La sécurité du cyberespace Tunisien:
Statistiques, constats et recommandations

Fadhel GHAJATI فاضل غجاتي

Octobre 2018

Plan

- Statistiques cybernétiques
- Tendances cybernétiques
- Mesures appropriées à l'échelle nationale et organisation
- Conclusion

Quelques chiffres en Tunisie

✓ Mobile et Internet (Source : Instance Nationale des Télécommunications, Juin 2018)

- **+ de 14 500 000** mobiles actifs (3 derniers mois),
- **+ de 7 500 000** abonnements mobiles (Wifi, 3G, 4G, …),
- **+ de 890 000** abonnements fixe (ADSL).

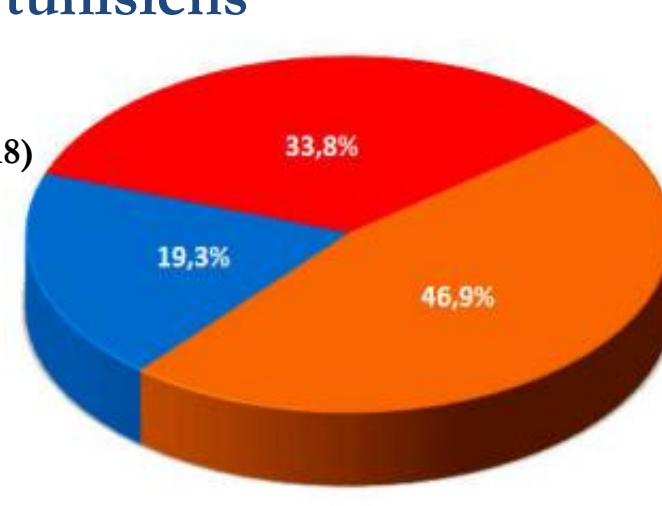
✓ Réseaux sociaux (Facebook) (Source : Etude Webanalytics 2017 de Medianet, Janvier 2018)

7 365 800 utilisateurs Facebook

✓ +40000 noms de domaine .tn

✓ +7000000 @IP sous 16 ASN / +100 DNS tunisiens

Segmentation du marché (Juin 2018)
Clés 3G 4G et ADSL



Statistiques Cybernétiques (Juin – Aout 2018)

- Les cinq BotNet les plus importants (ranomwares, DOS IoT, etc.)

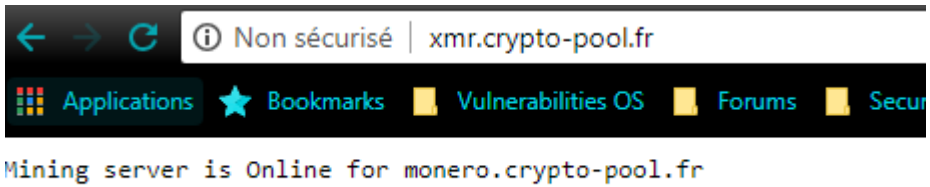
BotNet	Nombre
lethic	76013
sality p2p	45924
mirai	37219
wannacrypt	34439
virut	31306

