TP SEC-101

Gestion de risque

Sécurité des actifs de Toshiho lors du déplacement en train de son PDG

Contexte

L'organisation

Toshiho est une multinationale fictive qui se consacre à la fabrication et la distribution de matériel high-tech. L'entreprise est basée à Tokyo et possède des filiales dans de nombreux pays à travers le monde. Les produits de Toshiho incluent des ordinateurs portables, des smartphones, des tablettes et des appareils électroniques grand public. Toshiho est présente sur les 5 continents.

Périmètre de l'étude

Le PDG de Toshiho, M. John Smith, devra effectuer un déplacement professionnel en train entre Paris et Amsterdam afin de rencontrer des partenaires commerciaux. Il sera accompagné de dossiers papiers, de son téléphone portable ainsi que de son ordinateur portable. M. John Smith devra donc transporter des informations confidentielles sur les projets en cours et les stratégies de l'entreprise. **Cette étude se concentrera sur le respect de la sécurité des actifs de Toshio lors du déplacement professionnel en train de son PDG.**

Objectifs

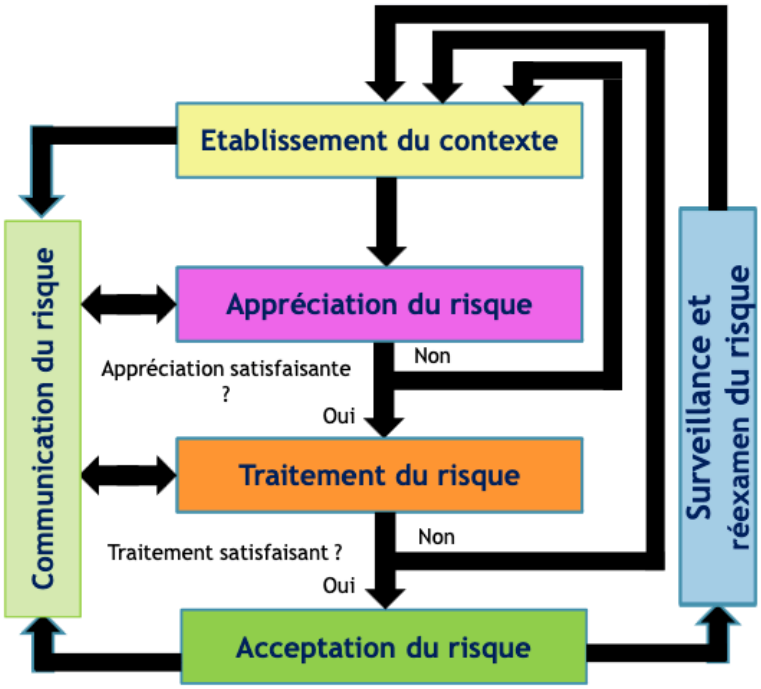
Le PDG de Toshiho est déjà paru dans la presse alors qu'il se rendait en train à des réunions confidentielles. Les agents de sécurité de Toshiho ont déjà dû répondre à des incivilités lors du déplacement en train des membres du bureau exécutif et du PDG de l'entreprise. **L'objectif est donc de garantir la sécurité des actifs de l'entreprises exposés pendant le déplacement en train de son PDG.**

Critères d'acceptabilité

- Les aspects légaux et règlementaires
    - Respecter les contrats de confidentialité avec les clients et fournisseurs
- Les aspects opérationnels
    - Respecter le rendez-vous que le PDG de Toshiho doit effectuer
- Les aspects technologiques
    - Respecter la sécurité des appareils électroniques et des périphériques transportés
- Les aspects financiers
    - Respecter la confidentialité des procédés industriels de Toshiho

Méthodologie

Les menaces et les contre-mesures présentés ci-dessous ont été établies dans dans le cadre de l'élévation continue de la sécurité tel que proposé par les normes ISO 27001 (27002 et 27005).



