Webinar

La cybersécurité : un élément essentiel de votre dispositif de conformité

Juillet 2020

DUFF & PHELPS

1

Le panorama des cybermenaces pour les SGP

Le panorama des cybermenaces pour les SGP

Catégories de menaces

Espionnage

Les secrets

- Vol de propriété intellectuelle et d'informations commerciales sensibles
- Attaques opportunistes – collecte de renseignements à court terme
- Attaques visant le vol d'informations, par exemple :
  - Stratégies d'investissement
  - Systèmes informatiques
  - Accords de partenariat

Exemples

- APT3 : originaire de Chine avec un niveau de sophistication élevé

Sabotage

L'impact

- Destruction de systèmes/données :
  - Programme malveillant destructif utilisé pour altérer les systèmes
  - Les systèmes cruciaux des entreprises les intéressent
- DDoS :
  - Les systèmes externes et internes sont visés pour provoquer une perturbation.
- Violation de données

Exemples

- OurMine : son modus operandi varie considérablement, mais il s'agit très souvent d'attaques DDoS et d'appropriations de compte

Criminels

L'argent

- Vol cybernétique
- Extorsion DDoS
- Garder des données en otage et logiciel rançonneur
- Chevaux de Troie et hameçonnage bancaires
- Fraude ciblée

Exemples

- APT34/OilRig : originaire d'Iran, cible le Moyen-Orient
- FIN7 : groupe malveillant motivé par des objectifs financiers, tels que les distributeurs automatiques de billets et les systèmes POS

Cyber-Activistes

La cause

- La défiguration de sites Web est la modalité la plus fréquente
- DDoS
- Violation de données

Exemples

- Anonymous : origine inconnue, n'importe qui peut être « Anonymous ». Son modus operandi varie considérablement mais il recourt très souvent à des attaques DDoS.

Le panorama des cybermenaces pour les SGP

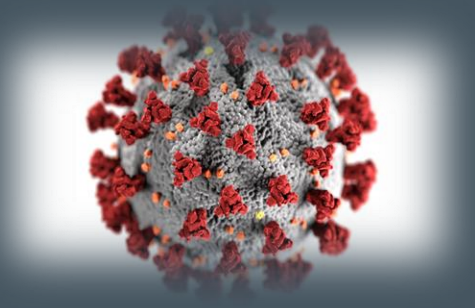
La crise de la COVID-19 a exacerbé certaines cybermenaces

« Bien connaître les risques permet de mieux détecter les attaques et de comprendre l'importance des mesures de sécurité à appliquer »

L'HAMECONNAGE

Dérober les informations confidentielles en prenant l'identité d'un tiers de confiance

Piratage de compte, fraude



LE VOL DE DONNEES

Intrusion dans le réseau de l'entreprise ou sur des hébergements externes pour dérober des données

Atteinte à l'activité et à l'image de l'entreprise

LES RANCONGICIELS

Empêcher l'accès aux données de l'entreprise et réclamer une rançon pour les libérer

Arrêt de l'activité, perte de données

LES FAUX ORDRES DE VIREMENT

Piratage d'un compte de messagerie en usurpant l'identité d'un prestataire, fournisseur ou autre pour demander un virement exceptionnel

Perte financière pour l'entreprise

02

La doctrine AMF – retour sur le contrôle SPOT

Anticiper les nouvelles exigences

La doctrine de l'AMF – Retour sur le contrôle SPOT

Synthèse des contrôles SPOT de l'AMF - 2019

L'AMF a publié en décembre 2019 la synthèse de ses contrôles thématiques « SPOT » sur les dispositifs de cybersécurité d'un échantillon de SGP

Non-conformités pouvant découler des risques cyber

- Niveau de fonds propres
- Politique rigoureuse de conservation et de maintien des données opérationnelles
- Plan de continuité de l'activité (PCA) adapté, testé et efficace
- Moyens informatiques adaptés et suffisants
- Dispositif solide de protection des données sensibles

Bonnes pratiques constatées

- **Prise en considération** des risques de cybersécurité à travers la **cartographie des risques**
- **Collecte des incidents** de cybersécurité subis
- **Vérification de la robustesse du SI** par des ressources ou prestataires spécialisés

