Quel rôle pour les superviseurs bancaires face à la cyber criminalité

Forum des Compétences

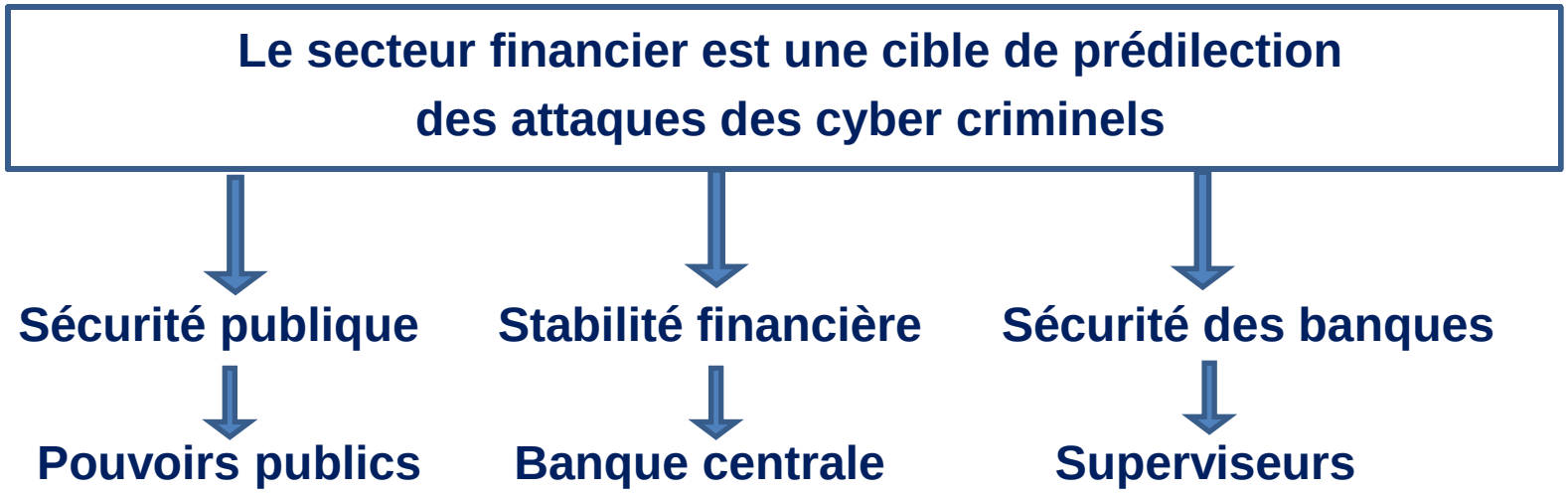
Rencontre Événementielle

Cyber - protection : au-delà de la LPM

Paris, le 27 mars 2015 Frédéric VISNOVSKY Secrétaire général adjoint

1 – La cyber criminalité, une réalité qui appelle à la mobilisation de tous les acteurs

- Le secteur financier est particulièrement exposé avec le développement soutenu de la dématérialisation : les évolutions technologiques ont permis de réduire certains risques opérationnels (notamment d'exécution) mais avec
  - l'expansion des réseaux et des technologies,
  - l'ouverture des systèmes d'information aux échanges extérieurs,
  - la croissance des transactions électroniques,…



1.1. L'action des pouvoirs publics dans un contexte européen

Un plan de cyber sécurité au niveau de l'Union européenne

5 priorités :

- parvenir à la cyber-résilience,
- faire reculer considérablement la cybercriminalité,
- développer une politique et des moyens de cyber défense en liaison avec la politique de sécurité et de défense commune ,
- développer les ressources industrielles et technologiques en matière de cyber sécurité,
- instaurer une politique internationale de l'Union européenne cohérente en matière de cyberespace et promouvoir les valeurs essentielles de l'UE.