Acceptation des risques

Les actifs

Actifs primordiaux :

- PDG de Toshiho
- Ordinateur portable
- Téléphone portable

Actifs supports :

- Dossier papier
- Cable USB-C
- Réseau 4G
- Transport ferroviaire
- Agents de sécurité de Toshiho

Critères de valorisation

Niveau de perte	Niveau de disponibilité - D	Perte d'intégrité - I	Perte de confidentialité - C	Impact sur l'activité
0	Toujours disponible	Pas de perte	Pas de perte	Aucun impact
1	< 5min	Faible	Non classifié	Faible
2	5 à 30 min	Moyen	Restreint	Moyen
3	30 min à 1h	Elevé	Confidentiel	Elevé
4	>1h	Fort	Secret	Fort

Valorisation des actifs

Processus	Type	Actif	D	I	C	VB	VS	NP
Déplacement en train du PDG de Toshio	Matériel	Ordinateur portable	3	3	4	10	4	3
		Téléphone portable	3	3	4	10	4	1
		Dossier papier	2	2	4	8	3	1
		Cable USB-C	1	0	4	5	2	1
	Services	Réseau 4G	3	0	4	7	3	1
		Transport féroviaire	4	3	2	9	3	3
	Personnes	Agents de sécurité	4	3	1	8	3	3
		PDG de Toshiho	4	4	4	12	4	4

Valeurs brutes des actifs	Valeurs simplifiées
0 à 2	1
3 à 6	2
7 à 9	3
10 à 12	4

Évaluation du niveau de risque

Actif	VS	NP	Menace	NM	Vulnérabilité	NV	ER	NR
Ordinateur portable	4	2	Vol	4	Fiabilité de l'OS et du chiffrement des disques	3	6	48
			Lecture de l'écran par un tiers	3	Luminosité et angles de vision des dalles IPS	3	5	40
			Attaque physique	2	Insertion d'un périférique compromis	3	4	32
			Attaque par wifi	2	Immitation d'un point d'accès de confiance	3	4	32
			Attaque par bluetooth	2	Failles bluetooth 5.3	3	4	32
			Ecoute par ondes électromagnétique	1	Raisonnance des composants	2	2	16
			Ecoute par ondes sonores du clavier	2	Bruits et latences entre les touches pressés	2	3	24
			Dégradation par un tiers	2	Faiblesse physique / Manque de vigilence	1	2	16
			Chute	4	Manque de protection	1	4	32
			Panne matérielle	2	Fiabilité du matériel	1	2	16
			Panne logicielle	3	Fiabilité des logicielles	1	3	24
			Vol suite à un accident	1	Fiabilité de la compagnie de train	3	3	0
Téléphone portable	4	1	Vol	4	Faiblesse physique / Manque de vigilence / Fiabilité de l'OS et du chiffrement des disques	3	6	24
			Lecture de l'écran par un tiers	3	Luminosité et angles de vision des dalles IPS	3	5	20
			Attaque physique	2	Insertion d'un périférique compromis	3	4	16
			Attaque par wifi	2	Immitation d'un point d'accès de confiance	3	4	16
			Attaque par bluetooth	2	Failles bluetooth 5.3	3	4	16
			Ecoute par ondes électromagnétique	1	Raisonnance des composants	2	2	8
			Ecoute par ondes sonores du clavier	2	Bruits et latences entre les touches pressés	2	3	12
			Dégradation par un tiers	2	Faiblesse physique / Manque de vigilence	1	2	8
			Chute	4	Manque de protection	1	4	16
			Panne matérielle	2	Fiabilité du matériel	1	2	8
			Panne logicielle	3	Fiabilité des logicielles	1	3	12
			Vol suite à un accident	4	Compagnie de train non fiable	3	6	24
Dossier papier	3	1	Vol	4	Faiblesse physique / Manque de vigilence	3	6	18
			Lecture par un tiers	4	Proximité des sièges des passagers / Absence de teinture des wagons	3	6	18
			Perte d'une feuille volante	4	Absence d'attache	2	5	15
			Vol suite à un accident	1	Compagnie de train non fiable	3	3	9
Cable USB-C	1	1	Remplacement par un cable piégé	1	Faiblesse physique / Manque de vigilence	2	2	2
Transport féroviaire	4	3	Ecoute des conversations par un tiers présent	4	Proximité des sièges des passagers	3	6	72
			Ecoute des conversations par un tiers distant	3	Présence de micro étrangers / exploit des micros de la compagnie	2	4	48
			Visibilité de la presence du PDG par un tiers présent	4	Proximité des sièges des passagers / Absence de teinture des wagons	3	6	72
			Visibilité de la présence du PDG par un tiers distant	3	Présence de caméras étrangères / exploit des caméras de la compagnie	2	4	48
			Accident féroviaire	1	Fiabilité de la compagnie de train	2	2	24
			Attaque / détournement du train	1	Faiblesse physique / Fiabilité de la compagnie de train	1	1	12
Agents de sécurité	3	3	Ingénierie sociale	4	Somnolence / Non-respet des procédures de sécurité	3	6	54
			Attaque / enlevement par un tiers	1	Faiblesse physique / Fiabilité de la compagnie de train	1	1	9
PDG de Toshiho	4	4	Ingénierie sociale	4	Somnolence / Non-respet des procédures de sécurité	3	6	96
			Attaque / enlevement par un tiers	1	Attaque / enlevement par un tiers	1	1	16

