Quantification des risques de cybersÃ©curitÃ© : mode ou innovation??
Accessoire
PostÃ© par : JulieM
PubliÃ©e le : 7/12/2022 13:00:00

La quantification des risques de cybersÃ©curitÃ© dÃ©signe une approche de lâ□□Ã©valuation des risques utilisant des modÃ¨les mathÃ©matiques et statistiques permettant de valoriser en termes financiers les consÃ©quences des Ã©vÃ¨nements cyber.

Lâ□□agence de notation Moodyâ□□s dÃ©clarait en 2021 : Â« La multiplication des mandats de cybersÃ©curitÃ©, le contrÃ´le de la conformitÃ© et les coÃ»ts plus Ã©levÃ©s des cyber-incidents faÃ§onnent des organisations qui ont de plus en plus besoin de communiquer avec les parties prenantes sur lâ□□exposition financiÃ¨re au risque cybernÃ©tique.

Par consÃ©quent, nous considÃ©rons lâ□□utilisation croissante des pratiques de quantification du risque cybernÃ©tique (Cyber Risk Quantification) comme un facteur positif Â».

Cette approche quantitative vivement recommandÃ©e gagne du terrain dans les analyses de risques de cybersÃ©curitÃ© menÃ©es au sein des grandes entreprises du Nasdaq et du Dow Jones.

La quantification des risques de cybersÃ©curitÃ© est alors exploitÃ©e comme un outil dâ□□aide Ã la prise de dÃ©cision business qui va parler au Board de ces grands groupes. Ce segment de marchÃ© est pris dâ□□assaut par des Ã©diteurs logiciels conscients de la demande et du besoin dâ□□industrialisation des analyses quantitatives.

Au-delÃ des dÃ©clarations, lâ□□agence Moodyâ□□s est positionnÃ©e en fer de lance de la Cyber Risk Quantification (CRQ) Ã travers son partenariat avec la sociÃ©tÃ© de rating cyber BitSight qui a dÃ©veloppÃ© une solution de CRQ avec lâ□□appui de lâ□□Ã©diteur logiciel Kovrr.

Ces solutions de CRQ apportent un second souffle aux mÃ©thodes quantitatives qui rappelons-le ne sont pas si rÃ©centes. A titre dâ□□exemple, la mÃ©thodologie FAIR (Factor Analysis of Information Risk) a Ã©tÃ© dÃ©veloppÃ©e depuis 2005 par le FAIR Institute aux Etats-Unis.

Concomitamment, nos entreprises francophones tendent Ã appliquer des mÃ©thodologies qualitatives (EBIOS Risk Manager est la mÃ©thode la plus citÃ©e aujourdâ□□hui), elles-mÃªmes promues par les agences nationales de cybersÃ©curitÃ© en France, en Belgique et en Suisse.

La qualification des risques de cybersÃ©curitÃ© est une Ã©valuation des risques Ã partir de donnÃ©es non mesurables et subjectives collectÃ©es auprÃ¨s des mÃ©tiers et de lâ□□IT.

Du fait des bÃ©nÃ©fices attendus, faut-il abandonner lâ□□approche qualitative au profit dâ□□une approche quantitative ? Utiliser les 2 approches ? Pourquoi lâ□□analyse de risques quantitative se fait difficilement une place sur le marchÃ© francophone alors que nos acteurs de la sÃ©curitÃ© informatique entendent parler de quantification du risque de faÃ§on rÃ©currente dans les forums Cyber ?

Les rÃ©ponses apportÃ©es par la quantification des risques de cybersÃ©curitÃ©

Une des rÃ©ponses Ã la faible diffusion de lâ□□approche quantitative des risques dans les entreprises francophones rÃ©side dans les cas dâ□□usage auxquels elle rÃ©pond. La quantification

des risques est employÃ©e pour :

Â· Communiquer en termes dâ□□exposition financiÃ¨re sur les risques cyber Ã un comitÃ© exÃ©cutif.
Â· Accompagner la prise de dÃ©cision du comitÃ© exÃ©cutif.
Â· Mettre en avant le Return On Investment du Plan de Traitement des Risques.
Â· DÃ©cider ou non de souscrire Ã une cyber assurance.
Â· DÃ©finir le bon niveau de police dâ□□assurance alignÃ© avec son exposition financiÃ¨re face au risque cyber.
Â· AmÃ©liorer sa cote de crÃ©dit intÃ©grant dÃ©sormais la notation en matiÃ¨re de cybersÃ©curitÃ© de lâ□□entreprise.

