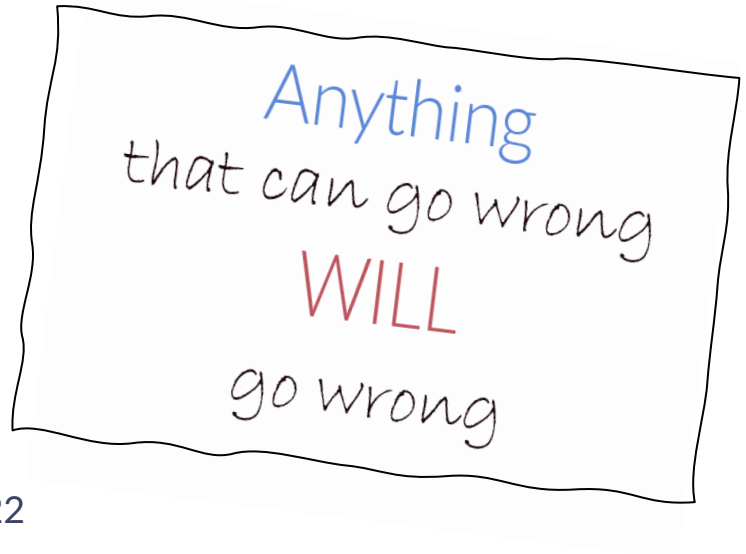
ANALYSES DE RISQUES ET LOI DE MURPHY

Tout ce qui peut bien… ou mal tourner



INTRODUCTION

Les analyses de risques appliquées à la sécurité des SI, apparues en même temps que les SI eux-mêmes, sont maintenant de plus en plus répandues, que ce soit dans les entreprises privées ou dans les organismes publics. Un grand nombre de méthodologies (gratuites ou payantes) existent, de même que des outils plus ou moins sophistiqués. De plus en plus de normes et de règlements nationaux ou sectoriels encadrent et/ou imposent la pratique de ces analyses.

Pour connaitre ces différentes méthodes, ainsi que leurs principes, avantages et inconvénients, se reporter au document du Clusif : « Analyse de risques en pratique ».

On pourrait donc penser que la réalisation d'analyses de risques SSI est devenue un exercice simple et maitrisé. Malheureusement, il n'en est rien, et le but de ce document est d'exposer – de façon légèrement humoristique, néanmoins réaliste – un certain nombre d'écueils rencontrés par toutes les entreprises dans leurs activités d'analyse de risques de sécurité.

Nous avons structuré ce document en plusieurs parties, correspondant aux divers temps des analyses de risques : stratégie, organisation, méthode, analyse des composantes des risques, résultats.

Dans chaque partie, nous citons les dysfonctionnements les plus courants, en les illustrant par le titre d'un film et une histoire vécue, puis nous exposons de façon très synthétique le rappel des bonnes pratiques. A ce propos, nous tenons à remercier tous les RSSI, Risk Managers et consultants qui nous ont aidés à enrichir ce document avec des anecdotes réelles.

Et comme il faut aussi parfois voir le verre à moitié plein, certaines anecdotes ne sont pas des écueils mais des success stories !

THÈMES

Loi de Murphy

Tout corps plongé dans une baignoire déclenche systématiquement la sonnerie du téléphone

CLUSIF

STRATEGIE

2021 : L'ODYSSÉE DE L'ANALYSE DE RISQUES

Comment se lancer dans l'aventure des analyses de risque ? Pour quelles raisons ? De quelle façon ?

Histoire vécue

Dans une entreprise du secteur de la Recherche, des analyses de risques sur la sécurité des SI sont faites chaque année. Cependant, étant commanditées tantôt par la Direction Générale, par la Direction de l'Audit et des Risques, par le RSSI ou par la DSI, les périmètres et les méthodes ne sont jamais les mêmes, laissant des zones d'exclusion et produisant des redondances dans les résultats.

Cette approche déstructurée produit un grand nombre de plans d'actions… jamais totalement mis en place ensuite.

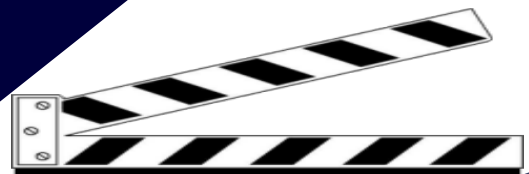
Conclusion

- Réaliser des analyses de risques est une odyssée au long cours, qui nécessite une vision, une approche, une stratégie.
- Il faut être conscient des raisons pour lesquelles on doit ou veut faire des analyses de risques, identifier leur attendu précis.

ORGANISATION

CLUSIF

Y A-T-IL UN PILOTE DANS L' AVION ?



L'importance d'avoir un coordinateur et un sponsor

Success story

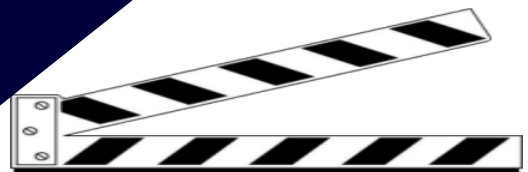
L'assureur d'une entreprise plasturgique possédant plusieurs usines en France avait exigé qu'elle réalise un plan de continuité global de ses activités et installations, sous peine d'augmenter fortement ses cotisations. Le sujet a été étudié par le comité de direction qui a désigné un sponsor (le directeur industriel) et un chef de projet (le responsable Qualité).

Une analyse de risques totale a d'abord été réalisée, à la fois sur les SI et sur les autres ressources matérielles (bâtiments, machines, matières…), ce qui a permis de prendre un grand nombre de mesures préventives, informatiques et techniques, et de réduire la surface du plan de continuité. Le projet a été long, mais très fructueux. Par la suite, le processus est devenu récurrent.