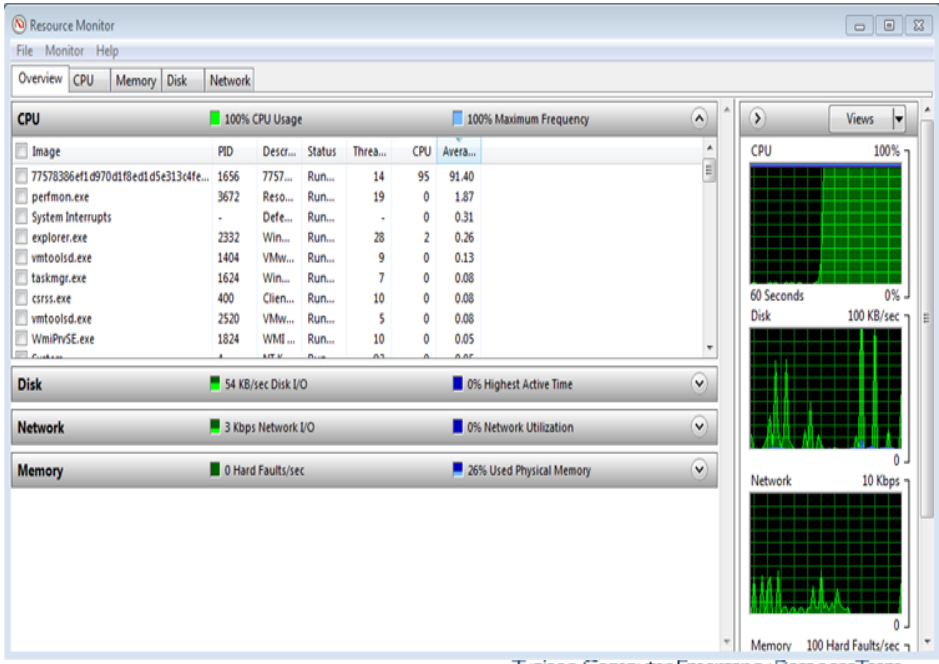
- Répartition

ASN	Nombre
Topnet	96074
Tunisia Backbone AS	84308
Orange Tunisie	51189
OOredoo	42156
ATI	34246
3S INF	13338

Cyberespace national: Tendances

- L'exploitation des vulnérabilités et la faiblesse des serveurs DNS : un catalyseur pour les attaques
- La variété des risques dont les utilisateurs sont exposés avec l'évolution des utilisations et la valeur des monnaies virtuelles (services de mining en Tunisie détectés par SAHER)

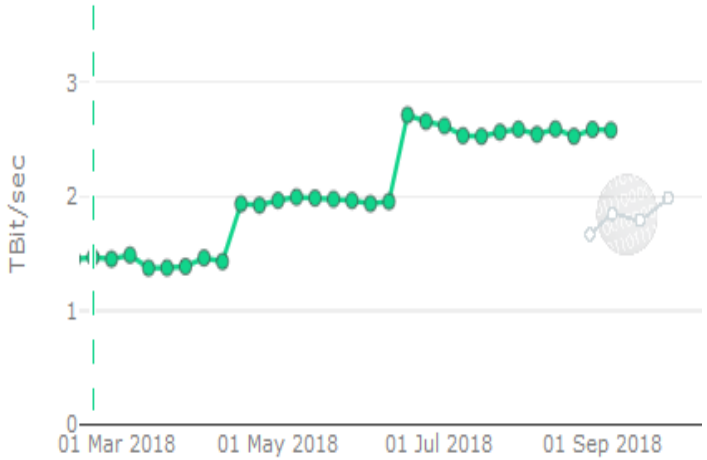




Cyberespace national: Tendances

- Evolution mentionnée dans les utilisations des protocoles SSDP au niveau des routeurs

DDOS | TUNISIA



https://stats.cybergreen.net/country/tunisia/

Behaving

Country	Count
China	628,121
Argentina	288,151
Russia	202,404
South Korea	139,623
Taiwan	96,162
USA	89,452
Italy	60,408
India	56,592
Brazil	54,603
Tunisia	51,178