Sur le terrain, ces cas dâ□□usage commencent Ã peine Ã Ã©merger et surtout restent cantonnÃ©es Ã quelques entreprises francophones trÃ¨s matures qui souhaitent considÃ©rer la cybersÃ©curitÃ© comme un axe de leur modÃ¨le de gouvernance.

Les Directions des SystÃ¨mes dâ□□Information ont lâ□□habitude de prÃ©senter les grands risques de cybersÃ©curitÃ© et de dÃ©fendre leurs programmes dâ□□investissement dans la cybersÃ©curitÃ© pour y rÃ©pondre auprÃ¨s de leur Direction.

Mais les comitÃ©s exÃ©cutifs sont de plus en plus exigeantset beaucoup attendent de la quantification des risques un moyen de prÃ©dire les pertes associÃ©es aux cyber-incidents et de rationaliser les budgets pour couvrir a minima ces pertes.

Tirant des enseignements de cyberattaques vÃ©cues ou observÃ©es dans des entreprises du mÃªme secteur ou de mÃªme dimension, les dirigeants ont conscience quâ□□ils ne pourront pas Ã©chapper Ã la cybermenace. Lâ□□enjeu dÃ©sormais est de se concentrer sur des mesures de sÃ©curitÃ© qui peuvent limiter les impacts pour la continuitÃ© opÃ©rationnelle et pour les rÃ©sultats de lâ□□entreprise en cas de survenance dâ□□une cyberattaque.

Une vision financiÃ¨re du risque cyber basÃ©e sur des modÃ¨les statistiques

Les indicateurs chiffrÃ©s de lâ□□approche quantitative sont rassurants et concrets pour un comitÃ© exÃ©cutif qui veut comprendre combien lui coÃ»terait son pire cas de scÃ©nario de risques, et quels sont les investissements nÃ©cessaires pour rÃ©duire cet impact pÃ©cuniaire. Lâ□□utilisation de la quantification permet de prÃ©senter les consÃ©quences dâ□□incidents de cybersÃ©curitÃ© avec des valeurs en â□¬ ou $, qui sont comprises de tout membre du ComEx, contrairement aux incidents cyber.

Le risque cyber devient le rÃ©sultat dâ□□un calcul associant probabilitÃ© de survenance et valeurs dâ□□impacts dâ□□Ã©vÃ©nements redoutÃ©s. La mÃ©thode de calcul de Monte Carlo appliquÃ©e Ã la mÃ©thodologie FAIR par exemple est une technique mathÃ©matique qui permet dâ□□estimer cette probabilitÃ©.

Cette dÃ©marche probabiliste sâ□□oppose Ã la vision empirique du risque perÃ§u comme un Ã©vÃ©nement incertain dont on ne peut maÃ®triser la survenance et les effets.

La quantification des risques cyber contribue Ã un mouvement global de recours au Big Data pour dÃ©ployer des modÃ¨les de prÃ©dictions de plus en plus performants en sâ□□appuyant sur des donnÃ©es de plus en plus nombreuses relatives aux incidents de sÃ©curitÃ© et Ã leurs consÃ©quences.

Lâ□□idÃ©e de la Cyber Risk Quantification est de consolider des ensembles de donnÃ©es internes et externes (donnÃ©es de base sur lâ□□entreprise â□□ taille, secteur, emplacement, CA â□□ donnÃ©es du contrÃ´le interne, donnÃ©es sur les programmes de cybersÃ©curitÃ© menÃ©s par

la DSI, donnÃ©es observable de lâ□□extÃ©rieur Ã travers des logiciels de Rating par exemple) pour alimenter un moteur de calcul capable dâ□□aboutir en sortie Ã une liste de risques cyber priorisÃ©s selon leurs consÃ©quences opÃ©rationnelles et financiÃ¨res et Ã un Plan de Traitement des Risques budgÃ©tÃ© et justifiÃ© par la priorisation des risques.

