

Sécurité & Continuité des affaires des disciplines Convergentes

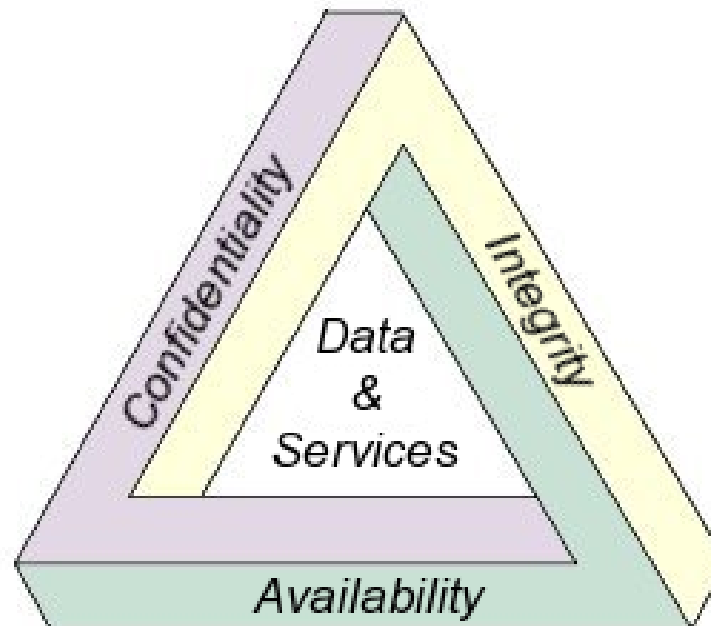


Gilles Lavoie – CPP, CBCP, CISSP
Aviser Principal Développement des programmes
Rio Tinto ALCAN

Présentation originale de Steve Hauser - PE, CBCP, CISSP
Manager, Business Continuity Services – SAIC

Partager de mêmes valeurs

Les professionnels en Sécurité de l'Information et de la Continuité des affaires ont toujours partagé les mêmes valeurs quant à la disponibilité (Availability) des données (*Le vertex "A" du triangle CIA - Confidentialité, Intégrité, Availability (Disponibilité) - de la sécurité de l'information*).



Partager de mêmes valeurs (suite)

De nos jours, comme les données deviennent de plus en plus accessibles, plus mobiles, plus ponctuelles, donc plus valables, les professionnels de la sécurité physique, de la sécurité de l'information et de la continuité des affaires trouvent de plus en plus de points communs quant à la confidentialité et l'intégrité des données.

Partager de mêmes valeurs (suite)

Un vol matériel est-il un incident de continuité des affaires , de sûreté ou de gestion de crise?

- Ordinateur portable
- Clef USB contenant de la propriété intellectuelle, des données client ou de l'information sur les employés.
- Est-ce qu'un ouragan représente une menace à la sécurité?
 - ❑ C'est le cas si dans l'accalmie suivant la tempête on découvre que des informations vitales devenues vulnérables ont été perdues ou volées.

Cette présentation vous fournira des idées sur la tendance grandissante d'intégrer et maximiser les approches de sécurité physique, sécurité de l'information, des efforts et ressources des architectures et de la continuité des affaires pour atteindre des buts plus étoffés de mitigation des risques recherchés par toutes les disciplines

Qu'est-ce que la convergence et pourquoi?

Converger, verbe, (*verbe*) – *utilisé sans objet* - tendre vers un résultat commun, une conclusion, etc. (*Synonymes*) approche, focus, réunion

Dictionary.com Unabridged (v 1.0.1)

- La “fusion” d’entités ou “phénomène”
- Traditionnellement entre les modèles sécurité physique et Sécurité TI
ASIS Study “Convergence of Enterprise Organizations” (2005)
- Pour être plus efficaces nous avons besoin d’avoir une vue plus large du “risque”:
 - La Sécurité physique implique les 3 “G’s” (Guns, Guards, and Gates)
 - La Sécurité TI implique les logiciels néfastes, les pirates, les initiés, les systèmes et les données
 - Pour les professionnels de la Continuité des affaires, les arrêts des processus d’affaires (Tremblement de terre, ouragan, feu, terrorisme, etc) sont leur préoccupation commune.
- Afin d’améliorer notre capacité de faire plus avec moins, nous devons incorporer un nouveau paradigme global de la gestion des risques sous le parapluie de la continuité des affaires.



Exemples de Convergence

Le partenariat au niveau des associations dans notre domaine – a eu pour résultat une adhésion combinée de plus que 90 000 personnes.



Des exemples...

1^{er} exemple

Un incident récent à la Banque Sumitomo Mitsui à Londres en Angleterre, au cours duquel des pirates informatiques ont tenté de dérober **£220 million de la banque**, met l'emphasis sur ce principe.

