صندوق النقد العربي
ARAB MONETARY FUND

الأمن السيبراني في القطاع المصرفي
عرض مقارن للمعايير والتجارب الدولية والعربية

د. محمد إسماعيل

الدائرة الاقتصادية والفنية

الاجتماع الثالث لمجموعة العمل الإقليمية للتقنيات المالية الحديثة

صندوق النقد العربي – أبو ظبي
9-10 ديسمبر 2019

نقاط العرض

اولاً: أهمية وجود معايير محددة تنظم المخاطر السيبرانية.

ثانياً: الأطر والمعايير الدولية المُنظمة للمخاطر السيبرانية.

ثالثاً: الجوانب المتعلقة بأمن الفضاء الإلكتروني في إطار المخاطر التشغيلية للبنوك المركزية العربية.

اولاً: أهمية وجود معايير محددة تنظم المخاطر السيبرانية

- **تختلف الآراء حول كيفية تنظيم مخاطر الإنترنت:**

  - **حيث يرى بعضها أن الطبيعة المتطورة للمخاطر السيبرانية ليست قابلة للتنظيم بشكل محدد، كما أن القضايا الخاصة بالإنترنت (cyber issues) يمكن معالجتها من خلال اللوائح الحالية المتعلقة بكل من المخاطر التشغيلية والتقنيات في القطاع المصرفي.**
  - **فيما يشير البعض الآخر إلى أن هناك حاجة ملحة إلى وجود هيكل تنظيمي للتعامل مع الطبيعة الفريدة للمخاطر الإلكترونية، وذلك بالنظر إلى التهديدات المتزايدة الناتجة عن التحول المكثف نحو قطاع مالي رقمي في الآونة الاخيرة.**

اولاً: أهمية وجود معايير محددة تنظم المخاطر السيبرانية

- إن التطور الحادث في المخاطر السيبرانية يحفز المؤسسات المالية على البحث المستمر والمكثف نحو اتخاذ إجراءات وقائية من تلك المخاطر من خلال لوائح تجعل تلك الإجراءات أكثر وضوحاً أمام مجالس إدارات تلك المؤسسات، الأمر الذي يؤدي إلى خلق حافز أكبر على الاستثمار بشكل مستمر في تعزيز الأمن السيبراني.

اولاً: أهمية وجود معايير محددة تنظم المخاطر السيبرانية

- إضافة إلى أن إدراج المخاطر السيبرانية ضمن المخاطر التشغيلية للمؤسسات المالية يعتبر غير كافي، حيث إن المعايير الرقابية على المصارف تتطلب أهمية تضمين الاستراتيجيات والسياسات الخاصة بتلك المصارف جزءً خاصاً بإدارة المخاطر السيبرانية، يتم مراجعتها بانتظام من قبل مجالس إدارات البنوك مع زيادة حجم المخاطر السيبرانية.

ثانياً: الأطر والمعايير الدولية المُنظمة للمخاطر السيبرانية

تغطي هذه الأطر والمعايير المحاور التالية:

1. الحوكمة الالكترونية (Cyber-governance):

- أهمية وجود استراتيجية للأمن السيبراني بحيث تضع كل مؤسسة مالية استراتيجية الأمن السيبراني الخاصة بها وفقًا لممارسات إدارة المخاطر المستندة إلى المبادئ.
- تقوم الجهات الرقابية بمراجعة هذه الاستراتيجيات كجزء من تقييمها للممارسات الشاملة لإدارة المخاطر في المؤسسة.

1. الحوكمة الالكترونية (Cyber-governance):

❑ **جميع الجهات الرقابية الدولية تؤكد على اهمية:**

- ❖الأدوار والمسؤوليات الإدارية والضوابط الخاصة بالحوكمة الإلكترونية.
- ❖تنمية الوعي الثقافي للأمن السيبراني للعملاء من خلال العاملين في القطاعات المالية.
- ❖توافر الكوادر المدربة القادرة على تحمل المسؤوليات والقيام بالمهام الوظيفية الموكلة اليها في مجال الأمن السيبراني.

