطوير نماذج نظرية جديدة تأخذ في الاعتبار الطبيعة الديناميكية للتهديدات السيبرانية خصوصًا مع صعود الذكاء الاصطناعي في قمة هذه التهديدات.
- **فجوة في فهم العلاقة بين إدارة المخاطر والأمن السيبراني:** هناك حاجة إلى مزيد من البحث لفهم العلاقة المعقدة بين إدارة المخاطر والأمن السيبراني في البنوك المركزية، وكيف يمكن دمج هذين المجالين بشكل فعال.

١,٢,٢. فجوات على المستوى التطبيقي

- **نقص في الوعي الأمني:** قد يفتقر موظفو البنوك المركزية إلى الوعي الكافي بالتهديدات السيبرانية وأفضل الممارسات الأمنية. هذا يمكن أن يجعلهم عرضة للهجمات التي تعتمد على الهندسة الاجتماعية، مثل التصيد الاحتيالي.
 - **اعتماد تقنيات أمنية قديمة:** قد تعتمد بعض البنوك المركزية على تقنيات أمنية قديمة لا يمكنها مواكبة التهديدات السيبرانية المتطورة. هناك حاجة إلى اعتماد أحدث التقنيات الأمنية، مثل الذكاء الاصطناعي والتعلم الآلي، للكشف عن التهديدات والاستجابة لها بشكل استباقي.
 - **عدم كفاية إجراءات إدارة المخاطر:** قد لا تكون إجراءات إدارة المخاطر في بعض البنوك المركزية شاملة أو فعالة بما يكفي للتعامل مع مجموعة واسعة من المخاطر، بما في ذلك المخاطر السيبرانية. هناك حاجة إلى تطوير وتطبيق السياسات وإجراءات إدارة مخاطر أكثر قوة.
 - **قصور في التعاون وتبادل المعلومات:** قد يكون هناك نقص في التعاون وتبادل المعلومات بين البنوك المركزية ومؤسسات الأمن السيبراني الأخرى. يمكن أن يؤدي هذا إلى عدم كفاية المعلومات الاستخباراتية حول التهديدات، مما يجعل البنوك المركزية أكثر عرضة للهجمات.
- من خلال سد هذه الفجوات، يمكن للبنوك المركزية تعزيز أمنها السيبراني وقدرتها على الصمود في مواجهة التهديدات المتزايدة.
- ما هي العوامل التي ساهمت في فشل إدارة المخاطر في بنك بنغلاديش المركزي وكيف أدى ذلك إلى سرقة عام ٢٠١٦، وما هي الدروس المستفادة التي يمكن أن تساعد في تعزيز الأمن السيبراني وإدارة المخاطر في البنوك المركزية الأخرى؟

هذا السؤال يغطي الجوانب الرئيسية للدراسة:

- تحديد عوامل الفشل: يسعى السؤال إلى تحديد نقاط الضعف المحددة في إدارة المخاطر التي استغلها المجرمون.

- الربط بين الفشل والسرقة: يهدف السؤال إلى فهم العلاقة السببية بين فشل إدارة المخاطر ونجاح السرقة.

- استخلاص الدروس المستفادة: يهدف السؤال إلى تقديم توصيات عملية بناءً على تحليل الحالة، والتي يمكن أن تفيد البنوك المركزية الأخرى في تعزيز أمنها.

هذا السؤال البحثي يوفر إطارًا واضحًا للدراسة ويوجه البحث نحو تحقيق أهدافه.

١,٣. أهمية الدراسة

يمثل هذا البحث مساهمة قيمة في كل من المجال النظري والتطبيقي. فهو لا يقتصر على مجرد تقديم تحليل نظري، بل يوفر أيضًا رؤى عملية يمكن أن تساعد البنوك المركزية في جميع أنحاء العالم على تعزيز أمنها السيبراني وإدارة المخاطر بشكل أكثر فعالية.

١,٣,١. على المستوى النظري:

تطوير المعرفة النظرية في مجال إدارة المخاطر والأمن السيبراني: يساهم هذا البحث في إثراء المعرفة النظرية في مجال إدارة المخاطر والأمن السيبراني، خاصة في سياق البنوك المركزية. من خلال تحليل حالة سرقة بنك بنغلاديش المركزي، يمكن للباحثين تطوير نماذج نظرية جديدة وأطر عمل لفهم وتقييم وإدارة المخاطر السيبرانية بشكل أكثر فعالية.

