Management des SI - Etude de cas Groupe DEV2 – CHONG Jong Hoa

**Partie 1 :** Résumé exécutif.

**Partie 2 :** Une synthèse de vos recommandations au management afin que ces risques soient traités à un niveau acceptable.

**Partie 3 :** Analyse de risque.

**Étape 1 : Identifier les actifs de l’entreprise.**

On peut regrouper les actifs de l’entreprise en plusieurs catégories :

1. Les actifs matériels : Imprim20000, les outils de production.
2. Les actifs immatériels : les licences et brevets associé à l’imprimante par exemple.
3. Les actifs financiers : les ressources financières de l’entreprise.
4. Les actifs humains : les employés et leurs compétences.
5. Les actifs clients : les relations et partenariats de l’entreprise.

**Étape 2 : Identifier la valeur de chaque actif à travers les critères en termes de Disponibilité, Intégrité et Confidentialité. Ces valeurs vont vous permettre ensuite d’établir l’impact sur la société en cas d’exécution d’un scénario à risque.**

En termes de disponibilité, les actifs matériels/immatériels/financiers doivent s’assurer qu’ils sont accessibles de manière fiable à tout moment pour tous les employés. En termes d’intégrité, les actifs financiers/immatériels doivent se protéger contre les fraudes. Pour les actifs matériels, ce sera contre les dégradations. Les 3 actifs doivent se protéger contre l’accès aux personnels non autorisés en termes de confidentialité. La perte de disponibilité peut entraîner des retards ou des arrêts de production. On peut aussi entraîner des erreurs de compatibilité et reporting dans l’intégrité, mais également des fuites d’informations sensibles dans la confidentialité pour les actifs immatériels/financiers. La perte d’intégrité dans les actifs matériels peut amener des coûts de réparation et maintenance pour les dégradations.

Pour les actifs humains, en termes de disponibilité, il faut s’assurer que les employés remplissent bien leurs fonctions correctement à tout moment. L’intégrité est de veiller les personnels soient digne de confiance et qu’ils respectent bien les valeurs et les règles de l’entreprise afin d’éviter une baisse de productivité et de qualité de travail. La confidentialité est de surveiller les informations confidentielles ne soient pas divulguées par ces employés.

Pour les actifs clients, en termes de disponibilité, les informations et services doivent être disponibles et fiable. L’intégrité est de veiller que les informations fournies soient authentiques et des services de qualité. Les informations confidentielles des clients ne soient pas divulguées. La perte de ces critères peut tous entrainer une perte de confiance et de fidélité de la part des clients.

**Étape 3 : Identifier les menaces et les vulnérabilités associées aux actifs**

Pour les actifs financiers :

* Vols de données financières
* Fraudes financières
* Pertes de revenus

Pour les actifs immatériels :

* Perte de la propriété intellectuelle
* Perte de la qualité de l'image de marque
* Perte de la confiance des clients

Pour les actifs matériels :

* Les vols ou les actes de vandalisme
* Les défaillances ou les pannes
* Les cyberattaques

Pour les actifs humains :

* Perte de compétences et de savoir-faire
* Accidents de travail
* Harcèlement ou discriminations

Pour les actifs clients :

* La perte de la loyauté des clients
* Les fuites de données ou les atteintes à la confidentialité
* Les litiges ou les controverses

**Étape 4 : Présenter 2 scénarios de risques combinant les actifs, leurs menaces et leurs vulnérabilités. Identifier la vraisemblance de vos scénarios. (Choisir les scénarios de risque qui vous semblent les plus réalistes).**

**Scénario 1 :** En arrivant dans mon école, on a découvert que 7 ordinateurs ont été volés.

Actifs concernés : Matériels

Menace : Vols ou actes de vandalisme

L’absence de mesures de sécurité adéquates comme un système de surveillance ou verrous de sécurité peut être identifier comme une vulnérabilité.

La vraisemblance est élevée.

**Scénario 2** : L'entreprise est victime d'une attaque informatique ciblée visant à voler des données financières.

Actifs concernés : Financiers et Immatériels (systèmes informatiques)

Menaces : Vol de données financières, attaques informatiques ciblées

Les failles de sécurité dans les systèmes informatiques de l'entreprise, manque de mesures de sécurité pour protéger les données financières peuvent être identifier comme une vulnérabilité.

La vraisemblance est élevée.

**Étape 5 : Réaliser une analyse de risque sur l’entreprise. (Basée sur le fichier Excel vu en cours)**

**Étape 6 : Réaliser une analyse de risque sur la nouvelle imprimante. (Basée sur le fichier Excel vu en cours)**

* Calculer l’EPU (Espérance de Perte Unique)

Chiffre d’affaires par jour : 35 000€

Incidents annuels : 7 (en moyenne)

EPU : 35 000 / 7 = 5000€ par incident.

* Calculer l’EPA (Espérance de Perte Annuelle)

EPU : 5000€ par incident

Incidents annuels : 7 (en moyenne)

EPA : 5000 \* 7 = 35 000€ par an

**(1 pts) Étape 7 : Une échelle des priorités des actions est proposée par la direction. Proposez une échelle de charge de correction et proposer un planning projet afin de suivre la remédiation.**