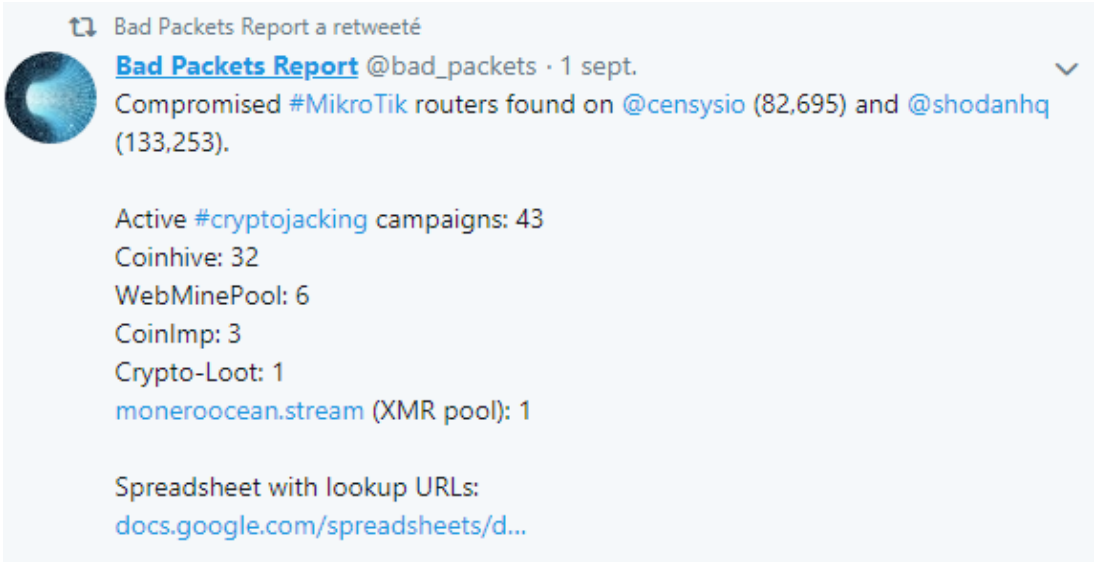
Source Arbor Network Juin

- Réticence de l'utilisation des DNS tunisiens
- Utilisation fréquente des serveurs IBM-Google 8.8.8.8 et 9.9.9.9

Cyberespace national: Tendances

- **Prolifération des cyberattaques:** Après les attaques Mirai (Caméras IP) et Saturi (Modem Huawai), l'apparition des attaques qui ciblent les vulnérabilités au niveau des routeurs pour des fin de crypto-mining

Aout 2008, une attaque visait le Brésil où les hackers ont réussi à pirater environ 7.200 routeurs de MikroTiK



HAKAI Botnet : un botnet découvert par Ahmed Jouini, ingénieur cybersécurité à l'ANSI

Security researcher Jouini Ahmed noted that Hakai had expanded its initial Huawei exploit to also include exploits that targeted D-Link routers supporting the HNAP protocol, but also Realtek routers and IoT devices that were using an older and vulnerable version of the Realtek SDK. Anubhav also told *ZDNet* that as Hakai matured, it also broadened its capabilities with two more D-Link router exploits [1, 2].