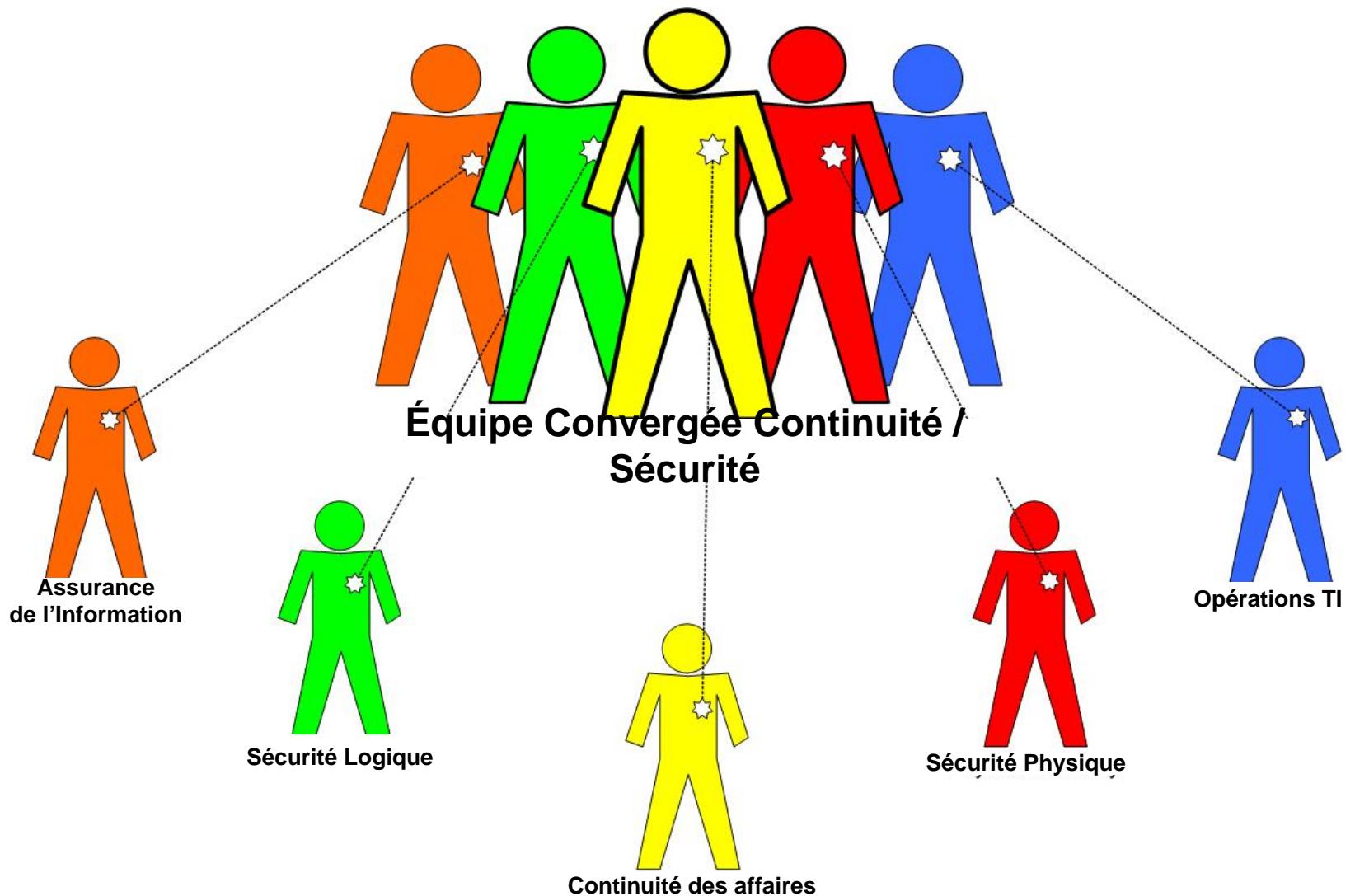
Quoique la banque avait **de solides mesures de sécurité des technologies de l'information (TI)** en place, une **défaillance au niveau de la sécurité physique** s'est produite...

- ❑ *Les « adversaires », déguisés comme préposés au nettoyage un pu installer des dispositifs (key loggers) sur les claviers qui leur ont permis d'obtenir les informations vitales lors du « log in ».*

2^e exemple - Film Firewall



Exemple d'équipes convergentes



Qu'est-ce que la convergence?

- La convergence EST la coopération formelle entre des fonctions auparavant incohérentes.
- La convergence N'EST PAS nécessairement de fusionner les groupes de Sécurité, de Continuité des Affaires, et autres groupes impliqués dans un organigramme
- Les efforts de convergence ont du succès lorsque basés sur la coopération de deux entités uniques ou plus.
- Travailler ensemble profite à tous les participants en créant des efficiences par une plus grande force et des nombres plus grands (*ressources regroupées ou empruntées avec effet de levier*)



Qu'est-ce qui amène tant d'efforts de convergence?