Niveau de menace	Caractéristique de la menace
1	Menace peu probable
2	Menace probable
3	Menace fréquente
4	Menace très fréquente

Niveau de vulnérabilité	Caractéristique de la vulnérabilité
1	Difficilement exploitable
2	Moyennement exploitable
3	Facilement exploitable

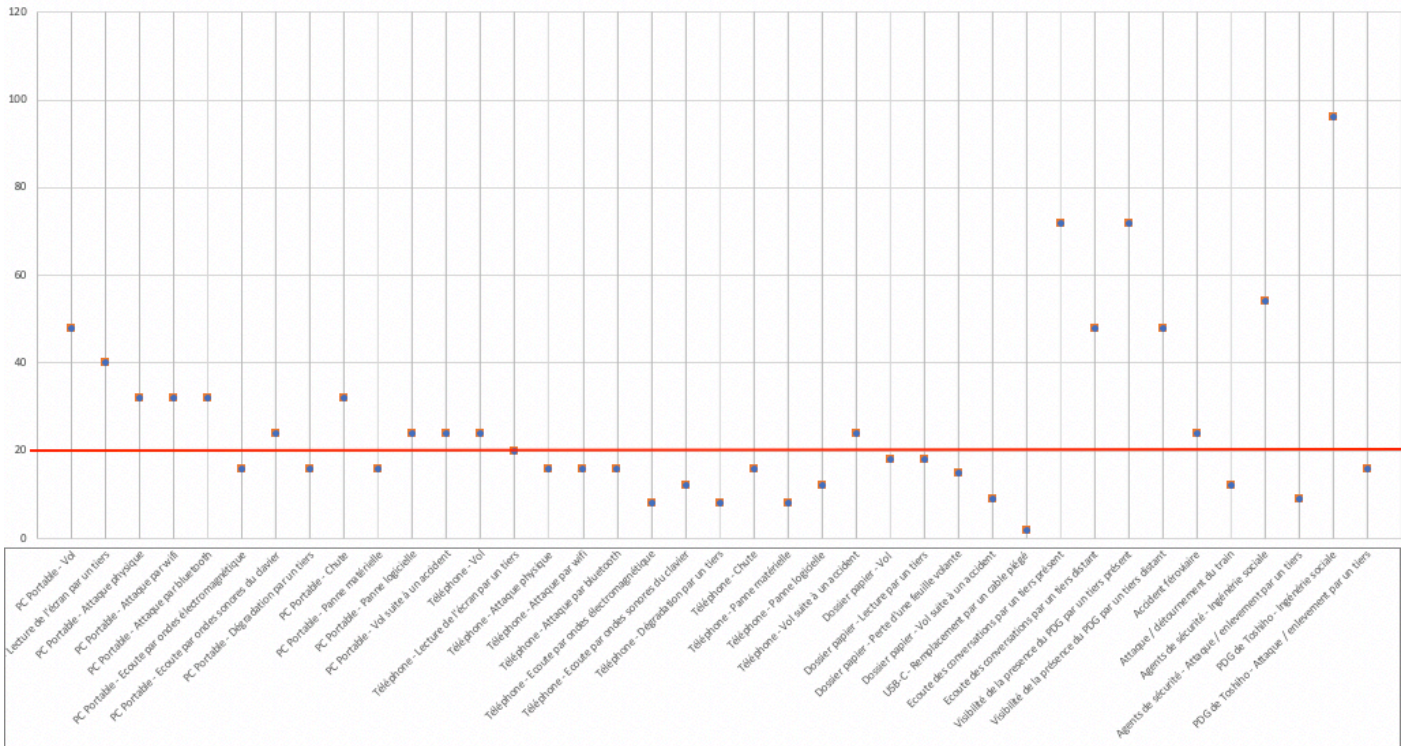
NP	Valorisation
1	Négligable
2	Limitée
3	Importante
4	Critique