Proposition de directive concernant la sécurité des réseaux et de l'information (SRI) :

(a) Adoption d'une stratégie de SRI et désignation des autorités pour prévenir et gérer les risques et incidents de SRI et intervenir en cas de nécessité,

(b) Mécanisme de coopération pour diffuser des messages d'alerte rapide sur les risques et incidents au moyen d'une infrastructure sécurisée,

(c) Pour les opérateurs d'infrastructures critiques : adopter des pratiques en matière de gestion des risques et signaler les incidents de sécurité significatifs touchant leurs services essentiels.

En France : rôle de l'ANSSI

1.2. L'action de la Banque de France

❑ L'organisation de la robustesse de la Place financière

Un Groupe de Place avec 5 objectifs :

- **Améliorer l'efficience** : consolider les dispositifs internes des établissements en situation de stress
- **Maîtriser les externalités** : besoin de coordination et de solidarité entre acteurs
- **Gérer l'incertitude** : le caractère évolutif des menaces exige une actualisation permanente des scénarios et des répondes à y apporter
- **Améliorer la capacité** de la Place financière de Paris à surmonter les chocs affectant des fonctions critiques telles que les systèmes de paiement, la gestion de la liquidité, le financement de l'économie
- **Renforcer l'attractivité** de la Place financière de Paris en montrant sa capacité à faire face à une crise opérationnelle majeure

Assurer la continuité en cas de crise

- Détecter et identifier les alertes pour mettre en place les mesures appropriées
- Etablir un état des lieux de la Place financière et informer les membres
- Etablir un dialogue permanent avec les services de l'Etat
- Prendre les décisions et les plans d'actions suite à une consultation collective
- Gérer la communication de crise

La cyber attaque est l'un des 8 scénarios de crise identifiés par le Groupe de Place

Un test de place réalisé en novembre 2012

1.3. L'action des superviseurs

Le risque IT est essentiel dans l'activité bancaire et pour les clients

Un risque multi forme : sécurité, continuité, réputation, conformité, confidentialité

Des obligations légales et réglementaires :

- Code monétaire et financier : LCB-FT
- Arrêté du 3 novembre 2014 (ex CRBF 97-02)
- Pratiques utiles : rapport Lagarde, Livres blancs de la Commission bancaire (informatique en 1996 et internet en 2000), étude sur le Cloud computing (2013)

Les outils de supervision :

- Contrôles sur place
- Rapports internes des banques
- Analyses transversales

Et la cyber criminalité ?

- Le senior supervisory group (SSG) a inscrit le sujet à son agenda
- L'une des priorités 2015 de la BCE

Définir une approche convergente au sein des superviseurs

Un questionnaire d'auto-évaluation (cf. annexe)

2 – Quelle approche par les superviseurs

2.1. Clarifier les concepts : de quoi parle-t-on ?

- **Mettre l'accent sur la 'cyber-sécurité'**
  - Protection des ordinateurs, des réseaux, des systèmes et bases de données contre les accès imprévus et non autorisés, les perturbations ou destructions
  - Objectifs : fraude, espionnage et sabotage/destruction malveillante
  - Menaces fréquentes : espionnage, vol de données, fraude, blocage
  - Attaques fréquentes : dénis de service (*dDoS*) , malveillances, défigurations de sites (*defacements*)…

- **avec pour objectif d'évaluer l'état de préparation des banques et leur capacité de réaction**

2 – Quelle approche par les superviseurs
2.2. Clarifier le champ : quelle partie de l'IT ?

- Tout l'IT ? (des milliers d'applications)
- Uniquement les applications critiques ? (des centaines)
- Internes et externes ?
- Et les paiements ?
- Et les données clients traitées en dehors de la banque ?