Conclusion

- Le sponsor est indispensable pour piloter l'avion, donner l'impulsion et apporter sa connaissance des enjeux de l'entreprise.
- Il doit être rattaché à la Direction, et dans l'idéal membre du comité de direction

LES BRONZÉS FONT DU SKI



Quand l'entreprise se lance sans expertise dans des analyses de risques

Histoire vécue

Un responsable Qualité qui devait préparer son établissement à la certification ISO 27001 mais ne connaissait pas les méthodes d'analyse de risques SSI s'est laissé persuader d'acquérir un logiciel d'analyse de risques très sophistiqué. Malheureusement, qui dit logiciel ne dit pas méthode. L'analyse de risques a été très difficile à réaliser et a fini par ne pas aboutir, personne ne sachant exactement comment structurer la démarche.

La certification n'a pas été obtenue. L'année suivante, les personnes se sont formées à une méthode d'analyse de risques, et ont tout repris sur Excel. La certification a été obtenue. Ils ne sont revenus à l'emploi de l'outil sophistiqué que plus tard.

Conclusion

- Comme en ski, le matériel ne suffit pas à avoir de bons résultats, il faut aussi avoir de la pratique.
- Il est donc nécessaire de disposer dans l'équipe projet d'au moins une personne qui connait la méthode et a déjà réalisé des analyses de risques, afin de guider les autres intervenants.

CLUSIF

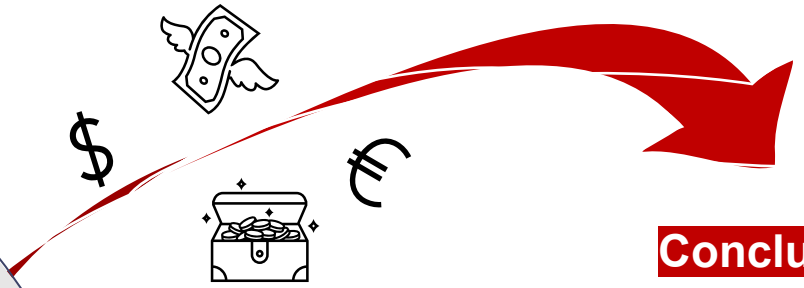
POUR UNE POIGNÉE DE DOLLARS

Quand les moyens ne sont pas à la hauteur des ambitions

Histoire vécue

Un grand groupe industriel souhaitait évaluer la sécurité de ses filiales à l'étranger afin de l'harmoniser et de la faire progresser. Le RSSI nouvellement nommé a commandité une analyse de risques auprès d'une société de conseil avec comme seule consigne de respecter le budget global. Résultat : la société de conseil a choisi comme référentiel l'ISO 27001, a effectué une analyse de risques très peu spécifique, identifié des centaines de risques élevés génériques, préconisé l'application de presque toutes les mesures de l'ISO 27002, et produit des rapports très volumineux et inutilisables qui n'ont pas permis de bâtir des plans d'actions.

Les années suivantes le RSSI a bâti sa propre méthode d'analyse de risques, basée sur les règles de sécurité spécifiques énoncées dans sa PSSI, et a pu proposer des mesures de sécurité justifiées et proportionnées.



Conclusion

- Identifier les attendus de l'analyse de risques et se donner des moyens adaptés d'y parvenir est primordial.
- Si les moyens sont réduits / limités, revoir ses ambitions à la baisse mais s'assurer de leur qualité.

CLUSIF

APOCALYPSE NOW

Quand l'analyse de risques tourne à la catastrophe, se perd dans la complexité, n'aboutit pas, ne produit pas de résultats utilisables

Histoire vécue

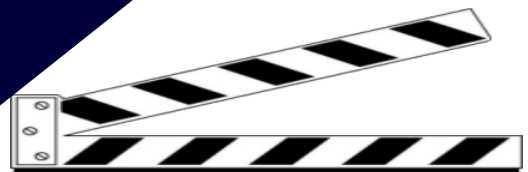
Dans une grande société de services en informatique, l'équipe de service delivery management avait souhaité lancer une vaste analyse de risques au niveau de chaque serveur client, dans son désir d'améliorer son image auprès de ses clients. Au travers de cette analyse, l'entreprise a donc essayé d'étudier les risques détaillés au niveau de chaque bien support… soit 3000 serveurs ! Les serveurs, leurs logiciels et leurs éléments réseau ont été considérés un par un, produisant des milliers de risques, dont certains majeurs.

Le plan de traitement a été impossible à définir. Le coût de l'opération a été considérable. L'année suivante il a fallu tout refaire, avec une autre méthode… et une autre équipe.

Conclusion

- Avant de lancer une analyse de risques, il faut considérer la volumétrie des biens et se poser la question de la granularité de l'étude.
- Pour éviter l'apocalypse, l'analyse de risques ne doit pas se dérouler sur plus de quelques mois, ni aboutir à l'identification de plus d'une centaine de risques.