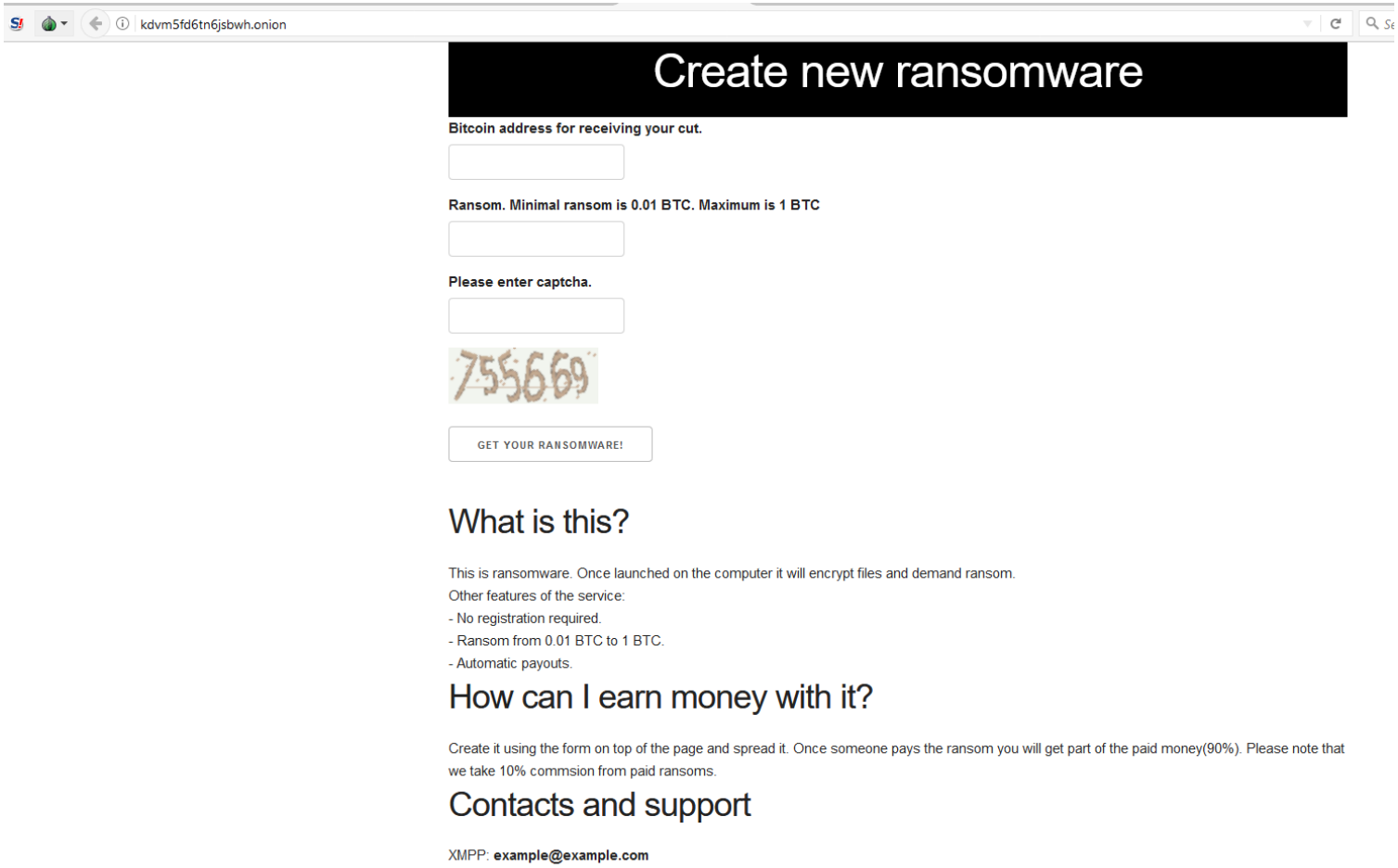
ZDNet

Around 62 percent of all Internet sites wil run an unsupported PHP version in 10 weeks

The highly popular PHP 5.x branch will stop receiving security updates at the end of the year.

Cyberespace national: Tendances

- Ransomware as service

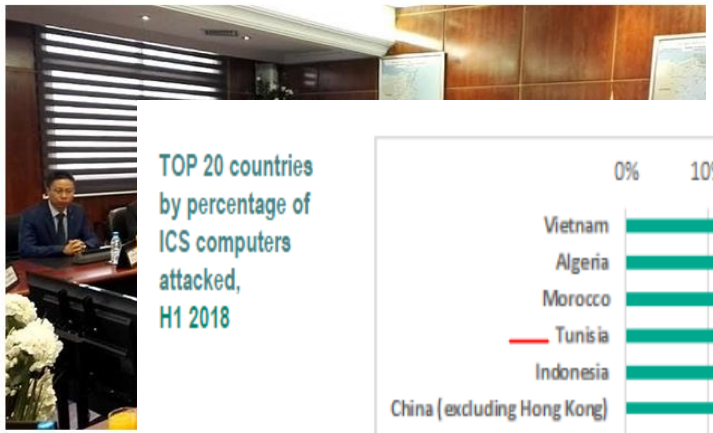


Cyberespace national: Tendances

Electricité : Huawei et Steg ont réussi la mise en place du projet Smart Grid

31 Mar 2017 | 10:58 ECONOMIE, Tunisie

12



La Steg se félicite de la r
collaboration avec Huaw

Une cérémonie de démons
tunisienne d'électricité et d
tenue récemment au siège
l'Energie, des Mines et des
Afrique du Nord, et Saeed
de cette opération.