سد الفجوات المعرفية: يهدف هذا البحث إلى سد الفجوات المعرفية الموجودة في الأدبيات الحالية حول إدارة المخاطر والأمن السيبراني في البنوك المركزية. من خلال التركيز على دراسة حالة واقعية، يمكن للبحث أن يوفر رؤى جديدة حول التحديات والفرص في هذا المجال.

تقديم إطار عمل لتحليل المخاطر السيبرانية: يمكن أن يساعد هذا البحث في تطوير إطار عمل نظري لتحليل المخاطر السيبرانية في البنوك المركزية، والذي يمكن استخدامه من قبل الباحثين والممارسين لتقييم نقاط الضعف وتطوير استراتيجيات فعالة لإدارة المخاطر.

دعم تطوير السياسات الأمنية: يمكن أن توفر نتائج هذا البحث معلومات قيمة لصانعي السياسات والجهات التنظيمية، مما يساعدهم على تطوير سياسات وإرشادات أكثر فعالية لتعزيز الأمن السيبراني في البنوك المركزية.

تعزيز التعاون البحثي: يمكن أن يشجع هذا البحث على المزيد من التعاون البحثي بين الأكاديميين والممارسين في مجال الأمن السيبراني وإدارة المخاطر، مما يؤدي إلى تطوير حلول مبتكرة للتحديات الأمنية التي تواجه البنوك المركزية.

١،٣،٢. على المستوى التطبيقي:

- **توفير دروس عملية للبنوك المركزية:** يقدم هذا البحث دروسًا عملية يمكن للبنوك المركزية الأخرى الاستفادة منها لتجنب الوقوع في الأخطاء التي أدت إلى سرقة بنك بنغلاديش. يمكن للبنوك المركزية استخدام نتائج هذا البحث لتقييم نقاط الضعف في أنظمتها الخاصة وتطوير استراتيجيات فعالة لإدارة المخاطر.
- **تعزيز الأمن السيبراني في البنوك المركزية:** من خلال تحديد نقاط الضعف في أنظمة الأمن السيبراني في بنك بنغلاديش، يمكن لهذا البحث أن يساعد البنوك المركزية الأخرى على تعزيز دفاعاتها ضد الهجمات السيبرانية.
- **تحسين إدارة المخاطر في البنوك المركزية:** يمكن أن يساعد هذا البحث البنوك المركزية على تطوير إجراءات إدارة مخاطر أكثر فعالية، من خلال تحديد أفضل الممارسات وتقديم توصيات عملية.
- **رفع مستوى الوعي الأمني:** يمكن أن يساهم هذا البحث في رفع مستوى الوعي الأمني لدى موظفي البنوك المركزية، مما يجعلهم أكثر قدرة على تحديد التهديدات السيبرانية والإبلاغ عنها.
- **تعزيز الثقة في النظام المالي:** من خلال تعزيز الأمن السيبراني وإدارة المخاطر في البنوك المركزية، يمكن لهذا البحث أن يساهم في تعزيز الثقة في النظام المالي العالمي.