2. مفاهيم إدارة المخاطر واختبارها وكيفية التغلب على الانتـــهاكات (Approaches to risk management, testing and incident response and recovery)

يشتمل هذا المحور أربع مفاهيم رئيسة تتمثل في:

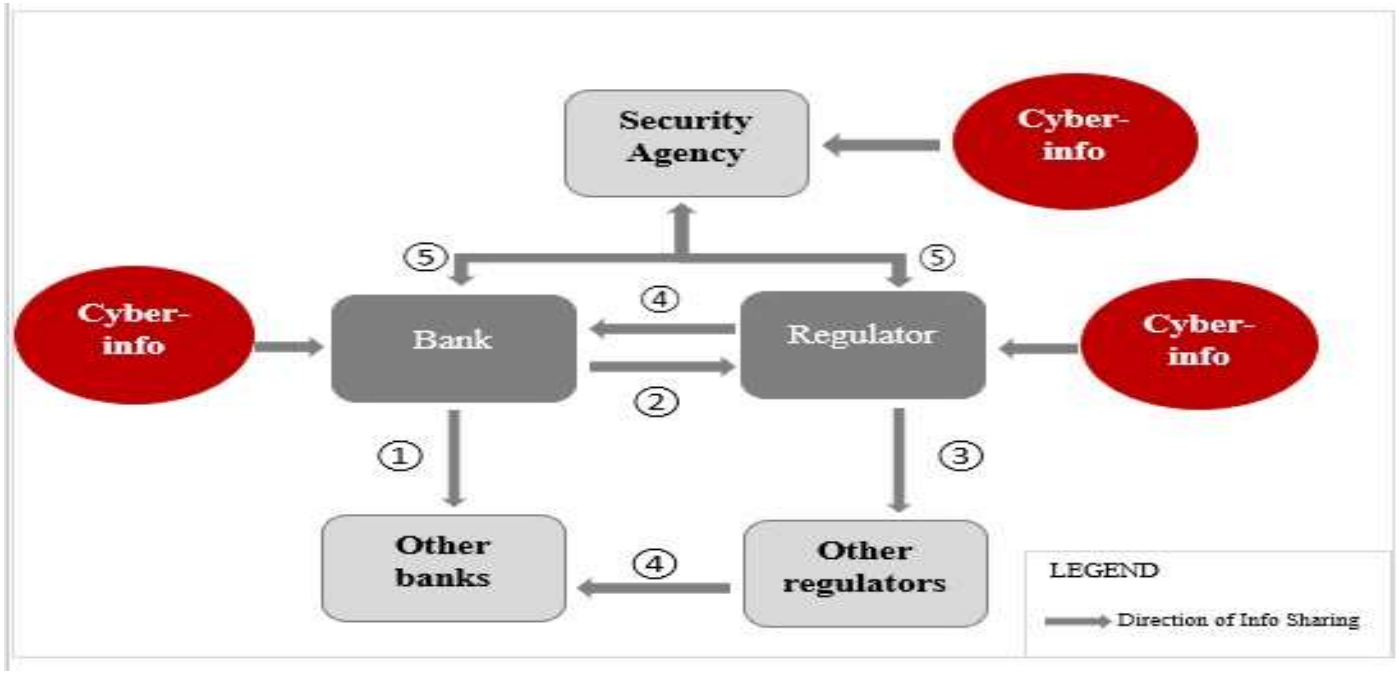
- طرق الرقابة على الأمن السيبراني (cyber-resilience).
- ضوابط أمن المعلومات وطرق اختبارها وضمان استقلاليتها.
- مدى الاستجابة للتغلب على المخاطر.
- مقاييس الأمن السيبراني والمرونة.

3. التواصل وتبادل المعلومات (Communication and sharing of information)

من الأنماط المتعارف عليها للتواصل في مجال مشاركة اهم الممارسات في مجال الامن السيبراني، يعتبر مشاركة المعلومات بين البنوك، والمشاركة بين البنك والجهات الرقابية، ومشاركة تلك المعلومات مع الأجهزة الأمنية من أكثر الممارسات المتعارف عليها في هذا المجال.

3. التواصل وتبادل المعلومات (Communication and sharing of information)

الأنماط المختلفة للتواصل في مجال الأمن السيبراني



Source: Basel Committee on Banking Supervision.

4. تعهيد أمن نظم المعلومات والأنظمة الإلكترونية إلى جهة ثالثة (Interconnections with third parties)

إن الاستخدام المكثف لخدمات التعهيد إلى طرف ثالث يزيد من التحدي أمام الهيئات والجهات الرقابية للحصول على رؤية كاملة للضوابط المعمول بها ومستوى المخاطر.