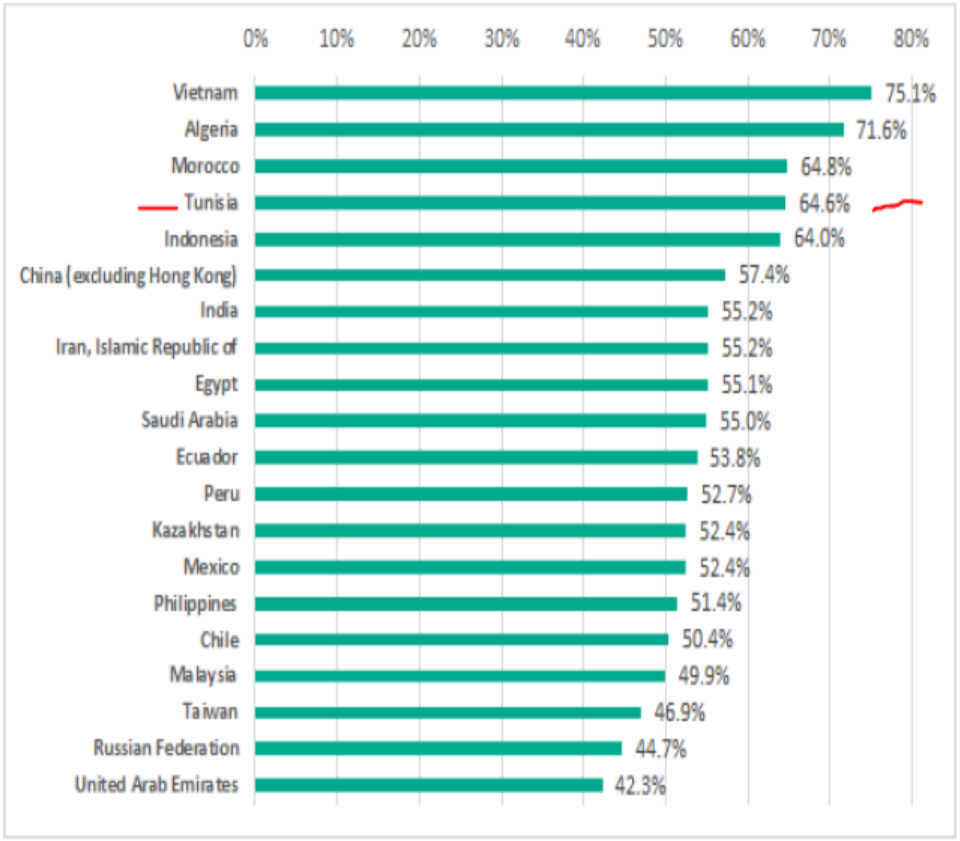
- Projet SMART GRID

lu mining

é ICS et

A

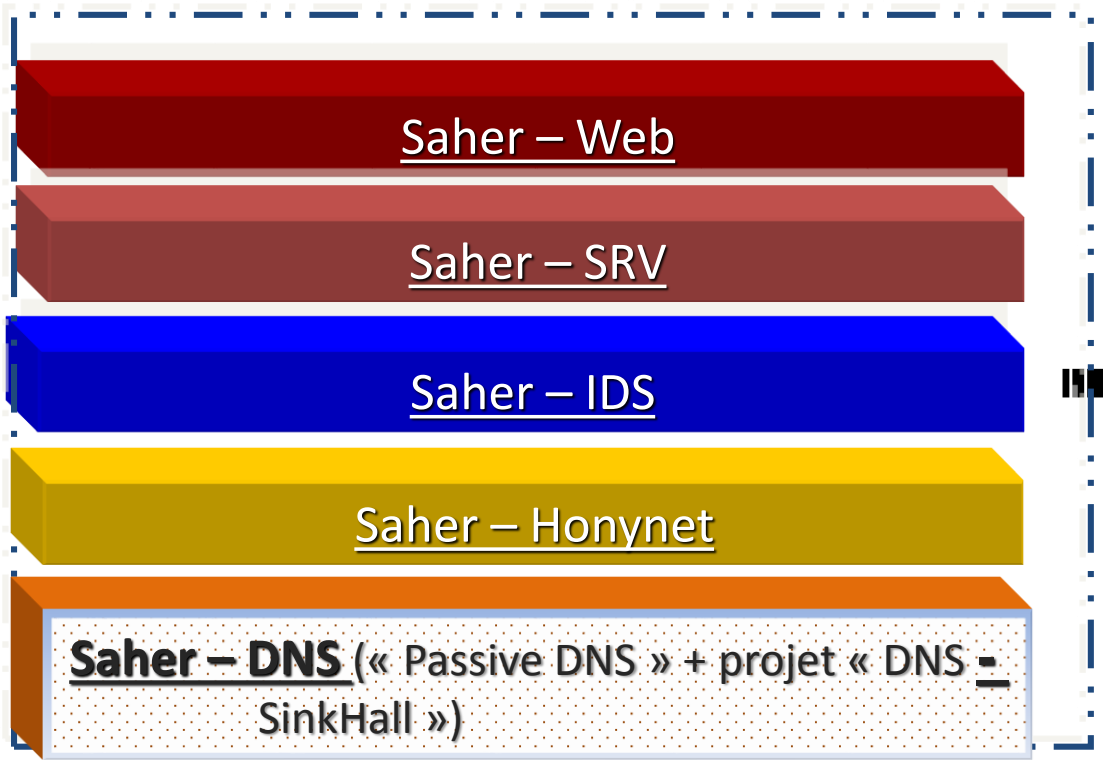
TOP 20 countries by percentage of ICS computers attacked, H1 2018