LES BISOUNOURS

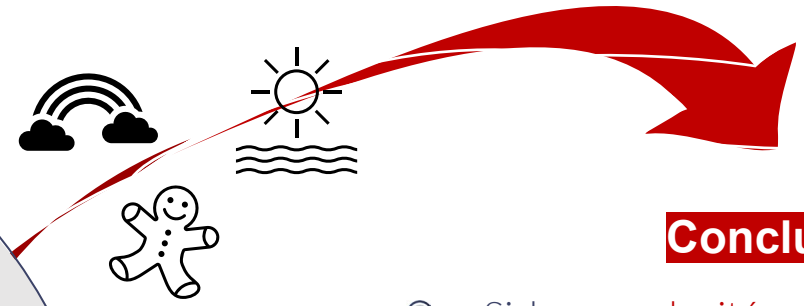


L'analyse de risques est trop simpliste et décrit une situation faussement idéale

Histoire vécue

Dans une grande entreprise du secteur pharmaceutique, l'équipe Risques a réalisé une analyse de risques, mais en utilisant une méthode habituellement employée pour étudier les risques opérationnels ou financiers, centrée autour des menaces possibles, sans analyser les vulnérabilités techniques.

Résultat, les conclusions se situent sur un plan tellement macroscopique qu'il n'y a que 7 risques, très vagues et très généraux, impossibles à corriger concrètement. L'entreprise a la fausse impression que tout va bien, la direction est rassurée par cette situation faussement idyllique.



Conclusion

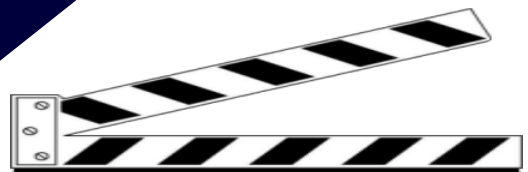
- Si la complexité extrême de la méthode ou de la granularité est à proscrire (Cf. ci-dessus), la simplification excessive l'est tout autant, pour ne pas vivre dans le monde des Bisounours
- Quand on ne chausse pas les bonnes lunettes… on ne voit rien… Un bon équilibre peut être d'identifier quelques macro-risques centrés sur l'impact (interruption d'activité, fuite de données, détournement de fonds, etc.) et identifier pour chacun une poignée de scénarios concrets pouvant conduire à leur survenance.

CLUSIF

MÉTHODE

CLUSIF

STAR WARS

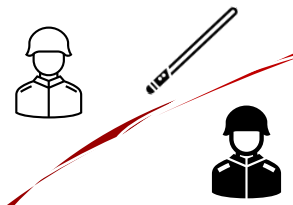


La guerre entre les « spécialistes » de la méthode d'analyse de risques

Histoire vécue

Dans une entreprise industrielle, le nouveau Risk Manager décide de moderniser l'approche de son prédécesseur. Confronté à la demande de sa Direction de fournir un profil des cyber risques, il décide d'employer une méthode nouvellement publiée par l'ANSSI. Cependant, une partie de l'équipe interne préfère en utiliser la version 2010, méthode éprouvée. Et les consultants mandatés ont une préférence pour ISO 27005.

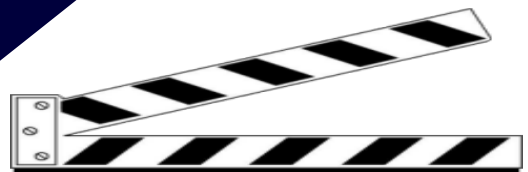
Finalement, un mélange des méthodes est appliqué, des discussions interminables sont nécessaires pour se comprendre et avancer, l'analyse de risques prend 2 ans ½ et ses conclusions sont déjà partiellement obsolètes au moment de la publication du rapport final.



Conclusion

- Chaque méthode a ses avantages, et ses inconvénients, ses objectifs et ses niveaux de détail. Le choix dépend des attendus qui doivent être précisément énoncés.
- Pour ne pas tomber dans une guerre d'experts, il faut donc choisir une méthode (éviter les mélanges ou alors, définir clairement quelles parties sont utilisées). Une fois ce choix établi, il ne faut pas en changer. Utiliser une méthode reconnue plutôt qu'une méthode maison aura l'avantage de disposer sur le marché d'experts connaissant la méthode.

SULLY



En dépit d'une mauvaise organisation, l'analyse de risques se termine bien et produit des résultats exploitables

Sucess story

Dans les années 1990, les premières analyses de risques appliquées à la SSI réalisées par une entreprise pharmaceutique (avec une méthode reconnue) conduisaient à multiplier les ateliers et interviews, avec beaucoup de doublons et de perte de temps.

Cependant, elles réussissaient à produire tout de même des résultats, car le RSSI qui les coordonnait était méthodique.

Conclusion

- Quand la « règle du jeu » de l'analyse de risques est complexe ou défaillante, il est tout de même possible d'obtenir des résultats utiles. A condition que les « joueurs » participent activement, soient motivés et méthodiques.

BIENVENUE CHEZ LES CH'TIS

Se comprendre est important…

Histoire vécue

Dans un site d'une entreprise industrielle certifiée ISO 27001, le nouveau RSSI devait mettre à jour les analyses de risques précédentes avant l'audit d'entretien annuel. Voulant comprendre les termes employés (ex. : biens essentiels / actifs / ressources), il fait une recherche dans les principales normes et méthodes, retrouve les définitions exactes, les présente au reste de l'équipe pour améliorer la compréhension. Malheureusement, l'auditeur qui vient effectuer l'audit d'entretien annuel a une préférence pour les termes et définitions de la méthode EBIOS RM, assez différents, et qui utilisent certains mots dans un autre sens.

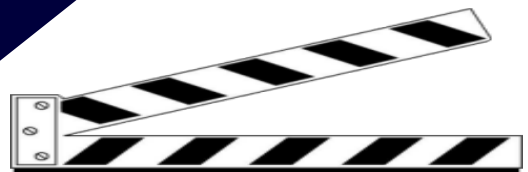
Beaucoup de confusion et d'incompréhension en découlent et le résultat de l'audit n'est pas aussi bon qu'escompté.