١,٤ . أسئلة الدراسة

١. ما هي طبيعة التهديدات السيبرانية التي تواجهها البنوك المركزية بشكل عام، وكيف تطورت هذه التهديدات على مر الزمن؟
٢. كيف تطورت التهديدات السيبرانية التي تستهدف البنوك المركزية من حيث التعقيد والأدوات المستخدمة؟
٣. ما هي أبرز الجهات الفاعلة التي تقوم بهذه الهجمات (دول، مجموعات إجرامية، أفراد)؟
٤. ما هي الأهداف الرئيسية وراء هذه الهجمات (سرقة الأموال، تعطيل العمليات، التجسس)؟
٥. ما هي نقاط الضعف المحددة في أنظمة الأمن السيبراني وإجراءات إدارة المخاطر في بنك بنغلاديش المركزي التي سمحت بحدوث السرقة؟
٦. هل كانت هناك ثغرات في البنية التحتية التكنولوجية للبنك (مثل أنظمة البرمجيات القديمة أو غير المرخصة)؟
٧. هل كانت هناك أخطاء بشرية أو إهمال من قبل موظفي البنك؟
٨. هل كانت هناك قصور في سياسات وإجراءات إدارة المخاطر في البنك؟
٩. كيف أصبح فقدان التواصل المؤسسي ثغرة استغلها المجرمون؟
١٠. هل كانت هناك عوامل خارجية أخرى ساهمت في حدوث السرقة (مثل ضعف التعاون مع المؤسسات المالية الأخرى)؟
١١. كيف تمكن المجرمون من استغلال هذه نقاط الضعف لتنفيذ السرقة، وما هي التقنيات والأدوات التي استخدموها؟
١٢. ما هي الخطوات التي اتخذها المجرمون لاختراق نظام سويفت التابع للبنك؟
١٣. كيف تمكنوا من تحويل الأموال المسروقة إلى حسابات خارجية؟
١٤. ما هي الأدوات والتقنيات التي استخدموها للتستر على آثارهم وإعاقة التحقيقات؟
١٥. ما هي الآثار المالية والتشغيلية والسمعة التي تترتب على سرقة بنك بنغلاديش المركزي؟
١٦. ما هو حجم الخسائر المالية التي تكبدها البنك نتيجة للسرقة؟
١٧. كيف أثرت السرقة على عمليات البنك وقدرته على القيام بمهامه؟
١٨. ما هو تأثير السرقة على سمعة البنك وثقة الجمهور في النظام المالي؟

١٩. ما هي الدروس المستفادة من سرقة بنك بنغلاديش المركزي التي يمكن أن تساعد في تعزيز الأمن السيبراني وإدارة المخاطر في البنوك المركزية الأخرى؟
٢٠. ما هي أفضل الممارسات في إدارة المخاطر والأمن السيبراني التي يمكن للبنوك المركزية تبنيها؟
٢١. كيف يمكن للبنوك المركزية تحسين التعاون وتبادل المعلومات مع المؤسسات المالية الأخرى ومنظمات الأمن السيبراني؟
٢٢. ما هي الخطوات التي يمكن اتخاذها لرفع مستوى الوعي الأمني لدى موظفي البنوك المركزية؟
٢٣. ما هي التوصيات المحددة التي يمكن تقديمها لبنك بنغلاديش المركزي والبنوك المركزية الأخرى لتحسين أمنها السيبراني وإدارة المخاطر؟
٢٤. ما هي التغييرات التي يجب إجراؤها على البنية التحتية التكنولوجية للبنك؟
٢٥. ما هي السياسات والإجراءات الجديدة التي يجب تطبيقها؟
٢٦. ما هي أنواع التدريب التي يجب توفيرها للموظفين؟

من خلال الإجابة على هذه الأسئلة الفرعية بشكل شامل وعميق، يمكن للبحث أن يقدم مساهمة قيمة في فهم التحديات الأمنية التي تواجه البنوك المركزية وتطوير استراتيجيات فعالة للتصدي لهذه التحديات.

١,٥ أهداف الدراسة

١. تحليل شامل لسرقة بنك بنغلاديش المركزي:

فهم السياق: توفير فهم شامل لسياق سرقة بنك بنغلاديش المركزي، بما في ذلك الخلفية التاريخية للبنك، والبيئة التنظيمية، والإطار القانوني الذي يعمل فيه.

وصف تفصيلي للسرقة: تقديم وصف تفصيلي لعملية السرقة، بدءًا من التخطيط الأولي وحتى تنفيذها، مع تحديد الأطراف المتورطة والأدوات والتقنيات المستخدمة.

تقييم الخسائر: تحديد وتقييم الخسائر المالية وغير المالية التي تكبدها البنك نتيجة للسرقة، بما في ذلك الخسائر المباشرة وغير المباشرة، والتأثيرات على السمعة والثقة.

٢. تحديد نقاط الضعف في إدارة المخاطر والأمن السيبراني:

تحليل إجراءات إدارة المخاطر: تقييم شامل لإجراءات إدارة المخاطر في بنك بنغلاديش المركزي قبل السرقة، مع التركيز على تحديد نقاط الضعف والقصور في السياسات والإجراءات.