Kaspersky

tunCERT
Tunisian Computer Emergency ResponseTeam

La nécessité de la généralisation de la plateforme SAHER



- Webdefacement
- DoS
- Intrusion
- Etc.

Mesures organisationnelles

La direction doit faire preuve de **leadership** et affirmer son engagement en faveur de la protection de l'information

Mesures organisationnelles

Etablir une politique de sécurité de l'information

La politique de sécurité de l'information doit être:

disponible sous forme d'information documentée;

communiquée au sein de l'organisation;

mise à la disposition des parties intéressées,

Mesures organisationnelles

Désigner qui a la responsabilité et l'autorité de s'assurer de la sécurité de l'information

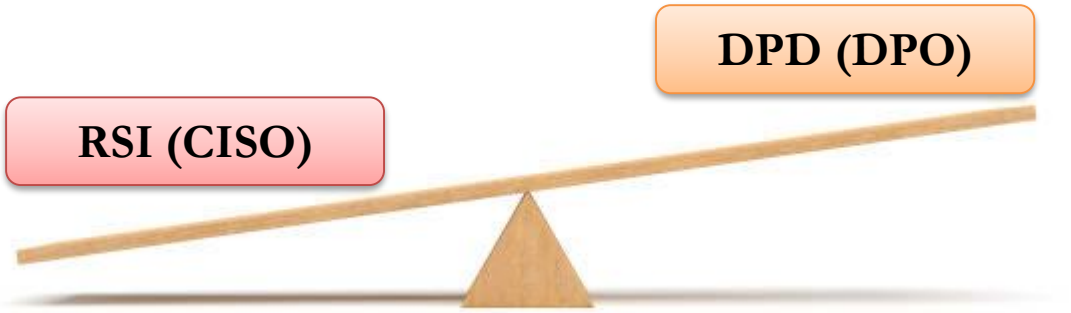
- RSI (CISO)

- RGPD → DPD (DPO)

Mesures organisationnelles

RSI & DPO doivent collaborer

Synergies



Réglementations

Loi de protection des DCP

ISO 27018

ISO 27001

Obligation de l'audit

Référentiels

PCI-DSS

Mesures organisationnelles

Définir et appliquer un processus d'appréciation des risques de sécurité de l'information

Etablir et tenir à jour les critères de risque de sécurité de l'information incluant

- les critères d'acceptation des risques;
- les critères de réalisation des appréciations des risques de sécurité de l'information

S'assurer que la répétition de ces appréciations des risques produit des résultats cohérents, valides et comparables