Conclusion

- Il est primordial d'employer un langage commun clairement défini lors d'une analyse de risques, sous peine de ne pas se comprendre. Mais ce n'est pas une finalité.
- Il suffit de faire un glossaire.

CLUSIF

HIBERNATUS



Les outils et les référentiels obsolètes produisent des résultats incomplets

Histoire vécue

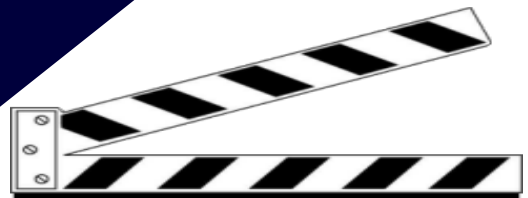
Une entreprise industrielle du secteur de l'énergie souhaitait faire certifier ISO 27001 une de ses filiales. Pour son analyse de risques, elle a choisi une méthode industrielle ancienne, non adaptée aux caractéristiques techniques de la cybersécurité, sans aucune liste de menaces ou de vulnérabilités adaptées au contexte actuel. Certains risques, essentiellement de sécurité physique, étaient tout de même identifiés.

Tout étant prêt (en apparence), elle a déclenché le début du processus d'audit de certification. Malheureusement, l'auditeur a refusé d'attribuer la certification, car la méthode retenue était obsolète et insuffisante pour révéler une grande partie des risques réels.

Conclusion

- Il faut faire évoluer les outils d'analyse de risques employés et les listes toutes faites, pour coller au contexte changeant et en perpétuelle évolution des attaques et des vulnérabilités, sous peine de rester à l'ère préhistorique de la sécurité.
- Pour la même raison, il faut aussi remettre à jour ses analyses de risques régulièrement.

JURASSIC PARK

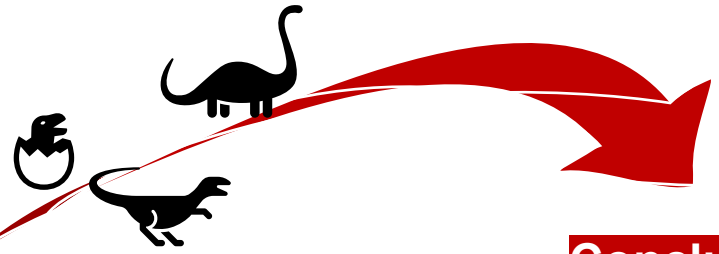


Quand une analyse de risques antédiluvienne est exhumée pour justifier la sélection de certaines mesures devenues désuètes au regard des avancées technologiques

Histoire vécue

Au sein d'une société d'assurances, dans le cadre d'un projet de migration d'un applicatif métier stratégique, le dossier de sécurité datant de plusieurs années a été revu à la seule lumière des exigences de sécurité émises à l'époque à l'issue d'une analyse de risques ponctuelle. Cependant, ladite migration prévoyait notamment de passer d'une architecture 3 tiers on-premise avec client lourd à une plateforme SaaS (qui induisait des exigences de sécurité différentes).

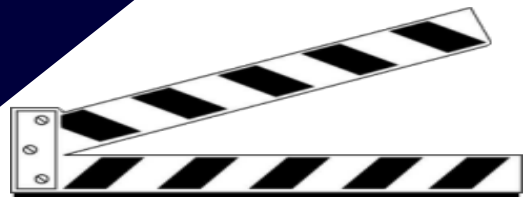
Les risques identifiés n'ont pas reflété la situation réelle.



Conclusion

A l'occasion d'une évolution majeure de périmètre fonctionnel et technique ou du contexte interne/externe, il convient de mener une nouvelle analyse de risques prenant en compte les nouveaux enjeux et les nouvelles menaces afin d'établir un nouveau plan de traitement du risque adapté (et éviter de ramener à la vie des mesures de sécurité « dinosaures »).

LA GUERRE DES CLONES

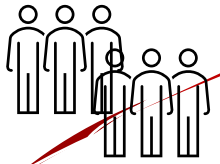


Lorsque toutes les analyses de risques projets sont réalisées en déclinant une analyse de risques type …

Histoire vécue

La DSI d'un opérateur télécom se devant de réaliser une analyse de risques pour chacun de ses projets avait fini par industrialiser la démarche via une solution d'IT GRC spécialisée, intégrant divers référentiels (critères et métriques, catalogues d'actifs, vulnérabilités, de menaces, mesures …) et visant à harmoniser les pratiques.

Pour finir, les différentes analyses de risques projets étaient quasiment identiques, car produites par copier-coller, alors que les applications considérées portaient des finalités et un écosystème opérationnel parfois très éloignés les unes des autres.

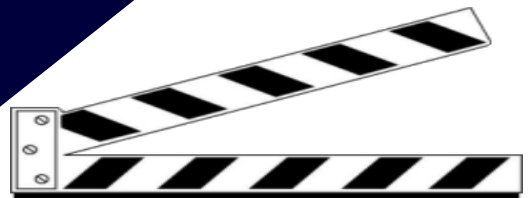


Conclusion

- L'harmonisation et l'optimisation des pratiques ne doivent pas se faire au détriment de la contextualisation et de l'adéquation des recommandations.
- Pour la même raison, il faut aussi remettre à jour ses analyses de risques régulièrement.