فحص البنية التحتية للأمن السيبراني: تحليل البنية التحتية للأمن السيبراني في البنك، بما في ذلك الأنظمة والبرمجيات والأجهزة، وتحديد نقاط الضعف والثغرات الأمنية التي تم استغلالها من قبل المجرمين.

تقييم العوامل البشرية: دراسة دور العوامل البشرية في السرقة، مثل الأخطاء البشرية والإهمال وعدم كفاية التدريب، وتقييم تأثيرها على فشل إدارة المخاطر.

٣. استخلاص الدروس المستفادة وتقديم التوصيات:

تحديد الدروس المستفادة: استخلاص الدروس المستفادة من سرقة بنك بنغلاديش المركزي، بما في ذلك أفضل الممارسات في إدارة المخاطر والأمن السيبراني، وأهمية التعاون وتبادل المعلومات، والحاجة إلى اليقظة المستمرة في مواجهة التهديدات المتطورة.

تطوير توصيات عملية: تقديم توصيات عملية لبنك بنغلاديش المركزي والبنوك المركزية الأخرى لتحسين أمنها السيبراني وإدارة المخاطر، مع التركيز على الحلول الممكنة والمناسبة للسياق المحلي لكل بنك.

اقتراح إطار عمل: اقتراح إطار عمل شامل لإدارة المخاطر والأمن السيبراني في البنوك المركزية، يمكن تطبيقه في سياقات مختلفة، مع مراعاة التحديات والفرص الفريدة التي تواجهها كل مؤسسة.

٤. المساهمة في المعرفة الأكاديمية والعملية:

إثراء الأدبيات الأكاديمية: المساهمة في الأدبيات الأكاديمية حول إدارة المخاطر والأمن السيبراني في البنوك المركزية، من خلال تقديم دراسة حالة مفصلة وتحليل متعمق.

توفير مرجع للممارسين: توفير مرجع للممارسين في البنوك المركزية والمؤسسات المالية الأخرى، لمساعدتهم على فهم التهديدات السيبرانية وتطوير استراتيجيات فعالة لإدارة المخاطر.

رفع مستوى الوعي: رفع مستوى الوعي بأهمية الأمن السيبراني وإدارة المخاطر في البنوك المركزية، من خلال نشر نتائج البحث في المؤتمرات والندوات ووسائل الإعلام المتخصصة.

من خلال تحقيق هذه الأهداف، ستساهم هذه الدراسة في تعزيز فهمنا للتحديات الأمنية التي تواجه البنوك المركزية، وتقديم حلول عملية لتعزيز أمنها السيبراني وإدارة المخاطر بشكل أكثر فعالية.

١,٦. فرضيات الدراسة

فشل إدارة المخاطر كان العامل الرئيسي الذي أدى إلى سرقة بنك بنغلاديش المركزي عام ٢٠١٦.

الفرضيات الفرعية:

نقاط الضعف في البنية التحتية التكنولوجية:

- كانت البنية التحتية التكنولوجية لبنك بنغلاديش المركزي غير كافية للتصدي للتهديدات السيبرانية المتقدمة.

- لم يتم تحديث أنظمة البنك بشكل منتظم، مما جعلها عرضة للاختراق.

- لم يتم تطبيق تدابير أمنية كافية لحماية شبكة البنك وأنظمة الدفع.

قصور في إجراءات إدارة المخاطر:

- لم تكن إجراءات إدارة المخاطر في بنك بنغلاديش شاملة أو فعالة بما يكفي لتحديد وتقييم والتصدي للمخاطر السيبرانية.

- لم يكن لدى البنك خطة استجابة للحوادث محددة بوضوح أو تم اختبارها بشكل كافٍ.

- لم يتم تخصيص موارد كافية لإدارة المخاطر والأمن السيبراني.

- عدم وجود ميزانية للتدريب.

العوامل البشرية:

- لعبت الأخطاء البشرية والإهمال دورًا كبيرًا في نجاح السرقة.