Les efforts de convergence sont normalement issus de:

- L'expansion rapide de l'écosystème de l'Entreprise
- La valeur de migration des actifs physiques vers des actifs basés sur l'information et intangibles.
- De nouvelles technologies de protection rendant floues les frontières fonctionnelles
- Nouvelles contraintes de conformité et de gouvernance
- Pressions permanentes pour réduire les coûts.

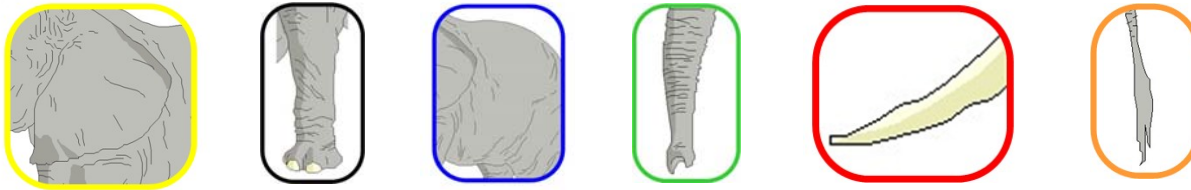
ASIS Study "Convergence of Enterprise Organizations" (2005)



Que demande la convergence?

Une convergence réussie requiert les choses suivantes:

- Partage d'information et coopération
 - Amener des membres d'équipe convergée ensemble, les réunir au sein d'une mission stratégique commune.
 - Disciplines uniques avec des vues différentes du même "animal"



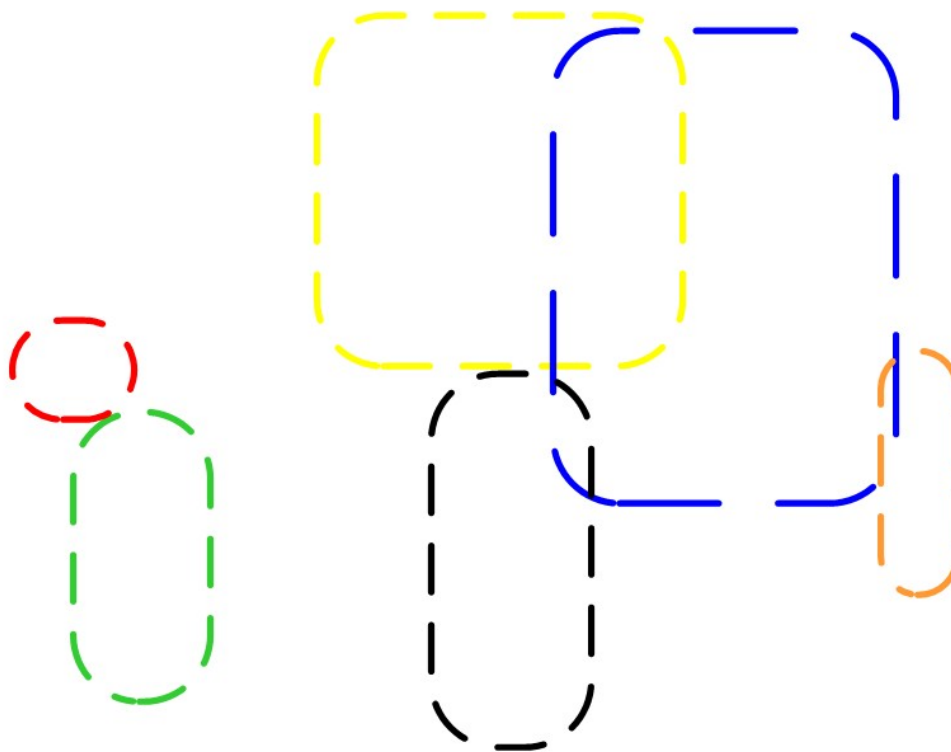
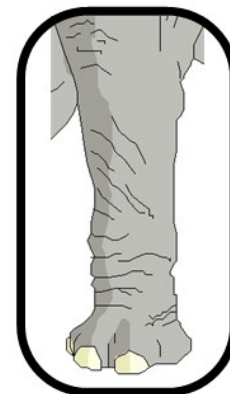
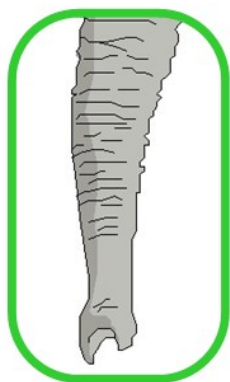
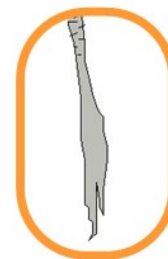
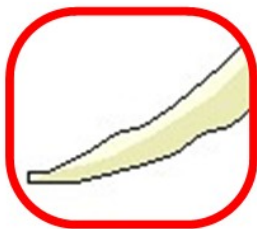
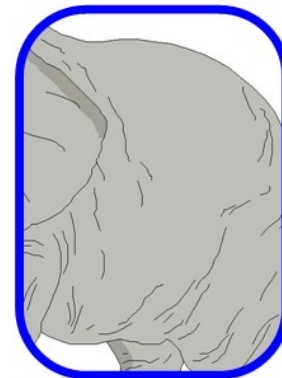
- Soutien de la direction envers des RSI (ROI) établis et répartis
- Coopération entre groupes qui traditionnellement ciblaient des parties spécifiques d'un plus grand ensemble
- Une entente et une volonté d'englober plus grand.