CLUSIF

INCEPTION



Les différents niveaux de granularité (métiers, fonctionnels, techniques) doivent être reliés et mis en cohérence

Histoire vécue

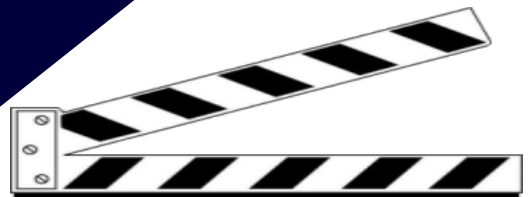
Une entreprise industrielle du secteur des transports terrestres avait pour habitude, dans la réalisation de ses analyses de risques portant sur des systèmes industriels, de modéliser le périmètre des actifs supports de manière très fine, jusqu'au composant technique, tandis que les fonctions métier restaient exprimées de façon macroscopique indépendamment.

Cela donnait des résultats techniques et des risques décorrélés des craintes métiers.

Conclusion

- Avant de se lancer dans la réalisation d'une analyse de risques, il est essentiel de prévoir une étape de cadrage visant à s'assurer de la cohérence et du lien entre les besoins exprimés par les métiers et les systèmes informatiques mis en place.
- Plus le périmètre sera important et complexe, plus l'analyse pourra être de haut niveau. Inversement, un périmètre restreint ou ciblé pourra justifier de pousser la modélisation de manière plus détaillée et donc plus précise, plus technique.

TITANIC



Quand le scénario-catastrophe écarté dès le début … est celui qui se réalise…et qu' il n'y a pas de canots de sauvetage

Histoire vécue

Dans une entreprise dont la spécialité est d'installer des réseaux de fibres optiques pour des opérateurs, un grand projet de réalisation du plan de continuité a été lancé. Lors de l'analyse de risques, le scénario de pandémie a été rejeté par la Direction dès le début, car « ce n'était jamais arrivé». Le risque n'est pas apparu dans les conclusions de l'étude, et n'a donc pas été traité. Deux ans plus tard, la crise sanitaire du Covid-19 a frappé le monde… et cette entreprise.

Il y a eu beaucoup d'interruptions de fonctionnement, de dysfonctionnements, de blocages. Si on regarde les statistiques, on s'aperçoit que les pandémies frappent en réalité tous les 50 ans.

Conclusion

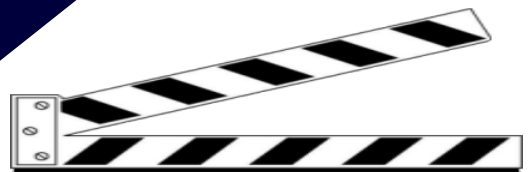
- Lors du choix des menaces considérées, il ne faut pas écarter trop vite celles dont la probabilité semble très faible. En effet, les probabilités reposent sur des statistiques de sinistralité, mais ces dernières n'ont pas encore un historique suffisamment long pour être fiables.
- Une menace non étudiée sera moins bien parée en cas d'occurence.

CLUSIF

ANALYSE DES COMPOSANTES DES RISQUES

CLUSIF

LES AVENTURIERS DE L'ARCHE PERDUE



Le travail d'enquête sur les vulnérabilités

Histoire vécue

Chez un constructeur d'ordinateurs, une application métier avait été mise en place pour supporter (selon la MOA) l'ensemble de l'activité du « Customer Service ». L'activité du support était bien plus importante que les Ventes, donc cette application, développée à l'extérieur, était classifiée à un haut niveau et sa protection avait bénéficié d'investissement très importants. L'application s'est arrêtée pendant plus d'une semaine en raison d'erreurs de code interne. On s'attendait à un impact très fort et une perte de clientèle mais le support et la facturation ont continué à fonctionner. Intrigués, les participants à l'analyse de risques ont mené leur enquête et ont constaté que chaque division support utilisait ses propres outils.

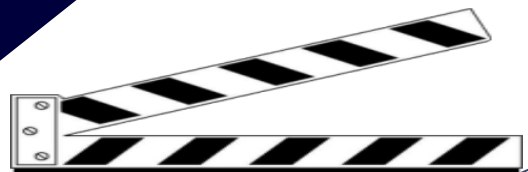
Cette application métier ne faisait que consolider les informations et permettait aux directeurs de chaque support de fournir des tableaux de synthèse au directeur général.

Conclusion

- Il est primordial d'analyser en détail – et de vérifier minutieusement, à la manière des archéologues – le périmètre qui formera la base de l'analyse de risques, afin de bien doser les efforts et les investissements.
- Un périmètre excessif ou non critique peut entrainer de gros surcoûts.
- Mener les ateliers avec les utilisateurs au quotidien des actifs informationnels améliore fortement la pertinence du périmètre

CLUSIF

RENCONTRES DU 3ÈME TYPE



L'importance de communiquer

Histoire vécue

Dans une grande entreprise du secteur médical, au tout début de l'instauration de son SMSI, les analyses de risques étaient coordonnées par la RSSI. Elle interrogeait les différents services un par un, pour étudier leurs vulnérabilités, et constatait souvent des divergences dans les réponses selon la personne ou le service questionné. Après quelques mois, elle a fini par organiser des groupes de travail transverses entre plusieurs services, afin de confronter les réponses et essayer d'obtenir un état des lieux réel.

Elle a constaté alors que les vrais « sachants » n'avaient pas toujours été identifiés au début, ou que certains services n'avaient pas connaissance de la réalité détaillée des moyens de sécurité.

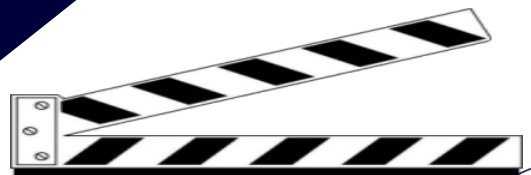
Conclusion

La grande difficulté des analyses de risques réside dans la mise en présence de profils très différents, et dans la communication entre eux. Il est important d'identifier et de réunir dans la même salle les bons interlocuteurs, les vrais « sachants », afin de faire énoncer l'état des lieux réel.