- **Tout l'IT doit être protégé**
  - Les menaces peuvent porter sur tous les systèmes
  - Les systèmes de paiements entrent dans le champ de la supervision
  - La protection des données clients hors de la banque n'est pas directement dans le champ

- **Mais l'approche retenue doit être fondée sur les risques :**
  - Sensibilisation (culture du risque/appétit au risque)
  - Prévention (politiques de sécurité)
  - Détection (outils de détection et d'information des dirigeants)
  - Réponse (contre mesures, plans de continuité, gestion de crise)

2 – Quelle approche par les superviseurs

2.3 Clarifier le champ d'action des superviseurs

- **Quelle articulation avec les agences de sécurité (ANSSI en France) ?**
  - Elles ont les outils et les expertises, mais
  - Elles mettent l'accent sur les institutions vitales et les grandes infrastructures
  - Elles s'occupent principalement des systèmes vitaux

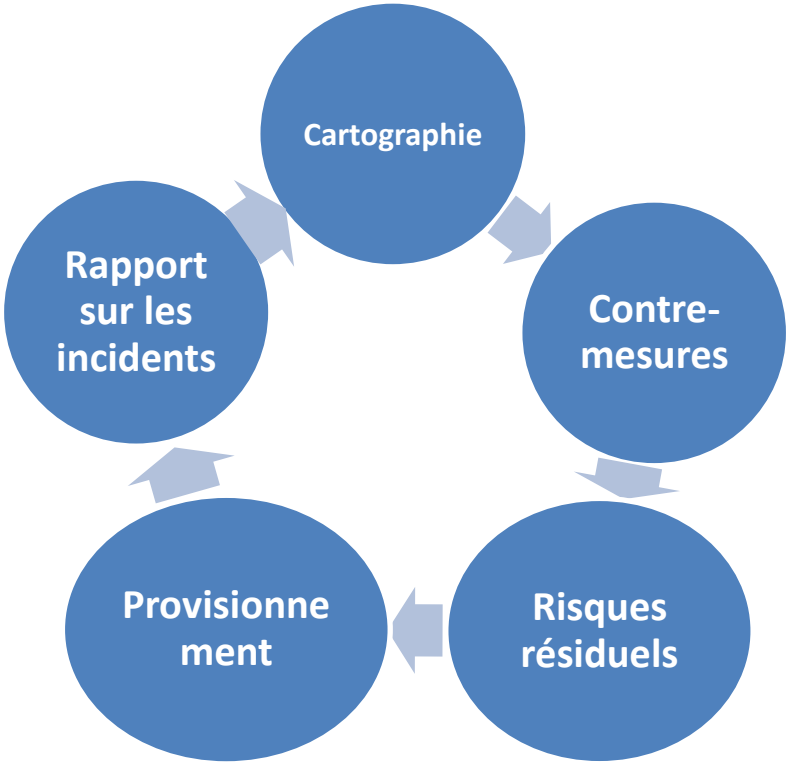
- **Les superviseurs doivent élargir leur champ habituel de contrôle**
  - IT est au cœur des métiers des banques et pour leurs clients
  - Les cyber-attaques sont plus nombreuses, intelligentes et plus préjudiciables
  - La cyber-sécurité est un risque spécifique au sein des risques IT

2 – Quelle approche par les superviseurs

2.4. Clarifier le cadre : le risque opérationnel

- **Le cadre pour le risque opérationnel n'a pas évolué depuis 2003. Couvre-t-il bien le cyber risque ?**

- **Le risque IT pourrait justifier un traitement spécifique :**
  - Toutes les attaques ne génèrent pas des pertes
  - Certains incidents méritent d'être identifiés pour mesurer l'intensité de l'attaque
  - Le provisionnement est-il la bonne réponse contre un cyber-risque résiduel ?



2 – Quelle approche par les superviseurs
2.5. Quel cadre de contrôle ?