Perceptions restreintes

Une vieille fable indienne

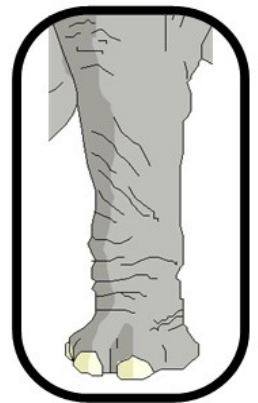
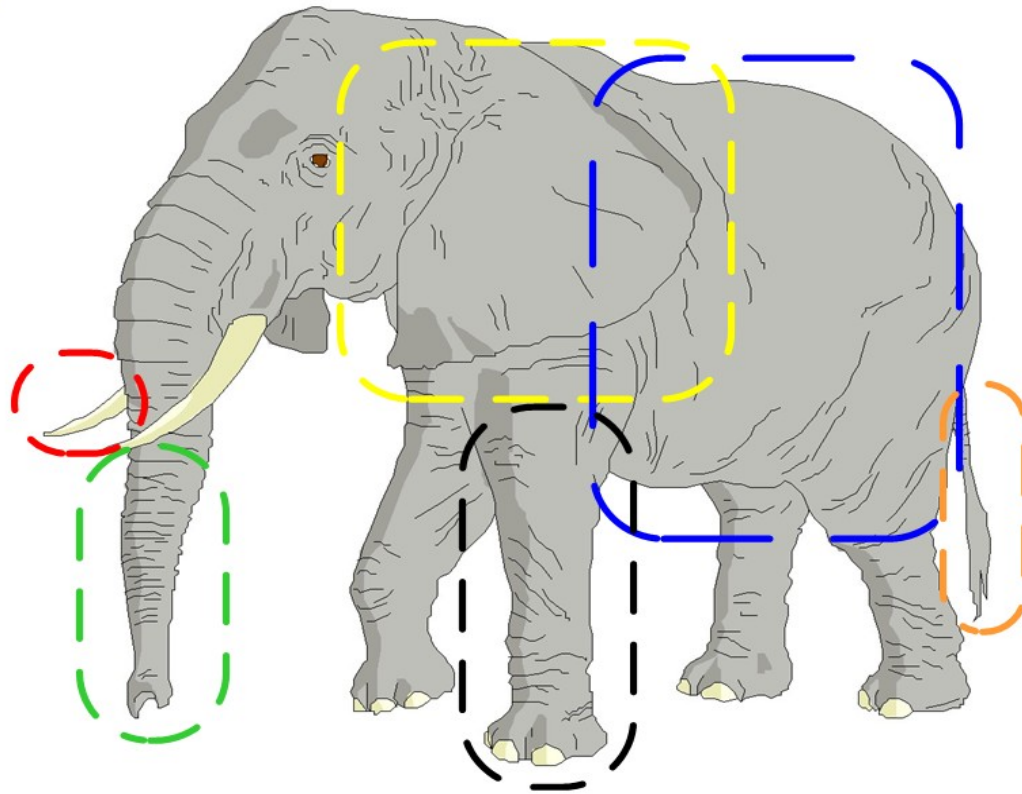
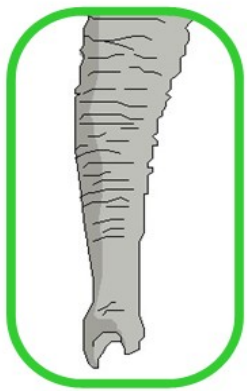
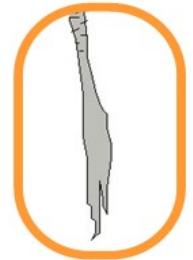
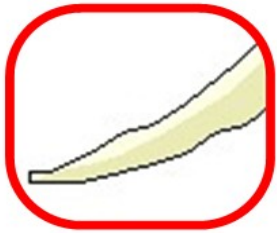
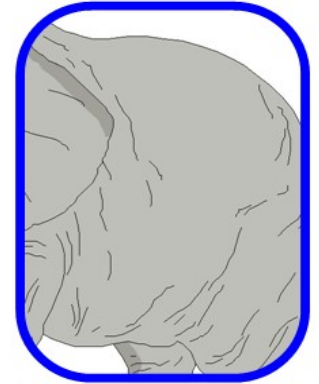
Est-ce que chaque
perception est la même?