Si les sujets évoqués portent des germes de discorde (la sécurité du réseau, des salles informatiques, ...), l'importance de la communication est encore plus grande pour dépasser les conflits et les non-dits.

CLUSIF

LA VÉRITÉ SI JE MENS

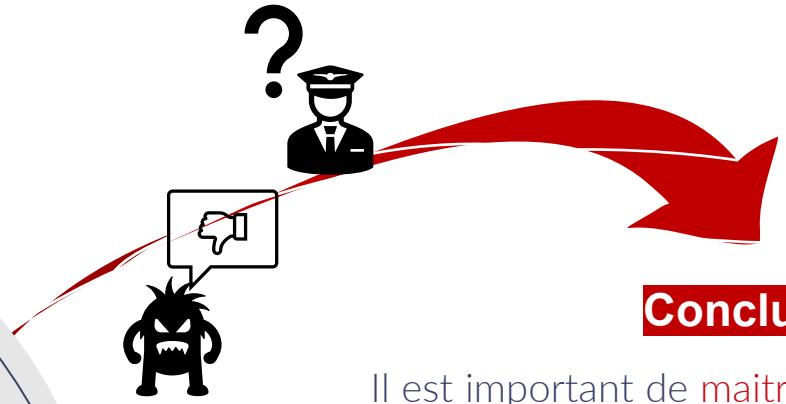


La vérification des réponses des groupes de travail

Histoire vécue

Dans une filiale chinoise d'une grande entreprise métallurgique, pour la 1ère fois une analyse de risques avait été demandée par le groupe et était conduite par une équipe française. Les sachants détachés par leurs équipes étaient trois, mais en général un seulement répondait. Les moyens de sécurité décrits étaient assez idéaux, peu de vulnérabilités apparentes, la situation semblait donc sous contrôle. Mais au bout de 3 jours, un membre de l'équipe française croise un des interviewés et en profite pour poser une question complémentaire. Et là, surprise : la situation réelle est très différente de ce qui avait été décrit. En effet, en Chine, c'est le chef de service qui a le droit de répondre, pas ses collaborateurs. Et il est important de donner une bonne image de soi donc les réponses n'étaient pas fiables.

Cette particularité culturelle étant comprise, il a fallu tout reprendre et effectuer des vérifications techniques poussées pour connaitre la situation réelle.

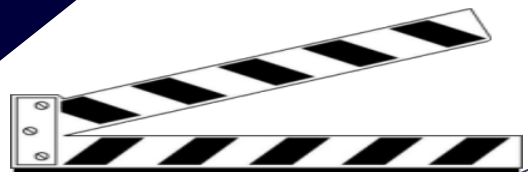


Conclusion

Il est important de maitriser les techniques de questionnement afin de recueillir les « vraies » réponses, puis d'aller faire des vérifications techniques. Comme lors des audits.

CLUSIF

OSS 117



Quand les outils ne fonctionnent pas ou sont mal utilisés …

Histoire vécue

Dans un organisme public, l'analyse de risques a été réalisée grâce à un tableau Excel « développé maison », afin de ne pas investir trop dans un outil. L'analyse a été menée entièrement, le plan d'actions produit, mais quand les mesures correctives ont commencé à être appliquées, un doute est apparu sur leur nécessité. Le responsable de l'analyse de risques a repris les tableaux Excel et… oups ! s'est rendu compte qu'il comportait des erreurs de calcul …

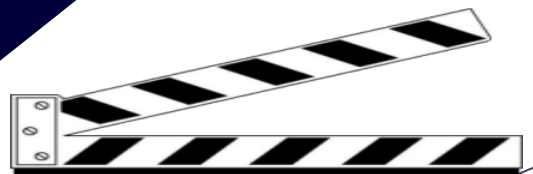
L'évaluation des risques était fausse, le plan d'action aussi.

Conclusion

- Les analyses de risques génèrent une assez grande quantité d'informations.
- Il est donc nécessaire d'employer des outils fiables et vérifiés, pour éviter les « gaffes ».
- Quelque soit le plan d'action automatique généré par un outil, une revue humaine avec l'œil de l'expert sera toujours pertinente

CLUSIF

UN JOUR SANS FIN



Quand il faut recommencer avant d'avoir terminé…

Histoire vécue

Nous sommes bien avancés sur la description des risques et du plan de traitement dans une analyse. Tout à coup le chef de projet nous indique qu'à l'occasion d'un nouveau sprint agile, de nouvelles données sensibles ont été ajoutées. Quelques jours après on découvre que le projet a changé d'optique et sera finalement hébergé chez un tiers. On reprend donc l'analyse rapidement, car la réunion de restitution approche.

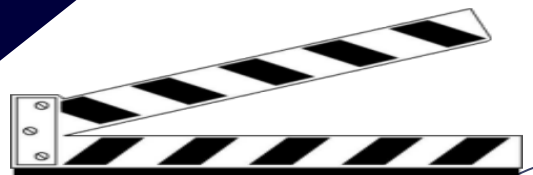
Enfin on arrive au bout ! En animant une pré restitution, on apprend qu'un audit a été fait et que des mesures du plan de remédiation ont comblé des failles qu'utilisaient certains risques.