Eléments d'amélioration

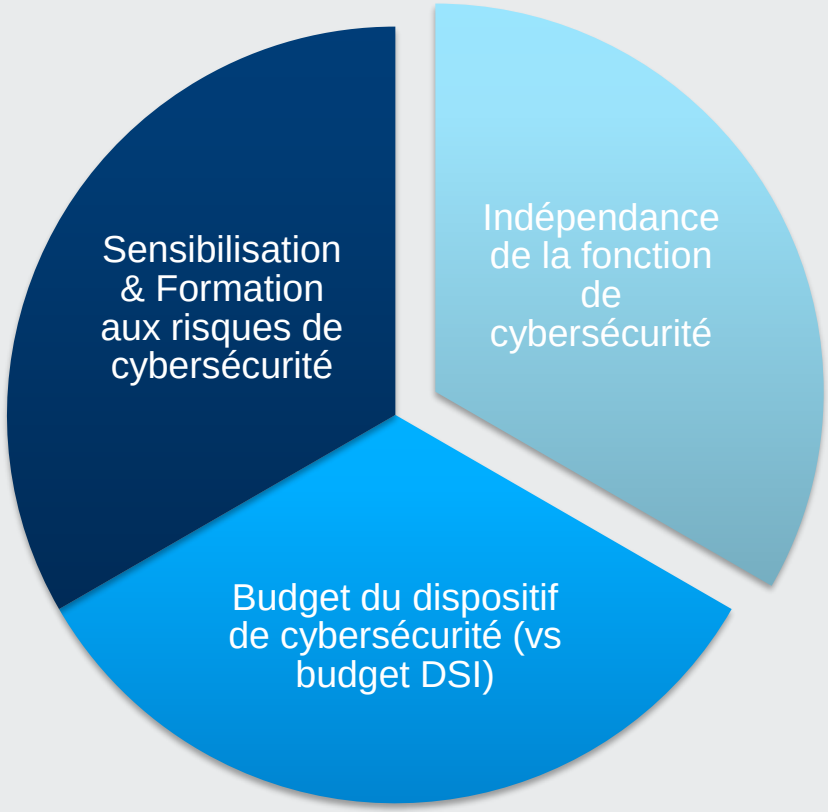
- **Non-prise en compte des impacts des risques de cybersécurité sur la conformité réglementaire** (i.e. fonds propres, conservation des données, plan de continuité de l'activité et moyens informatiques)
- **Absence de cartographie exhaustive de l'environnement IT** (i.e. données sensibles, systèmes critiques) et de classification des données
- **Difficulté à évaluer la matérialité des incidents de cybersécurité**
- **Pilotage insuffisant des prestations rendues par le Groupe** (i.e. non prise en compte des spécificités de la SGP et exonération de la gestion de la cybersécurité par les SGP)

Suite aux manquements constatés, l'AMF va reconduire ses contrôles SPOT sur ce thème en 2020

La doctrine de l'AMF – Retour sur le contrôle SPOT

Organisation du dispositif de cybersécurité

- **Formations qualifiantes** des employés dédiés à la cybersécurité
- Instauration d'un programme de **sensibilisation** aux risques de cybersécurité pour tous les salariés
- Suivi consolidé du niveau de prise de conscience des risques de cybersécurité par les utilisateurs du SI



- **Indépendance de la SGP** en fonction du Groupe (i.e. caractéristiques spécifiques vs standards du Groupe)
- **Indépendance du RSSI** par rapport au DSI
- **Dépendance à un prestataire externe unique**

Afin de démontrer **l'importance accordé au risque de cybersécurité de la SPG**

La doctrine de l'AMF – Retour sur le contrôle SPOT

Gouvernance du dispositif de cybersécurité

Pilotage des risques de cybersécurité par les instances de direction

Outils de pilotage des risques de cybersécurité

Stratégie claire et formalisée validée par la comité exécutif permettant de fournir un cadre formel stable, de prioriser les travaux en fonction de risques prioritaires et de les rendre accessibles aux non-spécialistes

Utilisation de référentiel reconnu pour appuyer la stratégie de cybersécurité (NSIT, COBIT 5, ISO, etc.)

Adaptation de la stratégie du Groupe **à la situation spécifique de la SGP**

A établir en fonction de l'organisation interne de la SGP

- **Cartographie des risques de cybersécurité** (impacts autant opérationnels que réglementaires, d'image, etc.)
- **Politiques**
- **Procédures**
- Modes opératoires
- **Référentiel de contrôles internes cybersécurité**
- **Cartographie des données sensibles**
- Etc.