La méthodologie d'appréciation des risques

Identifier les risques de sécurité de l'information

Analyser les risques de sécurité de l'information

Evaluer les risques de sécurité de l'information

Mesures organisationnelles

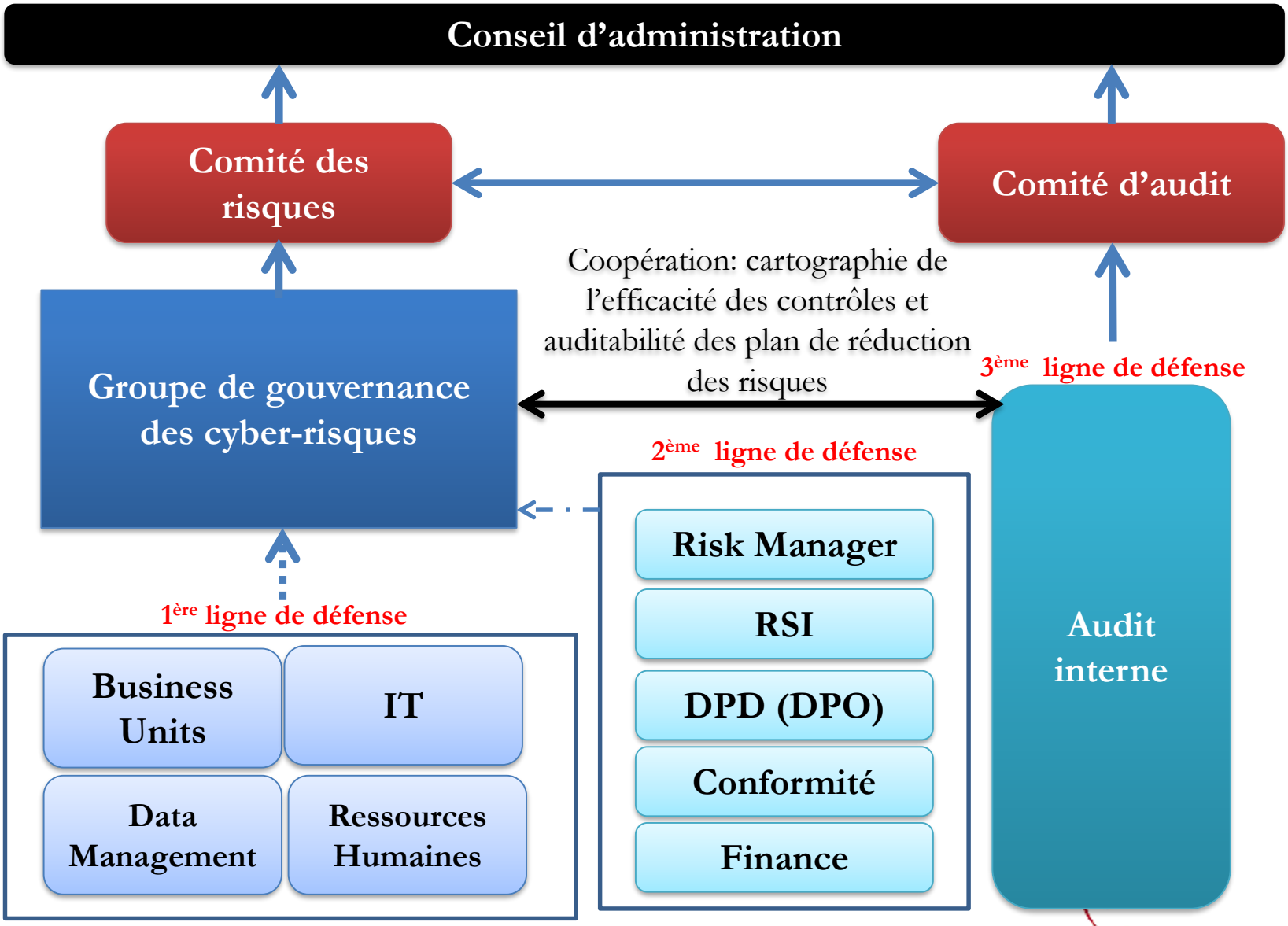
Définir et appliquer un processus de traitement de risque de sécurité de l'information

Choisir les options de traitement des risques appropriées, en tenant compte des résultats de l'appréciation des risques

Déterminer toutes les mesures nécessaires à la mise en œuvre de l'option de traitement des risques de sécurité de l'information choisie;