Il faut recommencer…

Conclusion

- Il faut fixer le périmètre en tenant compte des mesures de protection qui seront prochainement installées et pour lesquelles il n'y pas de débat/d'arbitrage quant à leur application.
- Il ne faut pas hésiter à élargir le périmètre pour y intégrer des évolutions à court terme.
- Une intégration de la réflexion sécurité dans une démarche agile (DevSecOps) doit permettre d'identifier rapidement à chaque sprint les nouveaux risques résiduels et les nouveaux risques induits (issus des nouvelles fonctions), afin de progresser et d'éviter un retour sans fin à la case « départ ».

LES DENTS DE LA MER



L'analyse de risques n'est pas un audit, elle ne doit pas être vécue comme une menace

Histoire vécue

Il n'est pas rare, dans la conduite d'une AR, d'être confronté à des biais comportementaux. En particulier, à l'occasion des entretiens et des séances de restitution, on voit parfois minimiser les vulnérabilités (ex : interfaces externes ou accès à privilèges partiellement déclarées) ou même le niveau de risque (en probabilité d'occurrence et/ou en sévérité d'impact) de manière à ne pas véhiculer un message anxiogène pour les décideurs et à ne pas se sentir pris en défaut…

… quitte à sous-estimer les risques et diminuer l'intérêt de l'évaluation des risques.

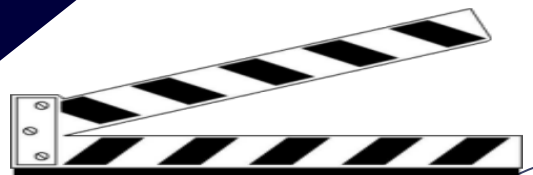
Conclusion

- Les analyses de risques ne sont pas des audits, aucun jugement de conformité ne doit être émis.
- L'analyse de risques est une description complète de la situation mise en perspective avec les menaces applicables à date. C'est tout.
- Il faut bien expliquer la finalité de l'analyse de risques aux personnes qui seront interviewées et à celles qui recevront les conclusions, pour éviter qu'elles se sentent en danger.

CLUSIF

RÉSULTATS

BEAUCOUP DE BRUIT POUR RIEN



L'analyse de risques qui enfonce des portes ouvertes

Histoire vécue

Dans une petite entreprise du secteur financier, un certain nombre de nouveaux moyens de sécurité avaient été identifiés comme nécessaires, mais le DSI ne parvenait pas à obtenir la validation et les ressources. Il a persuadé sa Direction d'instaurer une approche de gestion par les risques. L'analyse de risques sécurité qui a été réalisée a produit des résultats conformes à son analyse personnelle antérieure, les mesures qu'il avait déjà identifiées ont été proposées dans le plan correctif, et validées par la Direction.

On aurait pu faire l'économie de l'analyse de risques. Mais l'objectif a été atteint et la démarche qualité a été respectée.

Conclusion

- Réaliser une analyse de risques coûteuse pour officialiser des besoins déjà connus est toujours dommage, même si cela peut relever d'une approche politique.

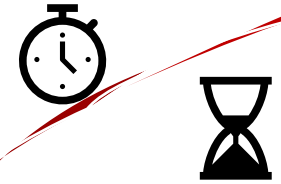
LE JOUR LE PLUS LONG

Histoire vécue

Dans une grande banque, l'analyse de risques annuelle produit à chaque fois plusieurs centaines de risques, en raison de la méthode détaillée employée. La présentation des risques à la Direction est interminable et de ce fait peu crédible. Il est impossible d'expliquer pourquoi des risques apparaissent aussi faibles ou aussi forts.

Il en résulte ensuite une phase de rejet par les différents services, puis de sélection des risques à retenir, avec de nombreux critères complexes, afin d'aboutir à un plan d'actions atteignable.

En définitive, seule une partie des risques est traitée mais pas forcément les plus importants.

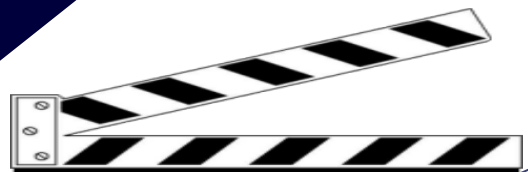


Conclusion

Il faut toujours garder à l'esprit que la matrice des risques doit être retravaillée, priorisée, regroupée, etc. avant d'être présentée et faire l'objet d'un plan de traitement. Le plan de traitement doit être atteignable, explicable et mesurable.

CLUSIF

SPY GAMES



Les résultats des analyses de risques sont très confidentiels

Histoire vécue

La plupart du temps, les résultats des analyses de risques sont partagés par mail sans chiffrement.

Cependant, ces résultats sont très confidentiels, car ils dévoilent tous les points faibles encore non corrigés.

Conclusion

- Il faut absolument protéger les résultats des AR, qui sont très confidentiels.
- Leur divulgation par fuite, vol ou espionnage, permettrait d'attaquer l'entreprise avec une grande facilité.

ACTIONS ET RÉACTIONS

CLUSIF

LES TONTONS FLINGUEURS

Les plans de traitement des risques peuvent conduire à des conflits internes

Histoire vécue

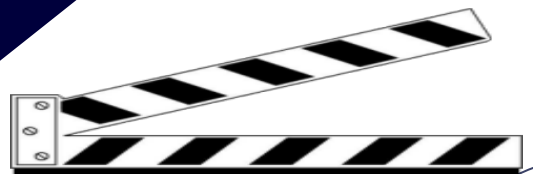
Dans un organisme public de recherche, la Direction des Risques avait souhaité remettre à jour la précédente analyse de risques sécurité. Les résultats ont montré que le précédent plan d'actions n'avait pas du tout été mis en œuvre par la DSI, voire que certains risques s'étaient aggravés.