$$ER = NM + NV - 1$$

$$NR = NP * ER * VS$$

Traitement du risque

Seuil d'acceptation



Plan de traitement des risques

Actif	Vulnérabilité	Traitement	Mesures	Délais	Coûts	Ressources	Risques résiduels
PC Portable	Vol	Réduction	Chiffrement des partitions pour les analyses à froid; chiffrement des fichiers pour les analyses à chaud	4 jours	€16 300	Main d'œuvre	Evolution des technologies de déchiffrement après un éventuel vol
	Lecture de l'écran par un tiers	Evitement	Placer un filtre opaque devant la dalle LCD	1 jour	€400,00	Filtre opaque	Un tiers peut toujours avoir le bon angle de vision
	Attaque physique	Evitement	Désactiver les ports USB pendant le trajet	2 jour	€300,00	Main d'œuvre	Aucun
	Attaque par wifi	Evitement	Désactiver le wifi pendant le trajet	1 jour	€200,00	Main d'œuvre	Aucun
	Attaque par bluetooth	Evitement	Désactiver le bluetooth pendant le trajet	1 jour	€200,00	Main d'œuvre	Aucun
	Ecoute des ondes sonores du clavier	Evitement	Mise en place d'un clavier virtuel	1 jour	€200,00	Main d'œuvre	Aucun
	Chute	Réduction	Changement de la coque de protection	1 jour	€100,00	Main d'œuvre / Coque de protection	Accident féroviaire
	Panne logicielle	Réduction	Mise à jour de l'OS	2 jours	€100,00	Main d'œuvre	Erreur logicielle
Téléphone	Vol	Réduction	Chiffrement des partitions contre les analyses à froid; chiffrement des fichiers contre les analyses à chaud	2 semaines	€20 000,00	Main d'œuvre	Evolution des technologies de déchiffrement après un éventuel vol
PDG de Toshiho	Ecoute des conversation par un tiers présent	Réduction	Formation	1 jour	€0,00	Main d'œuvre	Erreur humaine
	Ecoute des conversation par un tiers distant	Réduction	Analyse apparofondi en amont de la cabine	1 jour	€2 000,00	Main d'œuvre	Erreur humaine
	Visibilité de la présence du PDG par un tiers présent	Réduction	Port du masque	1 jour	€0,00	Masque	Erreur humaine / Présence de journaliste
	Visibilité de la présence du PDG par un tiers distant	Réduction	Analyse apparofondi en amont de la cabine	1 jour	€4 500,00	Main d'œuvre	Erreur humaine
	Ingénérie sociale	Réduction	Formation	1 jour	€4 000,00	Main d'œuvre	Erreur humaine
Agents de sécurité	Ingénérie sociale	Réduction	Formation	1 semaine	€12 000,00	Main d'œuvre	Erreur humaine

Communication

Les ingénieurs ont paramétrés l'ordinateur et le téléphone portable du PDG. La cabine du train devra être examinée par nos équipes 7h avant le départ du train de son dépôt.

Les agents de sécurité ont suivi une formation de 1 semaine ; dispensé par nos équipes ; afin de s'assurer que les bons réflexes contre l'ingénierie sociale ont bien été compris.