Les logiciels enrichissent la mÃ©thodologie dâ□□analyse quantitative par leurs bases de donnÃ©es sur la cybermenace et leur modÃ¨le algorithmique. Ils contribuent Ã la fourniture de rÃ©sultats et dâ□□indicateurs fins quâ□□une approche manuelle ne pourrait pas produire.

Des entrants plus complexes Ã dÃ©terminer

La quantification des risques de cybersÃ©curitÃ© prÃ©tend Ã une fiabilitÃ© mathÃ©matique issue dâ□□algorithmes. En complÃ©tant les logiciels de Cyber Risk Quantification, on constate que ces derniers sont trÃ¨s consommateurs en donnÃ©es prÃ©cises.

Par consÃ©quent, moins une entreprise est capable dâ□□agrÃ©ger des informations financiÃ¨res et cyber fiables sur sa situation en sâ□□appuyant sur ses Ã©quipes et ses logiciels mÃ©tiers, supports et IT, plus les rÃ©sultats en sortie du logiciel de CRQ seront discutables et discutÃ©s par le Comex Il faut souvent combler le manque de data des entreprises par des estimations qui ne collent pas avec le cadre rigoureux de mÃ©thodologies quantitatives, et encore moins avec des outils automatisÃ©s.

Lâ□□implÃ©mentation de la mÃ©thode devient vite une course Ã lâ□□information chronophage et surtout incomplÃ¨te. La diversitÃ© et la prÃ©cision des donnÃ©es attendues pour implÃ©menter une mÃ©thodologie quantitative implique lâ□□intervention de sachants quâ□□il est souvent difficile de rÃ©unir autour dâ□□une analyse de risques.

Il serait par exemple pertinent de faire intervenir des interlocuteurs tels que la direction administrative et financiÃ¨re afin dâ□□Ã©tablir le profil financier de lâ□□entreprise pour dresser au mieux le tableau adÃ©quat de lâ□□exposition financiÃ¨re de lâ□□entreprise face Ã des risques cyber.

Il est requis dâ□□intÃ©grer et de valoriser les hypothÃ¨ses dâ□□actions et de temps de gestion dâ□□incident ou de crise cyber en termes de frais dâ□□investigation, de frais de remÃ©diation.

Ces Ã©lÃ©ments sont dÃ©tenus par un SOC et/ou la Direction des SystÃ¨mes dâ□□Information et potentiellement enregistrÃ©s dans une multiplicitÃ© dâ□□outils, ce qui ne facilite pas la tÃ¢che des analystes risques.

En dÃ©finitive, le processus de gestion des risques dans un modÃ¨le quantitatif doit Ã©voluer et se nourrir de plusieurs expertises sur le volet financier de lâ□□entreprise, lâ□□Ã©valuation de la performance des mesures de sÃ©curitÃ©, les coÃ»ts des activitÃ©s cyber ou IT dâ□□audit, dâ□□investigation, de remÃ©diation.

Lâ□□obtention dâ□□un tel niveau dâ□□expertise nÃ©cessite une forte maturitÃ© en gestion des risques dâ□□entreprise et une forte adhÃ©sion au processus de gestion des risques par lâ□□ensemble des collaborateurs.

Par ailleurs, il est difficile pour un non-praticien des modÃ¨les statistiques dâ□□expliciter les rÃ©sultats obtenus via un logiciel. Cela demande de faire confiance Ã un moteur de calcul et cet argument peut gÃ©nÃ©rer du doute auprÃ¨s dâ□□une Direction qui a besoin de comprendre les tenants et les aboutissants des chiffres consolidÃ©s.

Il est recommandÃ© que le porteur de lâ□□analyse de risques dispose dâ□□une bonne maÃ®trise des grandes lignes des algorithmes afin de garantir la crÃ©dibilitÃ© des rÃ©sultats devant les

parties prenantes de lâ□□analyse dont la Direction.

Lâ□□analyse quantitative, oui dans certains cas

Lâ□□approche qualitative des risques de cybersÃ©curitÃ© a encore de beaux jours devant elle dans les entreprises francophones. DÃ©fendue par les agences nationales de cybersÃ©curitÃ©, elle a Ã son avantage de reposer sur le consensus des mÃ©tiers et de lâ□□IT quant aux risques cyber Ã adresser en se fondant sur des critÃ¨res de risques partagÃ©s par tous, comprÃ©hensibles et lisibles dans les Ã©chelles de risques.