Elaborer un plan de traitement des risques de sécurité de l'information

Cybergouvernance

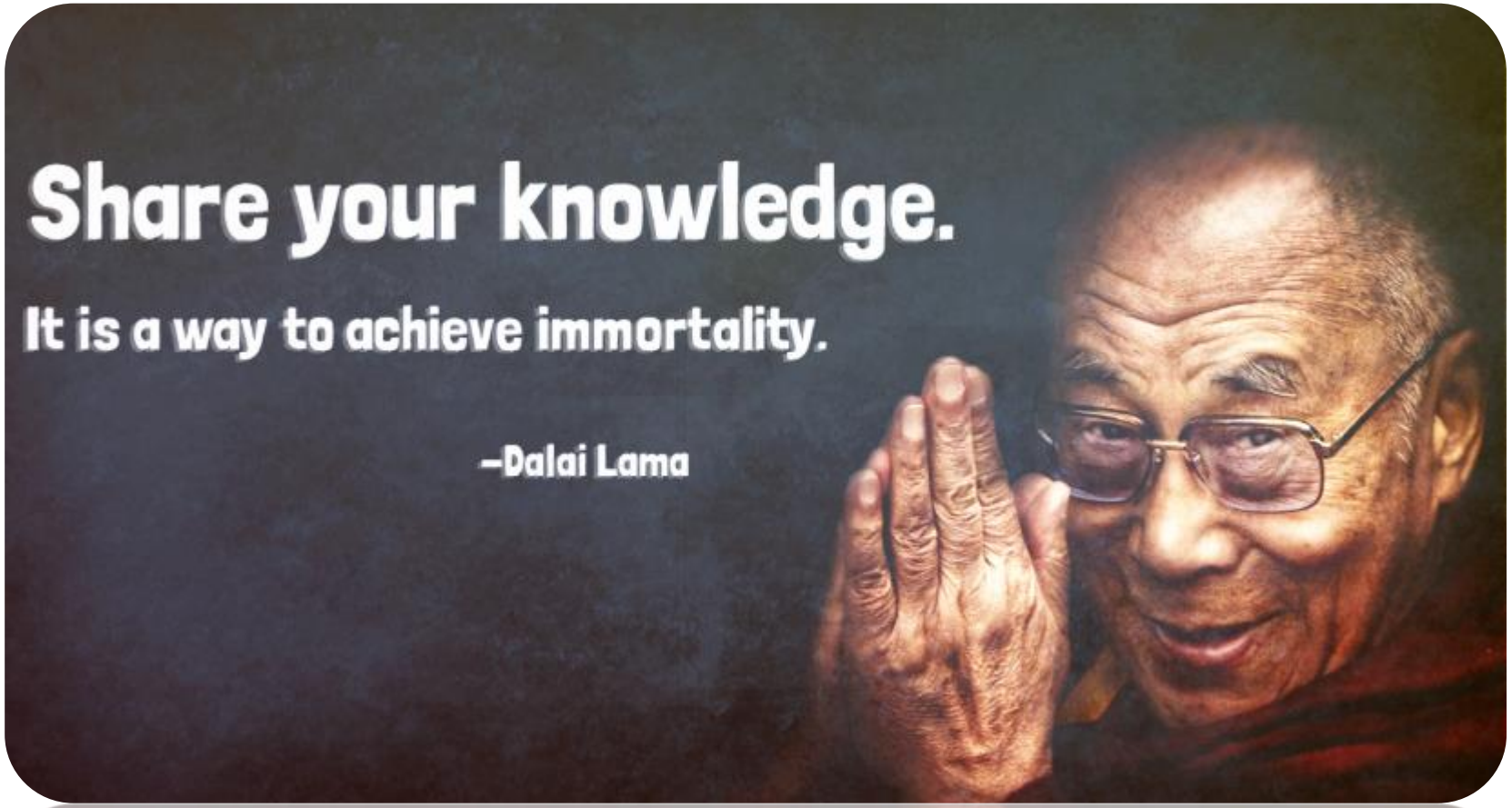


Conclusion

- Engagement du leadership
- Politiques de sécurité de l'information
- Formation et sensibilisation
- Attribution de rôle et d'autorité
- Processus d'appréciation des risques
- Processeurs de traitement de risque

- Classification
- Appréciation des risques
- Traitement des risques
- Application des mesures techniques,
- Sécurité phsyique
- Contrôle d'accès
- Chiffrement
- Journalisation
- Sauvegarde…

Gestion opérationnelle de la protection des données


Share your knowledge.
It is a way to achieve immortality.
–Dalai Lama