4. تعهيد أمن نظم المعلومات والأنظمة الإلكترونية إلى جهة ثالثة (Interconnections with third parties)

تتمثل خدمات التعهيد الى جهة ثالثة في كافة أشكال الاستعانة بمصادر خارجية بما في ذلك:

- خدمات الحوسبة السحابية (cloud computing services).
- الخدمات والمنتجات المعيارية وغير المعيارية التي لا تعتبر عادةً مصادر خارجية (power supply).

4. تعهيد أمن نظم المعلومات والأنظمة الإلكترونية إلى جهة ثالثة (Interconnections with third parties)

- خطوط الاتصالات السلكية واللاسلكية، الأجهزة والبرامج التجارية، ...إلخ.
- الأطراف الأخرى مثل (المؤسسات المالية أو غير المالية) والمؤسسات المالية الدولية (مثل أنظمة الدفع والتسوية، منصات التداول، أمناء حفظ الأوراق المالية المركزية والأطراف المقابلة المركزية).

ثالثاً: الجوانب المتعلقة بأمن الفضاء الإلكتروني في إطار المخاطر التشغيلية للبنوك المركزية العربية.

1. الإطار الرقابي العام للمخاطر المرتبطة بأمن نظم المعلومات والفضاء الإليكتروني.

اشارت النتائج الى قيام جميع الدول المستوفية للاستبيان :

- تضمين التعليمات الرقابية الخاصة بإطار المخاطر التشغيلية (Operational Risks) جزءً متعلقاً بمخاطر نظم المعلومات وأمن الفضاء الإلكتروني في القطاع المصرفي يحدد المعايير اللازم توافرها لضمان أمن الفضاء الإلكتروني.
- بتضمين عمليات الرقابة على أساس المخاطر (ongoing risk-based supervisory activities) لاختبارات توضح مدى قدرة المصارف على مواجهة مخاطر أمن الفضاء الإلكتروني (تجارب محاكاة لهجمات افتراضية)، وذلك بصفة دورية سنوية.
- قيام السلطات الرقابية بإصدار تعليمات وقواعد تنظم تقديم الخدمات المصرفية من خلال الانترنت. وتفاوتت سنة اصدار تلك التعليمات من دولة الى أخرى.

1. الإطار الرقابي العام للمخاطر المرتبطة بأمن نظم المعلومات والفضاء الإليكتروني (تابع).

اشارت النتائج الى قيام جميع الدول المستوفية للاستبيان :

- وجود توجيهات رقابية تلزم المصارف بتضمين استراتيجيات المخاطر المُقرة من قبل مجالس إدارات البنوك إطاراً يتعلق بالمخاطر الإلكترونية ومخاطر نظم المعلومات والهجمات الإلكترونية (Cyber attacks).
- التحقق من وجود استراتيجية للمخاطر من خلال عمليات الرقابة المصرفية مُقرة من قبل مجالس إدارات البنوك تتضمن مستوى المخاطر المتعلقة بأمن الفضاء الإلكتروني وإجراءات موازية لدعم مستويات أمن الفضاء الإلكتروني (cyber resilience).
- معظم الدول تلزم المصارف بتعيين مسؤول عن أمن المعلومات Chief Information Security Officer (CISO)من خلال إطار التعليمات الرقابية الخاصة بمخاطر أمن الفضاء الإلكتروني.

2. الضوابط والتعليمات الخاصة بتنظيم وإدارة الحسابات والخدمات المصرفية المقدمة عبر الانترنت

أشارت معظم الدول الى انه يسمح للعملاء بإنشاء أو فتح حساب مصرفي من خلال موقع البنك على شبكة الانترنت، وذلك في ضوء عدد من الضوابط والتعليمات بالنسبة للمصرف والعميل.

3. الضوابط والتعليمات الخاصة بتنظيم وسائل اثبات الهوية عبر الانترنت

استخدام عملية التوثيق two factor authentication

استخدام الرمز السري لمرة واحدة OPT

اتفقت معظم الردود الواردة من الدول على ان الوسائل التي تعتمد عليها البنوك في التحقق من هوية العميل المستفيد من الخدمات المصرفية من خلال الانترنت تكون من خلال:

استخدام الرقم السري Token

ارسال رسالة نصية للتحقق من هوية المستخدم

4. الضوابط والتعليمات الرقابية الخاصة بإدارة كلمة السر (Password)

اتفقت معظم الردود على ان التعليمات والتدابير الرقابية الخاصة بإدارة كلمة السر (Password) ومواصفاتها على ان المصرف المركزي يلزم البنوك بوضع سياسة شاملة لإدارة كلمة السر:

- ❑ حيث تضم هذه السياسة بعض الشروط مثل تغيير كلمة السر كل فترة زمنية.
- ❑ وبالنسبة لـ OTP فان مواصفاتها راجعة لسياسة كل بنك في هذا الشأن.