La mÃ©thode qualitative Ã©tant davantage rÃ©pandue et promue, elle est bien connue des auditeurs de certification et est encore Ã privilÃ©gier en cas dâ□□audit de certification dâ□□un SystÃ¨me de Management de la SÃ©curitÃ© de lâ□□Information ISO 27001.

Lâ□□approche quantitative plaÃ®t, intrigue mais peu dâ□□entreprises francophones passent le pas car cette approche nÃ©cessite un outillage logiciel, est mÃ©thodologiquement difficile Ã expliquer Ã quidam, et est longue Ã implÃ©menter.

Le temps qui devrait Ãªtre gagnÃ© sur la recherche de consensus est remplacÃ© par dâ□□importantes pÃ©riodes de collecte de donnÃ©es. Il faut aussi rÃ©percuter des coÃ»ts non nÃ©gligeables de formation Ã la mÃ©thodologie et au logiciel associÃ©, de licences logicielles et de rÃ©alisation de lâ□□analyse. Le jeu en vaut-il la chandelle ?

Almond vous recommande de choisir une approche quantitative si :

Â· Vous avez dÃ©jÃ rÃ©alisÃ© des exercices dâ□□analyses de risques,
Â· Vous Ãªtes dans un des cas dâ□□usage exposÃ©s plus haut,
Â· Câ□□est un choix mÃ©thodologique portÃ© et imposÃ© par votre Direction,
Â· Si votre processus de gestion des risques est suffisamment mature pour Ã©voluer et impliquer des contributeurs capables dâ□□apporter le niveau de prÃ©cision nÃ©cessaire aux donnÃ©es entrantes,
Â· Votre orientation Big Data est en forte progression.

Nous constatons que la distinction entre quantitatif et qualitatif nâ□□est pas si nette et quâ□□Ã lâ□□avenir les mÃ©thodes qualitatives embarquant du quantitatif vont probablement se dÃ©velopper dans toutes les entreprises pour deux motifs :

Â· La valorisation financiÃ¨re de lâ□□exposition au risque peu importe sa nature demeure un langage commun et parlant pour faciliter les prises de dÃ©cisions et la gouvernance. Câ□□est un indicateur fort qui permet Ã une Direction de rapprocher et comparer les donnÃ©es sur les grands risques de son entreprise.

Â· Lâ□□expÃ©rimentation de plus en plus frÃ©quente dâ□□incidents de cybersÃ©curitÃ© gÃ©nÃ¨re la crÃ©ation de bases de donnÃ©es riches et structurÃ©es qui permettront au fil du temps dâ□□alimenter finement les modÃ¨les.

Comme souvent en sÃ©curitÃ©, câ□□est au niveau du facteur humain que le bÃ¢t blesse, quid de la compÃ©tence et la capacitÃ© Ã maÃ®triser ces outils et ces mÃ©thodes mixtes dans des processus humainement gÃ©rÃ©s ?

Les plus de la Cyber Risk Quantification

Â· Outil de Gouvernance Business lisible dâ□□un ComitÃ© ExÃ©cutif
Â· Valorisation de lâ□□exposition financiÃ¨re au risque cyber et du ROI du Plan de Traitement des Risquespermettant de justifier les investissements nÃ©cessaires Ã la cybersÃ©curitÃ© et/ou de

dÃ©finir son besoin de couverture du risque par une cyber assurance
Â· Valeur ajoutÃ©e des logiciels de CRQ et de leur exploitation du Big Data

Les moins de la Cyber Risk Quantification

Â· Forte maturitÃ© en gestion de risques requise pour sâ□□y aventurer
Â· AgrÃ©gation chronophage dâ□□une diversitÃ© de donnÃ©es, de parties prenantes, de sources
Â· Recours Ã un logiciel dâ□□analyse de risques fortement recommandÃ©e
Â· Frais de formation et de licences
Â· MÃ©connaissance de la CRQ des auditeurs de certification dans le paysage francophone
Â· RÃ©sultats contestables car nâ□□Ã©manant pas dâ□□un consensus explicite mais dâ□□un algorithme perÃ§u comme abscons

Florence EXMELIN, Consultante gouvernance, risques et conformitÃ© chez Almond