- لم يكن موظفو البنك على دراية كافية بالتهديدات السيبرانية أو كيفية التعامل معها.

- لم يتم تدريب الموظفين بشكل كافٍ على إجراءات الأمن السيبراني وإدارة المخاطر.

العوامل الخارجية:

- ساهم ضعف التعاون وتبادل المعلومات مع المؤسسات المالية الأخرى في نجاح السرقة.

- ساهمت البيئة التنظيمية والقانونية في بنغلاديش في زيادة التعرض للمخاطر السيبرانية.

١,٧. نموذج الدراسة

في دراسة حالة سرقة بنك بنغلاديش المركزي، يمكن استخدام نموذج دراسة الحالة كمنهجية بحثية. يعتبر نموذج دراسة الحالة مناسباً بشكل خاص لهذا البحث للأسباب التالية:

التعمق في التفاصيل: يتيح نموذج دراسة الحالة التعمق في تفاصيل حدث معين (في هذه الحالة، سرقة البنك) وتحليل العوامل المختلفة التي ساهمت في حدوثه. يمكن للباحث جمع بيانات مفصلة من مصادر متعددة، مثل التقارير الرسمية، والمقالات الإخبارية، والمقابلات مع الأشخاص المعنيين، وتحليل هذه البيانات لتكوين فهم شامل للحدث.

التركيز على السياق: يركز نموذج دراسة الحالة على فهم الحدث في سياقه الخاص. في حالة سرقة بنك بنغلاديش، يمكن للباحث دراسة السياق التنظيمي والقانوني والسياسي الذي حدثت فيه السرقة، وكيف يمكن أن يكون هذا السياق قد ساهم في حدوثها.

استخلاص الدروس المستفادة: يهدف نموذج دراسة الحالة إلى استخلاص الدروس المستفادة من الحدث المدروس. في حالة سرقة بنك بنغلاديش، يمكن للباحث تحديد نقاط الضعف في إدارة المخاطر والأمن السيبراني التي أدت إلى السرقة، واقتراح توصيات عملية لمنع حدوث مثل هذه الحوادث في المستقبل. تطبيق النتائج على حالات أخرى: يمكن تعميم نتائج دراسة الحالة على حالات أخرى مماثلة. على سبيل المثال، يمكن تطبيق الدروس المستفادة من سرقة بنك بنغلاديش على بنوك مركزية أخرى لتحسين أمنها السيبراني وإدارة المخاطر.

خطوات تطبيق نموذج دراسة الحالة:

- **تحديد الحالة:** تحديد حالة سرقة بنك بنغلاديش المركزي كحالة الدراسة.
- **جمع البيانات:** جمع بيانات مفصلة حول السرقة من مصادر متعددة، مثل التقارير الرسمية، والمقالات الإخبارية، والمقابلات، والوثائق الداخلية للبنك (إن أمكن).
- **تحليل البيانات:** تحليل البيانات التي تم جمعها لتحديد العوامل التي ساهمت في السرقة، وتقييم إجراءات إدارة المخاطر والأمن السيبراني في البنك، وتحديد نقاط الضعف.
- **استخلاص النتائج والتوصيات:** استخلاص النتائج من التحليل وتقديم توصيات عملية للبنك المركزي والبنوك المركزية الأخرى لتحسين أمنها السيبراني وإدارة المخاطر.

١,٨ . منهجية الدراسة

١. تصميم البحث:

سيتم استخدام تصميم دراسة حالة (Case Study) كمنهجية بحثية رئيسية في هذه الدراسة. يعتبر هذا التصميم مناسباً نظراً لطبيعة الموضوع، حيث يتيح لنا التعمق في تفاصيل حدث معين (سرقة بنك بنغلاديش المركزي) وتحليل العوامل المختلفة التي ساهمت في حدوثه.

٢. جمع البيانات:

سيتم جمع البيانات من مصادر ثانوية متنوعة، بما في ذلك:

التقارير الرسمية: مثل تقرير التحقيق الذي أجراه بنك بنغلاديش المركزي، وتقارير المؤسسات المالية الدولية (مثل صندوق النقد الدولي والبنك الدولي) التي تناولت الحادثة.