Perceptions améliorées

Ce qui est vu communément...

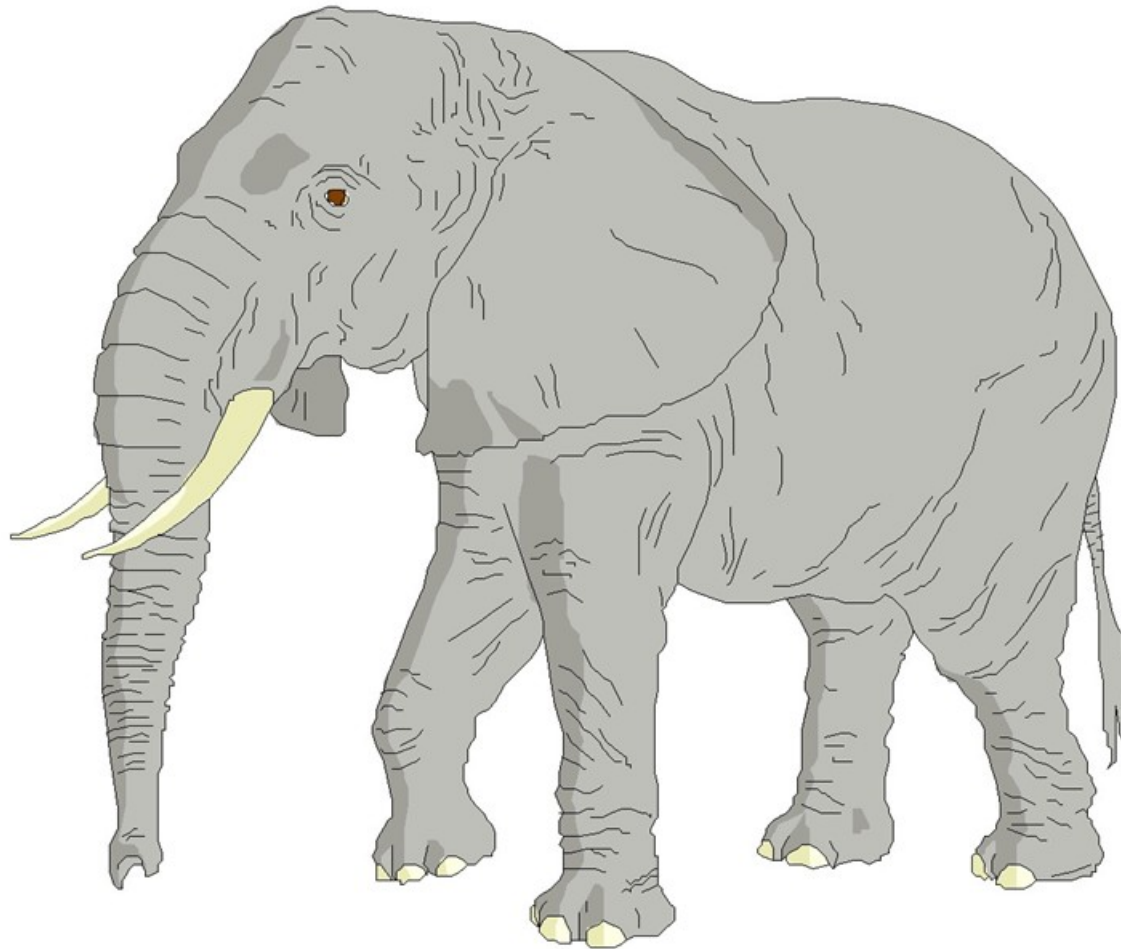
Est seulement partie de toute l'image



Une perception complète

De très près il est facile de manquer...