Les relations entre les deux directions, déjà médiocres, se sont encore plus dégradées…

Conclusion

- Les résultats produits par les analyses de risques peuvent conduire à révéler des manquements internes plus ou moins graves et générer des règlements de comptes.
- Pour éviter que les services entrent encore plus en conflit et « s'éparpillent façon puzzle », un sponsor est indispensable. Il arbitrera et traduira la volonté de la Direction.

ON NE MEURT QU'UNE FOIS



Quand la Direction accepte un risque inacceptable, pour de soi-disant « bonnes » raisons…et que le risque se réalise

Histoire vécue

- *Dans une multinationale pharmaceutique, le risque « tremblement de terre » pour ses filiales japonaises avait été accepté, malgré sa forte probabilité et son impact élevé, car il était jugé trop coûteux à corriger par la Direction. Un important tremblement de terre à Osaka a entrainé la destruction du centre de recherche, dont ni le bâtiment ni les équipements n'avaient d'équivalent dans une autre filiale.*

Cela a généré de fortes pertes à court et long terme

- *Dans la plupart des entreprises hébergées dans les tours du World Trade Center, le risque de destruction terroriste n'avait jamais été imaginé sous cette forme extrême.*

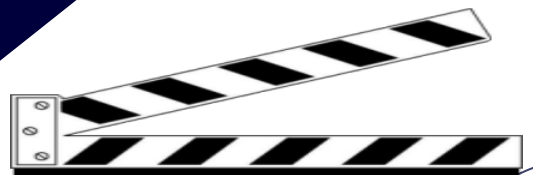
Plusieurs entreprises ont fait faillite à la suite de l'attentat du 11 septembre 2001.

Conclusion

- Lorsque des risques sont liés à des menaces improbables (mais pas totalement impossibles) ou trop coûteuses à réduire, il ne faut les écarter que pour une période temporaire, et les réviser comme les autres. Sous peine de subir des dommages définitifs.
- Mais lorsque des menaces ne peuvent même pas être imaginées, comment éviter leurs risques ?

CLUSIF

ATTRAPE-MOI SI TU PEUX – PARTIE 1



Quand une décision d'acceptation des risques est prise volontairement, sachant qu'elle constitue une infraction à une règlementation

Histoire vécue

Dans une entreprise, qui par exigences règlementaires doit réaliser des analyses de risques sur ses systèmes sensibles, la direction décide d'accepter certains risques sous l'impulsion de mauvais conseils: alors que son SI ne devrait pas être au contact d'Internet, l'analyse de risques montre que des systèmes sensibles sont localisés sur le même hyperviseur que des systèmes non sensibles en frontal d'Internet. L'entreprise considère que le niveau de sécurité par les mesures techniques sur l'ensemble des systèmes et de l'hyperviseur est suffisant. L'idée de segmenter et cloisonner les hyperviseurs et les systèmes ne leur parait pas être de nature à réduire et maitriser les risques.

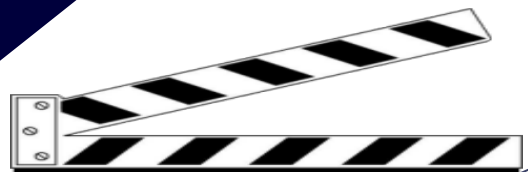
Les risques sont donc acceptés en l'état, à tort, ce qui constitue une non-conformité grave au regard des règlementations en vigueur.

Conclusion

- Quelle est la réalité d'un risque ? Quand le malade ne veut pas se voir malade, il casse le thermomètre, espérant que le médecin ne vérifiera pas par lui-même.
- Il faut se confronter à la réalité des constats, ne pas sous-estimer la vraisemblance des dysfonctionnements redoutés ou les règlementations applicables.

CLUSIF

ATTRAPE-MOI SI TU PEUX – PARTIE 2



Quand une décision d'acceptation des risques est prise volontairement, sachant qu'elle constitue une infraction à une règlementation

Histoire vécue

Un organisme public réalise son Registre des traitements et données à caractère personnel (RGPD). Réalisant que beaucoup de collaborateurs font des exports de données personnelles dans des fichiers Excel, échangés ensuite sans protection ni contrôle, la Direction des Risques décide … de ne rien faire pour réduire ou éviter ce risque. Au motif « qu'il est difficile de changer les habitudes des gens ».

Il y a donc une grosse non-conformité vis-à-vis du RGPD, de nombreuses possibilités de fuites de données, et de sanction potentielle en cas de contrôle.

Conclusion

- Tenter d'échapper à la règlementation, en matière de sécurité, n'est jamais une bonne idée. Il s'agit avant tout de protéger son entreprise.
- Si l'incertitude est une composante de l'appréciation du risque, il convient de garder une forme de lucidité pour que le résultat d'une analyse de risques et les décisions de traitement qui en découlent ne soient pas biaisés par une posture désinvolte face à une situation qui deviendra un jour une réalité : l'occurrence du risque.
- Dans la mesure du possible, l'acceptation du risque résiduel doit être du ressort de la Direction Générale.

CLUSIF

REMERCIEMENTS

Le Clusif remercie très chaleureusement :

Les animateurs (successifs) de l'Espace qui ont initié et porté ce document

Jean-Marc Grémy	Cabestan consultants
Jean Olive	CGI France
Hélène Courtecuisse	Lisis Conseil
Anne-Catherine Vié	ALL4TEC

Ainsi que les membres contributeurs

Nathan Voisin	Schneider Electric
Lazaro Pejsachowicz	Clusif
William Bourgeois	William Bourgeois Consulting
Michaël Jacques	Inventipharma
Thierry Pertus	Conix
Thimotée Laumann	Suez
Jean-Philippe Jouas	Clusif