المقالات الصحفية: سيتم جمع المقالات الإخبارية والتحليلات التي نشرتها وسائل الإعلام العالمية الموثوقة حول السرقة، مثل قناة الجزيرة، نيويورك تايمز، ورويترز، وبلومبيرغ.

الأوراق البحثية والأكاديمية: سيتم البحث عن الدراسات والأبحاث الأكاديمية التي تناولت الأمن السيبراني وإدارة المخاطر في البنوك المركزية، بالإضافة إلى دراسات الحالة حول سرقات بنوك أخرى.

الكتب والمؤلفات: سيتم الرجوع إلى الكتب والمؤلفات التي تتناول إدارة المخاطر في البنوك وأمن المعلومات، والتي يمكن أن توفر إطارًا نظريًا لتحليل حالة بنك بنغلاديش.

مصادر الإنترنت: سيتم البحث في المدونات والمواقع الإلكترونية المتخصصة في الأمن السيبراني، والتي قد تحتوي على تحليلات وآراء خبراء حول السرقة.

٣. تحليل البيانات:

سيتم تحليل البيانات التي تم جمعها باستخدام مجموعة من التقنيات النوعية، بما في ذلك:

التحليل الموضوعي: سيتم تحديد الأنماط والموضوعات الرئيسية التي تظهر في البيانات، مثل نقاط الضعف في إدارة المخاطر، والثغرات الأمنية، والأخطاء البشرية، والعوامل الخارجية.

التحليل السببي: سيتم تحديد العلاقات السببية بين العوامل المختلفة التي ساهمت في السرقة، وتحديد العوامل الرئيسية التي أدت إلى فشل إدارة المخاطر.

التحليل المقارن: سيتم مقارنة حالة بنك بنغلاديش مع حالات أخرى لسرقات البنوك المركزية لتحديد أوجه التشابه والاختلاف، واستخلاص الدروس المستفادة.

٤. التحقق من صحة النتائج:

للتحقق من صحة النتائج، سيتم استخدام تقنيات التحقق التالية:

- **التثليث:** سيتم مقارنة البيانات والنتائج من مصادر مختلفة للتأكد من اتساقها.
- **مراجعة الأقران:** سيتم عرض النتائج على خبراء في مجال الأمن السيبراني وإدارة المخاطر للحصول على تعليقاتهم وتقييمهم.

٥. كتابة التقرير:

سيتم كتابة تقرير البحث بطريقة أكاديمية ومنهجية، مع مراعاة المعايير الأخلاقية للبحث العلمي. سيتضمن التقرير الأقسام التالية:

- **مقدمة:** تقديم خلفية عن الموضوع وأهميته، وتحديد المشكلة البحثية وأهداف الدراسة.
- **مراجعة الأدبيات:** استعراض الدراسات السابقة ذات الصلة وتحديد الفجوات المعرفية.
- **منهجية البحث:** وصف المنهجية المستخدمة في جمع وتحليل البيانات.
- **نتائج البحث:** عرض النتائج التي تم التوصل إليها من خلال تحليل البيانات.
- **مناقشة النتائج:** مناقشة النتائج في ضوء الأدبيات السابقة وتقديم تفسيرات لها.
- **الاستنتاجات والتوصيات:** تلخيص النتائج الرئيسية وتقديم توصيات عملية للبنوك المركزية.

١,٩. الدراسة الميدانية

بالنظر إلى طبيعة دراسة الحالة هذه، والتي تعتمد على تحليل حدث سابق (سرقة بنك بنغلاديش المركزي)، فإن الدراسة الميدانية التقليدية - التي تتضمن جمع بيانات أولية من المشاركين أو الملاحظة المباشرة - قد لا تكون ممكنة أو مناسبة.