La doctrine de l'AMF – Retour sur le contrôle SPOT

Administration du système d'information

Cloisonnement du réseau

- **Séparation du réseau de la SGP**

ou

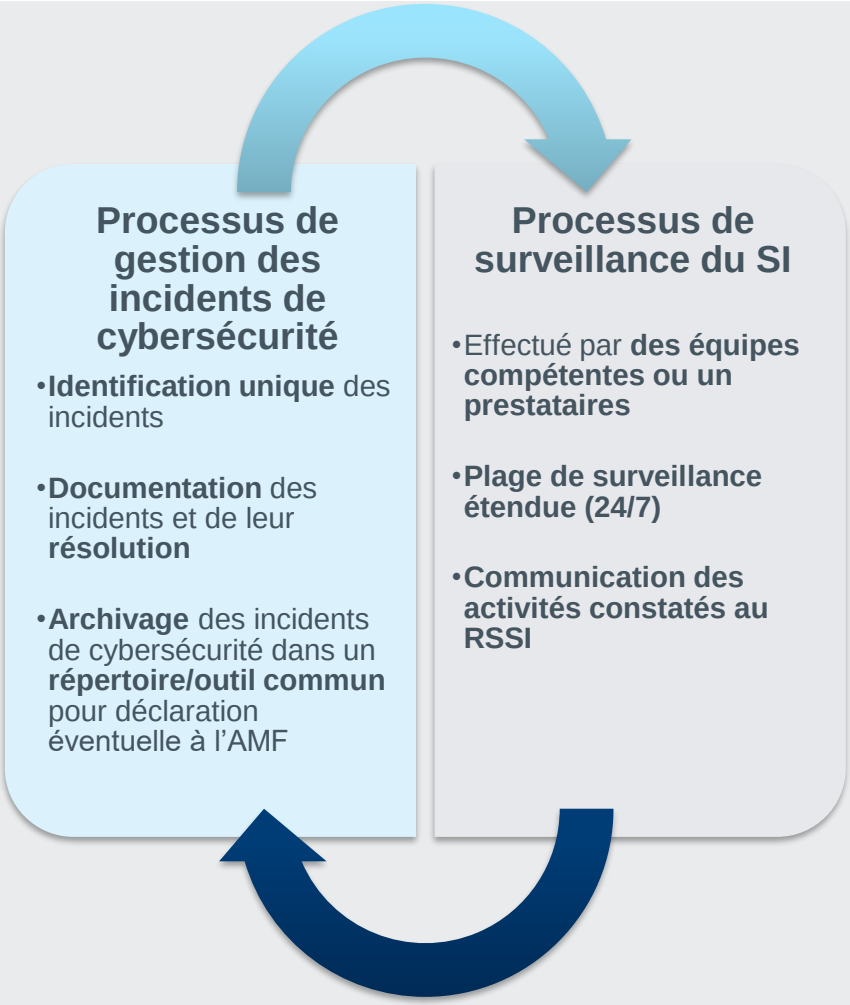
- **Habilitations** des droits d'accès logiques au SI commun favorisant les « murailles de Chine »

Processus d'administration du SI

- **Procédures d'administration du SI** incluant tous les équipements informatiques
- **Inventaire à jour des équipements informatiques**
- **Contrôles des connexions internes et externes**

La doctrine de l'AMF – Retour sur le contrôle SPOT

Surveillance du système d'information



Rappel réglementaire

- **Les dirigeants de la SGP informent sans délai l'AMF** des incidents dont la survenance est susceptible d'entraîner une perte ou un gain, un coût lié à la mise en cause de sa responsabilité civile ou pénale, à une sanction administrative ou à une atteinte à sa réputation et résultant du non-respect des règles d'organisation générale d'un montant brut dépassant 5 % de ses fonds propres réglementaires.
- Dans les mêmes conditions, **ils informent également l'AMF de tout événement ne permettant plus à la SGP de satisfaire aux conditions de son agrément.** Ils fournissent à l'AMF un compte rendu d'incident indiquant la nature de l'incident, les mesures adoptées après sa survenue et les initiatives prises pour éviter que des incidents similaires ne se produisent.
- **La SGP établit une base de données historique, dans laquelle sont enregistrés tous les dysfonctionnements, les pertes et les dommages** – articles 321-35 (g) (gestion d'OPCVM) et 318-6 (gestion de FIA) du règlement général de l'AMF.