5. الضوابط والتعليمات الرقابية الخاصة بعمليات تحويل الأموال من خلال خدمات الانترنت

اشارت معظم الردود في هذا الشأن انه اثناء عملية تحويل الأموال من حساب إلى حساب آخر عن طريق الانترنت، يتم استخدام:

- عملية التوثيق المزدوجة وذلك للتحقق من هوية منفذ العملية (two-factor authentication).
- كما أن هناك حد أقصى للمبالغ التي يستطيع العميل تحويلها إلى حساب آخر عن طريق الانترنت البنكي.

6. الضوابط والتعليمات الرقابية الخاصة بسرية وسلامة المعلومات

اشارت الدول المستوفية للاستبيان ان:

- المصرف المركزي يلزم جميع البنوك باتخاذ كافة الإجراءات والتدابير الأمنية لضمان سرية وسلامة معلومات العملاء، حيث:
  - ✓ يجب على البنك القيام بعملية تقييم للمخاطر لتحديد المخاطر المحتمل وقوعها واتخاذ التدابير اللازمة للوقاية منها.

- كما يقوم المصرف المركزي بوضع معايير معينة لأدوات وبرامج الحماية التي يجب على البنك استخدامها. (مثل كلمات السر الخاصة بالمعاملات المالية والخدمات المقدمة من خلال الانترنت وخلاف ذلك من المعلومات السرية الأخرى الخاصة بالعملاء).

7. الضوابط والتعليمات الرقابية الخاصة بتأمين التطبيقات الالكترونية المستخدمة في تقديم الخدمات والمعاملات البنكية من خلال شبكة الانترنت

اشارت معظم الردود الواردة بالاستبيان الى ان البنك المركزي قام بوضع لائحة من التعليمات لتأمين التطبيقات الإلكترونية الخاصة بالبنوك، ومن أهمها:

- تثبيت برامج الحماية للحفاظ على هذه التطبيقات من الاختراق.
- إجراء الاختبارات الأمنية على التطبيقات (قبل تثبيتها وبعده).
- يجب على البنوك تقييم نقاط الضعف الموجودة في التطبيقات مرتين على الأقل سنوياً، والعمل على خطة للحد من نقاط الضعف ومشاركة الخطة مع الإدارة العليا.
- إضافة إلى العديد من التعليمات والضوابط الأخرى التي تهدف إلى حماية التطبيقات الإلكترونية المستخدمة في البنوك من الاختراقات.

8. التعاون والتنسيق مع السلطات الرقابية الأخرى عبر الحدود والشركاء في صناعة تكنولوجيا المعلومات فيما يتعلق بالمخاطر المرتبطة بأمن نظم المعلومات والفضاء الإلكتروني

أوضحت الدول المستوفية للاستبيان انه يتم التعاون مع المؤسسات الإقليمية والسلطات الرقابية في الخارج وذلك من خلال:

- المشاركة في اللجان المختلفة بهدف تبادل الخبرات والتعرف على أهم ما توصلت له هذه المؤسسات في مجال تطوير الأمن الإلكتروني في القطاع المالي.

- إضافة الى انه يتم التعاون مع مختلف المؤسسات والمراكز البحثية من خلال توقيع اتفاقيات التدريب والتطوير والتعاون للبحث عن سبل تطوير أمن المعلومات في القطاع المالي.

9. بناء القدرات الرقابية في مجال أمن نظم المعلومات والفضاء الإلكتروني

اشارت نتائج الاستبيان الى قيام المصارف المركزية:

- بتدريب موظفي الأمن الإلكتروني من خلال مشاركتهم في الدورات التدريبية (الداخلية والخارجية) المتعلقة بأمن المعلومات.
- تقوم بحث الموظفين على استكمال الدراسات العليا في مجال أمن المعلومات مما يعزز فرص تطويرهم ويصقل خبراتهم.

10. التحديات الرقابية في مجال أمن نظم المعلومات والفضاء الإليكتروني

أوضح الاستبيان ان أهم التحديات تتمثل في التطور السريع في مجال تقنية المعلومات والاعتماد المتزايد على التكنولوجيا للقيام بمعظم العمليات المالية، مما يؤدي إلى زيادة التعرض للتهديدات والحوادث الالكترونية.

مع الشكر،،