Tout l'éléphant au lieu que seulement des parties de l'éléphant



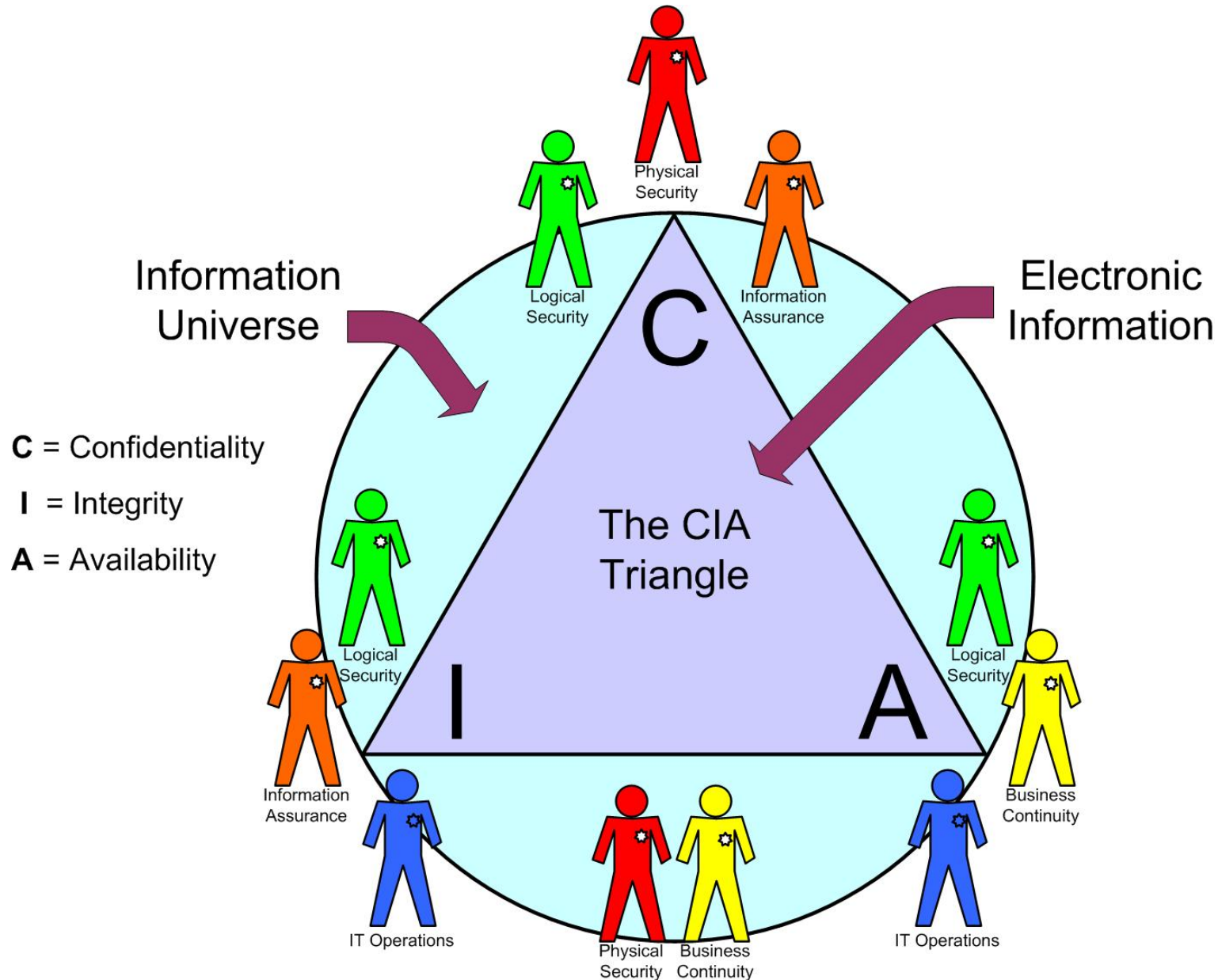
Les bénéfices évidents de la convergence?

L'utilisation de tactiques de convergence peut résulter en:

- Aborder le risque plus efficacement
 - Les professionnels de la Sécurité et de la continuité sont confrontés avec le défi de capter et garder l'attention de la direction sur des points affectant les deux disciplines
 - Utiliser la continuité des affaires comme "parapluie" pour identifier et catégoriser le risque
- RSI (ROI) amélioré donc résilience d'affaires améliorée
 - La continuité ce n'est plus juste les tremblements de terre, les ouragans et l'incendie. Nous appliquons maintenant la même discipline de planification contre les bris de sécurité, les attaques virales, et les menaces à l'interne qui peuvent être aussi dommageables que les désastres
 - En combinant nos objectifs, nous générons des bénéfices d'économie d'échelle



Domaines d'intérêts traditionnels



Buts premiers de la Convergence

Les programmes de risques convergés doivent tendre vers:

- Améliorer l'identification des risques
 - Les approches multidisciplinaires amèneront une vue plus complète de l'environnement réel du risque
 - Former des disciplines connexes à reconnaître un plus grand éventail de risque est comme de déployer plus de policiers dans la rue
- Quantifier le plein potentiel d'impact des risques identifiés
 - Les approches uni-disciplinaires ne savent pas ce qu'ils ne connaissent pas et peuvent banaliser le vrai potentiel d'une menace donnée
- Découvrir et classifier des vulnérabilités jusque là inconnues
 - La collaboration d'enquête peut amener à des découvertes "analytiques" et est partie prenante de garder l'initiative / se garder à niveau avec "les mauvais gars"