La doctrine de l'AMF – Retour sur le contrôle SPOT

Gestion de la continuité de l'exploitation

En complément d'un plan de continuité de l'activité couvrant la perte ou l'indisponibilité du SI et garantissant une infrastructure robuste et résilient en cas de crise

Test de restauration des données sauvegardées

Installations informatiques de secours

Vérification des procédures et test de la perte ou de l'indisponibilité du SI

Inclure des tests pour toutes les données, en fonction de leur criticité sur un plan de rotation approprié

- Les installations de secours doivent bénéficier d'une protection physique suffisante afin d'être intègres et disponibles en cas de PCA
- Les attaques cyber sur les installations de secours, en cas d'une pandémie globale qui nécessite un déploiement du télétravail, doivent aussi être prise en compte dans le PCA et le plan de surveillance du SI

- Sur un périmètre représentatif de la SGP afin de s'assurer de l'efficacité du PCA
- Effectuée de façon régulière

Gestion adéquate de la continuité d'activité

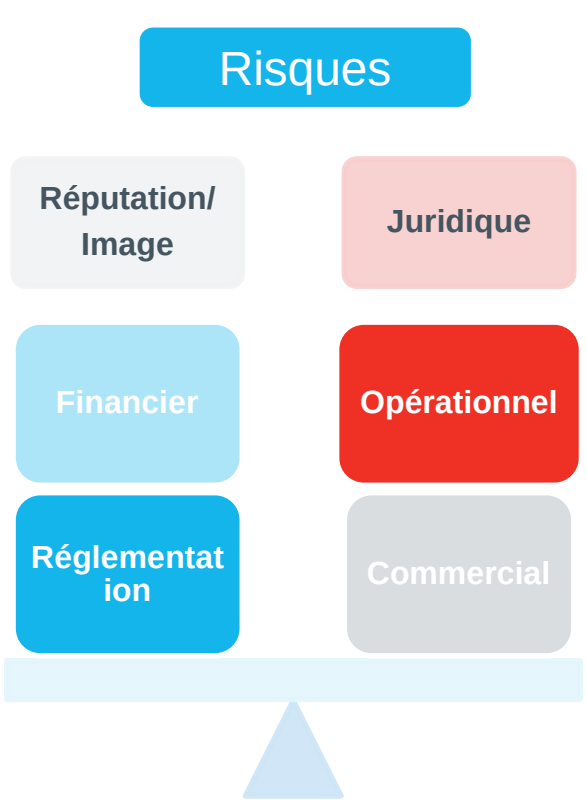
03

Dispositif de prévention de cybersécurité

Approche par les risques pour garantir l’efficacité de l’infrastructure

Dispositif de prévention de cybersécurité

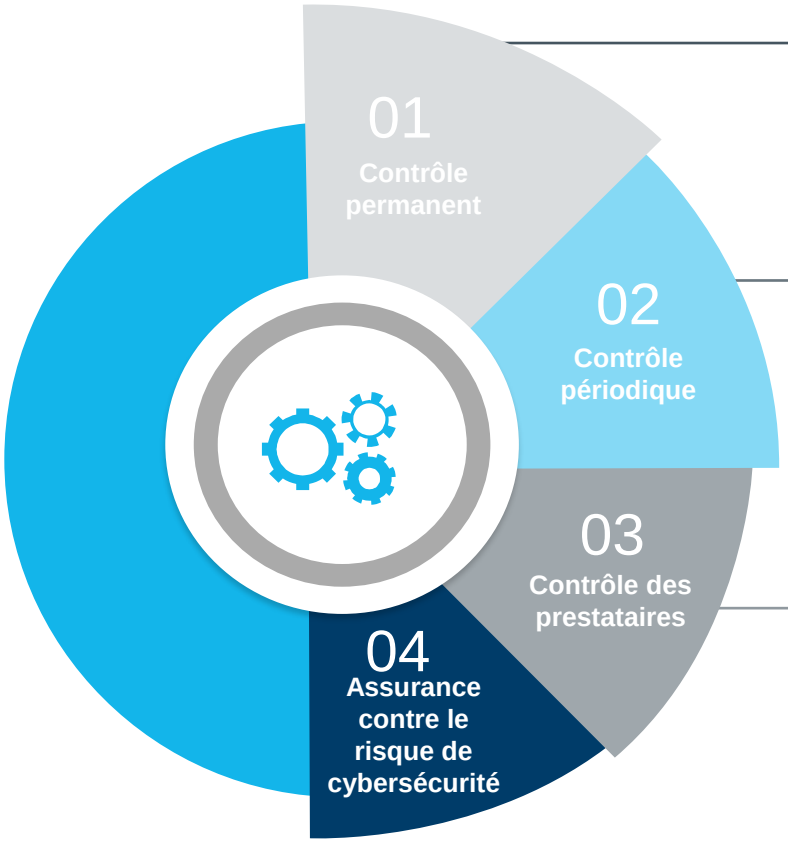
L'identification des risques comme assise du dispositif