ومع ذلك، يمكن إجراء دراسة ميدانية "معدلة" أو "محدودة" من خلال:

- **المقابلات مع الخبراء:** يمكن إجراء مقابلات مع خبراء في مجال الأمن السيبراني وإدارة المخاطر في البنوك المركزية، للحصول على رؤيتهم وتحليلهم للحادثة، وتقييمهم لإجراءات إدارة المخاطر في بنك بنغلاديش المركزي، واقتراحاتهم لتحسين الأمن السيبراني في البنوك المركزية بشكل عام.
- **زيارات ميدانية (إن أمكن):** إذا كان ذلك ممكناً، يمكن القيام بزيارات ميدانية إلى بنك بنغلاديش المركزي أو بنوك مركزية أخرى مماثلة، للتعرف على البنية التحتية التكنولوجية وإجراءات الأمن السيبراني المتبعة، ومقابلة المسؤولين عن إدارة المخاطر والأمن السيبراني.

- **ورش عمل أو مجموعات نقاش:** يمكن تنظيم ورش عمل أو مجموعات نقاش مع خبراء وممارسين في مجال الأمن السيبراني وإدارة المخاطر، لمناقشة نتائج البحث والحصول على تعليقاتهم واقتراحاتهم.
- **استبيانات (اختيارية):** يمكن تصميم استبيانات إلكترونية لتوزيعها على موظفي البنوك المركزية والمتخصصين في الاقتصاد، لجمع بيانات حول وعيهم بالتهديدات السيبرانية، وتقييمهم لإجراءات إدارة المخاطر في مؤسساتهم.

١٠، ١. مخطط المشروع المقترح

الفصل الأول: مقدمة

- خلفية عن الموضوع وأهميته
- بيان المشكلة البحثية
- أسئلة البحث وأهداف الدراسة
- أهمية الدراسة
- حدود الدراسة

الفصل الثاني: مراجعة الأدبيات

- إدارة المخاطر في البنوك المركزية
- الأمن السيبراني في البنوك المركزية
- التهديدات السيبرانية الناشئة
- دراسات حالة سابقة لسرقات البنوك

الفصل الثالث: منهجية البحث

- تصميم البحث (دراسة الحالة)

- مصادر البيانات (ثانوية وميدانية)
- أدوات جمع البيانات (تحليل الوثائق، مقابلات مع الخبراء، استبيانات اختيارية)
- أدوات تحليل البيانات (تحليل موضوعي، تحليل سببي، تحليل مقارنة)
- اعتبارات أخلاقية

الفصل الرابع: نتائج البحث

- وصف تفصيلي لسرقة بنك بنغلاديش المركزي
- تحليل نقاط الضعف في إدارة المخاطر والأمن السيبراني
- البنية التحتية التكنولوجية
- إجراءات إدارة المخاطر
- العوامل البشرية
- العوامل الخارجية
- تقييم تأثير السرقة على البنك والنظام المالي

الفصل الخامس: مناقشة النتائج

- مناقشة النتائج في ضوء الأدبيات السابقة
- تحليل مقارنة مع حالات أخرى
- استخلاص الدروس المستفادة

الفصل السادس: الاستنتاجات والتوصيات

- تلخيص النتائج الرئيسية
- تقديم توصيات عملية لبنك بنغلاديش المركزي والبنوك المركزية الأخرى
- اقتراح إطار عمل شامل لإدارة المخاطر والأمن السيبراني

- Schneier, B. (1998). Security is a process, not a product. Crypto-Gram Newsletter. Retrieved from <https://www.schneier.com/crypto-gram/archives/1998/1215.html>
- Mitnick, K. & Simon, W. L. (2002). The Art of Deception: Controlling the Human Element of Security. Wiley.
- How the New York Fed fumbled over the Bangladesh Bank cyber-heist By Krishna N. Das and Jonathan Spicer
- Bangladesh Bank Cyber Heist Case Study
- SWIFT. (2016). Customer Security Program Framework.
- Hossain, M. A., Sarker, M. D. A., Hossain, M. S., Shaon, M. A. R., Hossain, M. S., Rayhan, M. M. H., & Astudillo, J. G. S. Bangladesh Bank Money Heist: A Concern of Cybersecurity System of Bangladesh Bank and Way Forward. Shanahan, M. (2016, March 7). How Hackers Stole \$81 Million From Bangladesh Central Bank. The New York Times.
- Hull, J. (2012). Risk management and financial institutions,+ Web Site (Vol. 733). John Wiley & Sons.
- Mitnick, K. D., & Simon, W. L. (2003). The art of deception: Controlling the human element of security. John Wiley & Sons.