- **Sensibilisation :**
  - Gouvernance et stratégie
  - Identification des menaces
- **Prévention :**
  - Politiques de sécurité
  - Cartographie des systèmes IT
  - Evaluation des risques, tests de vulnérabilité
  - Mesures de sécurité
  - Formations, gestion de crise
- **Détection :**
  - Outils de détection
  - Analyses
  - Information du management => reporting aux superviseurs
- **Réponse :**
  - Contre mesures
  - Plans de continuité et de rétablissement

Annexe

Questionnaire d’auto évaluation

	IDENTIFY	
1	**Asset Management** The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to business objectives and the organization's risk strategy	* Physical devices and systems within the organization are inventoried. * Software platforms and applications within the organization are inventoried * Maps of network resources, connections with external and mobile resources and data flows are created and updated * Resources (e.g., hardware, devices, data, and software) are prioritized for protection based on their sensitivity and business value * The institution can rely on a qualified workforce IT Security Professionals, with no relevant shortage and low turnover
2	**Business Environment**	* The organization's place in critical infrastructure and its industry sector is identified and communicated * Priorities for organizational mission, objectives, and activities are established and communicated * Dependencies and critical functions for delivery of critical services are established * Resilience requirements to support delivery of critical services are established
3	**Governance**	* The Senior Management is involved in Cybersecurity and receives adequate management information/reporting * Organizational information security policy is established * Cybersecurity roles and responsibilities for the entire workforce are established and aligned with internal roles and responsibilities The Organization has a Chief Information Security Officer or an equivalent position * Outsourced IT resources comply with the same requirements as inhouse resources (and processes are in place to manage that) * Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed * Governance and risk management processes address cybersecurity risks

4	**Risk Assessment** The organisation understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets and individuals.	* Asset vulnerabilities are identified and documented * Threats, both internal and external, are identified and documented * Potential business impacts and likelihoods are identified * Threats, vulnerabilities, likelihoods, and impacts are used to determine risk * Risk responses are identified and prioritized * Residual risk is evaluated and accepted by senior management * Risk assessment is a continuous process * IT audits are performed regularly and planning is in line with risk profile
5	**Risk Management Strategy** The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.	* Risk management processes are established, managed, and agreed to by organizational stakeholders * Organizational risk tolerance is determined and clearly expressed * The organization’s determination of risk tolerance is informed by its role in critical infrastructure and sector specific risk analysis

	PROTECT	
6	**Access Control** Access to assets and associated facilities is limited to authorized users, processes , or devices, and to authorized activities and transactions	* Identities and credentials are managed for authorized devices and users * Physical access to assets is managed and protected * Remote access is managed and restricted to those networks necessary for the users'business functions * Access permissions are managed, incorporating the principles of least privilege and separation of duties * Network integrity is protected, incorporating network segregation where appropriate
7	**Awareness and Training** The organization's personnel and partners are provided cybersecurity awareness education and are adequately trained to perform their information security-related duties and responsibilities consistent with related policies, procedures, and agreements.	* All users are informed and trained about Cybersecurity (including removable and mobile media) * Privileged users understand roles & responsibilities * Third-party stakeholders (e.g., suppliers, customers, partners) understand roles & responsibilities * Senior executives understand roles & responsibilities * Physical and information security personnel understand roles & responsibilities

8	**Data Security** Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.	* Data-at-rest is protected * Data-in-transit is protected * Assets are formally managed throughout removal, transfers, and disposition * Adequate capacity to ensure availability is maintained * Protections against data leaks are implemented * Integrity checking mechanisms are used to verify software, firmware, and information integrity * The development and testing environment(s) are separate from the production environment
9	**Information Protection Processes and Procedures** Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets.	* A baseline configuration of information technology/industrial control systems is created and maintained * A System Development Life Cycle to manage systems is implemented * Configuration change control processes are in place * Backups of information are conducted, maintained, and tested periodically * Policy and regulations regarding the physical operating environment for organizational assets are met * Data is destroyed according to policy * Protection processes are continuously improved * Effectiveness of protection technologies is shared with appropriate parties * Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed * Response and recovery plans are tested * Cybersecurity is included in human resources practices (e.g., deprovisioning, personnel screening) * A vulnerability management plan is developed and implemented * Penetration tests are required and performed regularly