Convergence des risques cyber et des risques de la SGP

Dispositif de prévention de cybersécurité

Contrôle du SI sensible et de la cybersecurité



- **Plan de contrôle permanent** effectué par **une fonction dédiée**
- **Communication** des résultats à **l'instance dirigeante**
- Mise en place **d'un plan d'action** global identifiant des **anomalies récurrentes**

- Touchant **la globalité du périmètre de la SGP** afin de mesurer l'efficacité du dispositif de cyber sécurité en place
- Les résultats doivent faire l'objet d'un **plan de remédiation** réalisé par une ressource interne ou un prestataire externe spécialisé

- **Internes et externes** (applications & ressources)
- **Pilotage** par une ressource possédant les **compétences** nécessaires
- Identifier les **prestataires externes sensibles** (passation des ordres, valorisation, gestion du passif) et piloter les prestations
- Rédaction d'une **convention de services avec indicateurs de performance**

Dispositif de prévention de cybersécurité

Une checklist pour la direction

- Identifiez et mettez en place une cartographie des menaces contre votre organisation
- Répertoriez vos actifs critiques et comprenez votre surface d'attaque
- Adoptez un cadre de référence pour organiser votre cybersécurité reconnu
- Établissez une cybergouvernance appropriée, y compris le sponsoring des cadres et managers au niveau du conseil
- Vérifiez l'efficacité des installations informatiques de secours et des restaurations des sauvegardes lors d'une organisation du travail à distance
- Testez et exercez régulièrement vos compétences (y compris votre capacité d'intervention)
- Dressez un plan d'amélioration pour affiner les compétences cybernétiques et faire face aux menaces

04

Notre valeur ajoutée

NOTRE VALEUR AJOUTEE

Duff & Phelps - Des expertises complémentaires

Des experts en conformité

Une expertise reconnue sur la réglementation et sur les sociétés de gestion d'actifs permettant de couvrir les aspects réglementaires

Des experts en cybersécurité

Une équipe experte en cybersécurité permettant de couvrir les aspects techniques relatifs à la cybersécurité

Notre approche unique se base sur une expertise reconnue en matière d'expertise réglementaire et de gouvernance des systèmes d'information et de cybersécurité prenant en compte les risques de votre société pour délivrer une solution unique à votre société et à votre stratégie

Disposant de bureaux dans de nombreux pays en Europe, nos équipes peuvent vous accompagner dans la mise en œuvre de mesures adaptées à toutes les principales juridictions européennes

NOTRE VALEUR AJOUTEE

COVID – 19: Pallier aux défaillances émanant des opérations réalisées en mode dégradé

Objectif : rétablir votre niveau de conformité

La crise de la COVID-19 a exacerbé les cybermenaces, augmentant ainsi la prise de conscience de l'impact de la cybersécurité sur les opérations

En conséquence, l'efficacité de l'infrastructure déployée pour assurer la gouvernance et la sécurité des systèmes d'information et des données est primordiale

Nos solutions pour améliorer votre résilience et vous accompagner dans votre gestion du changement

Procédures

Cartographie des risques
Politiques & Procédures
Formation & Sensibilisation

Dispositif

Installation informatiques de secours
Revue du processus de gestion des violations de données
Cloisonnement du réseau & Système de surveillance

Opérations

Protection des données
Plan de continuité de l'activité
Contrôle du dispositif & des prestataires

Reporting

Rapport au Comité Exécutif

Support conformité réglementaire

DUFF & PHELPS

For more information, please contact:

CAROLINE LEBLANC

Director, Compliance & Regulatory Consulting

Duff & Phelps SAS
4, square Edouard VII
75009 Paris, France
E: caroline.leblanc@duffandphelps.com
T: 01 40 06 40 34
W: www.duffandphelps.com

COLINE PAUL

Vice President, Compliance & Regulatory Consulting

Duff & Phelps SAS
4, square Edouard VII
75009 Paris, France
E: coline.paul@duffandphelps.com
T: 01 40 06 40 38
W: www.duffandphelps.com

ABOUT DUFF & PHELPS

Duff & Phelps is the global advisor that protects, restores and maximizes value for clients in the areas of valuation, corporate finance, investigations, disputes, cyber security, compliance and regulatory matters, and other governance-related issues. We work with clients across diverse sectors, mitigating risk to assets, operations and people. With Kroll, a division of Duff & Phelps since 2018, our firm has nearly 3,500 professionals in 28 countries around the world. For more information, visit www.duffandphelps.com.