Buts et objectifs communs

Les professionnels de la continuité et de la sécurité poursuivent tous:

- Des solutions pour prévenir la perte d'information (incluant le vol, les défaillances de systèmes, la destruction, et la corruption de l'information - négligente, frauduleuse, ou accidentelle).
- Mettant en oeuvre des pratiques standard envers l'assurance de l'information dans un programme complet des données vitales (incluant la sauvegarde des données, la restauration et le recouvrement, le contrôle des accès, la classification des données, l'archivage, et le retrait).
- Mettant en oeuvre des pratiques complètes sur la sécurité des données (incluant archives papier, information classifiée, dépôt des données électroniques stagnantes, transferts électroniques des données, et médias portatifs / mobiles).
- Capacité de réponse rapide face aux menaces (incluant des événements naturels ou induits par l'homme de magnitude et durée variées).



Comprendre les risques

Les professionnels de la continuité sont aguerris dans:

- Les analyses d'impact d'affaires / Gestion de crise
 - Les professionnels de la continuité étudient, évaluent et planifient les actions de mitigation du risque/menace afin de minimiser le potentiel des impacts de la disruption des affaires sur les opérations
 - Les gestionnaires d'urgences prennent part à une préparation proactive de gestion de crise et de réallocation des ressources



Comprendre les risques (suite)

Les professionnels de la sécurité sont aguerris dans :

- La prévention, le suivi et l'enquête / réponse
 - Les professionnels de la sécurité conçoivent et font le suivi du filtrage, de la surveillance et des processus qui contrôlent l'environnement
 - Le personnel de la sécurité exécute des actions en réponse à des crises et effectue des activités de réduction des dommages et d'évaluation.

Confidentialité de l'information

Pour le professionnel de la sécurité cela veut dire:

- Protéger l'information/données d'être vues, utilisées ou altérées par ceux qui n'ont pas reçu la permission de le faire (i.e. contrôle des accès)

Pour le professionnel de la continuité cela veut dire:

- Empêcher que l'information confidentielle soit perdue, volée ou autrement exposée et donc exploitée d'une façon qui nuirait la capacité opérationnelle immédiate de l'organisation ou sa capacité future de faire des affaires (i.e. évitement du risque/menace)

Chaque groupe a le même but – garder l' information confidentielle – ils voient juste leurs missions de perspectives différentes.



Intégrité de l'information

Pour le professionnel de la continuité cela veut dire:

- Que l'information requise pour les affaires est fiable et précise à la fois avant, pendant et après qu'un événement significatif soit arrivé (incluant les infos nécessaires au recouvrement et la restauration des systèmes, des fonctions et services vitaux)

Pour le professionnel de la sécurité cela veut dire:

- Que l'information peut seulement être modifiée par ceux qui sont autorisés de le faire et que ceux qui ont la permission de créer ou modifier des données doivent conspirer avec d'autres et non pas agir seuls pour commettre toute fraude (i.e. séparation des responsabilités et donner le moins de privilèges)

Là encore, chaque groupe poursuit le même but – protégeant l'information de la compagnie de la corruption délibérée ou accidentelle



Disponibilité de l'information

Pour le professionnel de la sécurité cela veut dire:

- Que l'information ne devient pas inaccessible et résulte en une interruption des affaires courantes résultant de la négligence ou d'un plan conçu (i.e. vol, attaques de déni de service, etc.)

Pour le professionnel de la continuité cela veut dire:

- Que l'information nécessaire pour conduire les affaires tel que nécessaire - afin de prévenir soit des pertes opérationnelles ou des pertes d'opportunités - est accessible et utilisable peu importe lorsqu'elle est requise (selon les analyses de l'AIA [BIA]).

Garder les systèmes d'information opérationnels et accessibles est le but commun – la seule différence tient du fait que chaque groupe se concentre contre différentes menaces qui impactent la disponibilité.



Autres bénéfices de la convergence?

La convergence peut aussi amener:

- De meilleures AIA/BIA et analyses de vulnérabilité
 - L'équipe de sécurité se concentre sur les vulnérabilités d'une compagnie et ses opérations. Joindre les requêtes de continuité avec une revue de sécurité combinera tous les facteurs de risques tangibles qui sont le plus susceptibles de se produire dans cette organisation.
- Plus grande connaissance / Comprendre le risque
 - Avec le partage d'information entre les groupes, les professionnels de la continuité accroissent leur connaissance des menaces quotidiennes, alors que les professionnels de la sécurité augmentent leur compréhension sur le fait que les préparatifs de continuité des affaires aident à minimiser les impacts potentiels et le risque d'escalade lors d'événements significatifs.