10	**Maintenance** Maintenance and repairs of industrial control and information system components is performed consistent with policies and procedures.	* Maintenance and repair of organizational assets is performed and logged in a timely manner, with approved and controlled tools * Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access
11	**Protective Technology** Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements.	* Audit/log records are determined, documented, implemented, and reviewed in accordance with policy * Removable media is protected and its use restricted according to policy * Access to systems and assets is controlled, incorporating the principle of least functionality (only what is needed) * Communications and control networks are protected (o.a. Firewalls) * The Institution maintains protection against Distributed Denial of Services (DDoS) attacks for critical internet-facing IP addresses

	DETECT	
12	**Anomalies and Events**	
	Anomalous activity is detected in a timely manner and the potential impact of events is understood.	* A baseline of network operations and expected data flows for users and systems is established and managed * Detected events are analyzed to understand attack targets and methods * Event data are aggregated and correlated from multiple sources and sensors * Impact of events is determined * Incident alert thresholds are established
13	**Security Continuous Monitoring**	
	The information system and assets are monitored at discrete intervals to identify cybersecurity events and verify the effectiveness of protective measures.	* The network is monitored to detect potential cybersecurity events * The physical environment is monitored to detect potential cybersecurity events * Personnel activity is monitored to detect potential cybersecurity events * Malicious code is detected * Unauthorized mobile code is detected * External service provider activity is monitored to detect potential cybersecurity events * Monitoring for unauthorized users, connections, devices, and software is performed * Monitoring of remotely-initiated requests for transfers of customer assets is performed (fraud detection) * Vulnerability scans are performed * Penetration tests are performed
14	**Detection Processes**	
	Detection processes and procedures are maintained and tested to ensure timely and adequate awareness of anomalous events.	* Roles and responsibilities for detection are well defined to ensure accountability * Detection activities comply with all applicable requirements * Detection processes are tested * Event detection information is communicated to appropriate parties * Detection processes are continuously improved

	RESPOND	
15	**Response Planning** Response processes and procedures are executed and maintained, to ensure timely response to detected cybersecurity events.	* Response plan is executed during or after an event * A crisis management organisation is in place and their members are regularly trained
16	**Communications** Response activities are coordinated with internal and external stakeholders, as appropriate, to include external support from law enforcement agencies.	* Personnel know their roles and order of operations when a response is needed * Events are reported consistent with established criteria * Information is shared consistent with response plans * Coordination with stakeholders occurs consistent with response plans * Voluntary information sharing occurs with external stakeholders to achieve broader cybersecurity situational awareness
17	**Analysis** Analysis is conducted to ensure adequate response and support recovery activities.	* Notifications from detection systems are investigated *The impact of the incident is understood * Forensics are performed * Incidents are categorized/prioritized consistent with response plans
18	**Mitigation** Activities are performed to prevent expansion of an event, mitigate its effects, and eradicate the incident.	* Incidents are contained * Incidents are mitigated * Newly identified vulnerabilities are mitigated or documented as accepted risks
19	**Improvements** Organizational response activities are improved by incorporating lessons learned from current and previous detection/response activities.	* Recovery plans incorporate lessons learned * Recovery strategies are updated

	RECOVER	
20	**Recovery Planning** Recovery processes and procedures are executed and maintained to ensure timely restoration of systems or assets affected by cybersecurity events.	* Recovery plan is executed during or after an event * The Institution has subscribed an insurance policy against IT risk or Cybercrime
21	**Improvements** Recovery planning and processes are improved by incorporating lessons learned into future activities.	* Recovery plans incorporate lessons learned * Recovery strategies are updated
22	**Communications** Restoration activities are coordinated with internal and external parties, such as coordinating centers, Internet Service Providers, owners of attacking systems, victims, other CSIRTs, and vendors.	* Public relations are managed * Reputation after an event is repaired * Recovery activities are communicated to internal stakeholders and executive and management teams