Bénéfices nets pour la compagnie?

Pour être valable, la convergence doit:

- Épargner de l'argent
 - Les projets qui bénéficient à plus d'un groupe peuvent aisément être perçus comme étant plus rentables
 - Formation croisée du personnel dans des disciplines connexes
 - Augmentation du niveau de sensibilisation aux risques sans augmentation d'effectifs.
- Réponse rationalisée aux événements/Versatilité du personnel
 - Avec le partage d'information et la coopération entre le personnel, la réponse aux événements imprévisibles devrait être plus fluide et plus structurée.
 - La connaissance plus à fond des menaces combinées est accrue/étendue.
 - Une seule vue globale du même "animal" (consistance).



Sommaire des bénéfices de la convergence



Le partage de l'information amène une compréhension plus universelle des risques, des menaces et des mitigations requises.



Adoption par l'exécutif à l'usage d'une approche convergée augmente la probabilité de soutien et d'approbations



Une voix plus forte est créée lorsque les membres d'une équipe convergée ne font qu'un lors des discussions relatives à des initiatives communes.



RSI amélioré résultera en une division des coûts de mitigation et des programmes communs sur une base de bénéfices élargie



Les économies sont le premier avantage de tout effort de convergence qui peut être ensuite utilisé envers de nouvelles initiatives



Réponses rationalisées aux événements seront le fruit d'une meilleure coordination, moins de chevauchements/brèches et une plus grande efficacité



Meilleures AIA/BIA et analyses de vulnérabilités sont possibles à travers les aptitudes analytiques d'équipes combinées.



Plus grande connaissance / Compréhension du focus de chacune des disciplines des partenaires génère une plus grande versatilité des participants



Réduire ou éliminer les conflits sectaires et/ou « les balles échappées » entre des groupes de travail s'ils travaillent côte-à-côte.

La gouvernance de la convergence

Les conseils de gouvernance TI et Sécurité globale peuvent:

- Réviser de nouveaux projets pour des bénéfices combinés (des exemples)
 - Est-ce qu'un nouveau système de notification de masse pourrait être élargi pour faire plus qu'émettre des avis d'urgence? Peut-il être utilisé pour une réponse interne aux incidents et/ou informer les clients?
 - Est-ce que les mises à niveau proposées du système des RH peuvent être adaptées pour aider aux besoins de soutien aux opérations d'urgence et besoins de décompte du personnel en situation d'urgence?
- Les représentants sécurité physique/TI et Continuité peuvent "se couvrir".
 - Les "Yeux et Oreilles" convergées peuvent surveiller de plus grandes portions de la toujours-changeante entreprise pour garder les disciplines concernées au courant de changements pouvant affecter un partenaire de convergence.
 - Les représentants d'équipes convergées peuvent obtenir une voie plus forte à la table des besoins lorsque des critères d'architecture sont établis.



Meilleures pratiques émergentes

Utilisez la fonction d'assurance de l'information comme point central (Hub)

- Utilisez comme levier les mandats de conformité légale
 - La pratique opérationnelle et les critères de performance affectant un membre de l'équipe de convergence aura sans doute des répercussions sur d'autres membres de l'équipe. En travaillant ensemble sur des projets de conformité améliore les chances de succès et de disponibilité des ressources requises
 - Les meilleures pratiques émergentes pour l'Assurance de l'Information tels que FISMA (Federal Information Security Management Act) sur les lignes directrices de conformité font un excellent point de départ pour lancer un programme de convergence
- Déployez une équipe d'analyse de vulnérabilité couvrant tous les risques
 - Incorporer les experts (*SMEs*) en sécurité physique, la sécurité TI, de continuité, d'assurance de l'information, des Opérations TI et des opérations d'urgence au sein de l'équipe



Sommaire des opportunités intégrées

Là où des nouvelles équipes convergées peuvent être testées.

- Les enquêtes expertes de juricomptabilité (Forensic Investigations)
- La planification et la dotation des opérations d'urgence
 - Doter en personnel les centres d'opérations d'urgence
 - Développer des équipes CERT* et/ou BERT* en entreprise
- Interviews d'AIA ou d'analyse des vulnérabilités
 - Adresser les opérations courantes indépendantes des TI
 - Adresser les opérations dépendant des TI et les applications/services
 - Adresser la sécurité logique et physique et les préoccupations de santé sécurité
- Développant des programmes conformité légale
 - Identifiez les besoins uniques et ceux qui se chevauchent
 - Testez pour la réutilisation au sein de domaines de gouvernances uniques



Questions & Commentaires

