# L'enseignement du management de la Sécurité de l'Information à un public technique à travers des exercices de crise cyber : Une approche innovante favorisant l'engagement de l'apprenant

Bérengère Branchet
*De Vinci Higher Education, De Vinci Research Center*
Paris, France
berengere.branchet@devinci.fr

Walter Peretti
*De Vinci Higher Education*
Paris, France
walter.peretti@devinci.fr

***Abstract*—Nous nous proposons dans cette présentation de partager notre expérience d'une pédagogie innovante pour enseigner la GRC (*Gouvernance, Risque, Conformité*) à des étudiants ingéneurs. Nous sommes dans une période d'obligations légales de se mettre en conformité pour beaucoup d'entreprises, avec les nouvelles réglementions imposées par l'UE (DORA, NIS2, CRA).**

**La gouvernance pour les systèmes d'information, est souvent abordée dans les filières de formation en management. Depuis quelques années, elle est aussi très présente dans les filières de formation techniques, car les entreprises recherchent des étudiants capables de "faire de l'analyse de risques, ET de comprendre le fonctionnement du réseau" (par exemple) pour mieux définir les risques inhérents.**

**Or l'enseignement de la gouvernance, avec l'étude et l'application des normes concernées peut paraitre très rébarbatif s'ils est uniquement descendant, et est encore plus perçu comme tel par un public technique plus habitué à apprendre aussi par la pratique. Nous avons donc mis en place une pédagogie active, utilisant la méthode interrogative et basée sur le travail en équipe projet. Nous avons intégré aussi une sous-partie de la GRC, la gestion de crise et la résilience, et utilisé cela comme fil rouge très motivant.**

***Index Terms*—pédagogie active, enseignant-facilitateur, mode projet, risque, gouvernance, résilience, gestion de crise**

## I. Introduction

Le Management de la Sécurité de l'Information regroupe, sous l'acronyme GRC, les activités de gouvernance de la sécurité, de mangement des risques et de la mise en conformité réglementaire et normative. L'enseignement de ces concepts à un public technique, notamment des futurs ingénieurs, présente des défis significatifs quand il s'agit de conserver l'engagement des apprenants :

- Introduire des concepts non techniques liés au management
- Mettre en évidence les enjeux stratégiques qui guident une organisation
- Comprendre la dynamique interne d'une organisation, et particulièrement les métiers, fonctions et processus.
- Lire, interpréter et mettre en œuvre les textes normatifs (par ex : ISO27001, ISO27005…) ou réglementaires (RGPD, directive NIS2, etc…)

Les approches traditionnelles en pédagogie descendante sont vite perçues comme théoriques et déconnectées des compétences nécessaires pour une réelle application métier. Pour surmonter ces difficultés, nous avons délocaliser l'enseignement de la GRC autour de la notion de résilience et de ce point paroxystique qu'est la crise d'origine cyber.

## II. Innovation pédagogique

Un constat s'impose de plus en plus en enseignement : il devient très compliqué de capter l'attention active des étudiants sur une durée dépassant les 10 minutes. Ils ont l'habitude d'être sans arrêt sollicités par des stimuli externes, et ont du mal à rester concentrés sur une tâche, surtout lorsque celle-ci n'appelle pas leur intérêt. Ce problème n'est pas récent et ne touche pas que les jeunes, mais il s'amplifie avec les générations de plus en plus nourries au "tout numérique".

Pour permettre aux étudiants de dernière année en formation ingénieurs d'appréhender au mieux les principes de gouvernance, nous avons ainsi décidé de ne pas faire de cours magistraux et descendants, pour enseigner l'analyse de risque (norme ISO27005), le management de la sécurité du SI (norme ISO27001), la résilience et la continuité (norme ISO22301). Nous avons mis les apprenants en situation d'acteurs, rejoignant en cela la théorie de l'apprentissage expérenciel de D.A. Kolb [1]. Le principe est de leur proposer un objectif motivant, et de les guider tout au long du chemin qu'ils devront parcourir pour l'atteindre. Ne pas perdre de vue l'objectif permet de conserver la motivation, et d'apprendre les notions prévues de façon naturelle car le besoin est là. Pour permettre le bon fonctionnement de cette pédagogie, il faut aussi un travail collaboratif, une participation de chacun. L'objectif choisi permettait d'avoir une dimension un peu gamifiée, ce qui est toujours fédérateur, et de permettre un travail en équipe projet. Et surtout, le rôle de l'enseignant est ici très important. il n'est plus le "sachant", mais l'accompagnateur, le facilitateur. Comme le développait Jacques Rancière dans son ouvrage "le Maitre ignorant" [3] l'enseignant a ici le rôle d'aider l'étudiant à apprendre par

lui-même. Il doit donc être à l'écoute, et utiliser une méthode interrogative pour amener les étudiants à aller chercher par eux mêmes les briques nécessaires à l'apprentissage. L'intérêt de cette approche réside dans l'engrammage des connaissances : ce que les étudiants cherchent, trouvent, analysent, critiquent eux-mêmes, s'engramme beaucoup plus que le discours du professeur. L'enseignant conserve bien sûr son rôle de superviseur, mais il montre le chemin et accompagne, il ne délivre pas la connaissance avant d'avoir déclancher la demande, le besoin, de l'apprenant.

La pédagogie mise en œuvre suit un déroulé thématique très précis qui vise in fine la création d'un exercice de gestion de crise et surtout la mise en pratique de l'exercice. C'est par cet axe que nous sollicitons l'intérêt des étudiants : l'idée de créer une situation de crise, de construire tout un scénario, et de le faire jouer à une équipe de camarades a un côté ludique que nous pouvons mettre en avant. Et pourtant, au travers de cette démarche les étudiants vont devoir apprendre et réaliser toutes les étapes d'apprentissage que nous visons.

Les apprenants sont ainsi mobilisés par équipe de 10. Ce nombre est fixé par la taille de la cellule de crise qui devra subir l'exercice, ce chiffre permet d'inclure les rôles propres à la cellule de crise (directeur et coordinateur de la cellule, bookkeepers) et suffisamment de fonctions métiers.

Nous allons détailler rapidement les différents étapes que chaque équipe aura à traverser avant la "récompense" finale : jouer et faire jouer un exercice de crise.

### *A. La création de la cible de l'exercice de gestion de crise*

L'équipe doit, sur un draft d'organisation que nous leur fournissons :

1) Créer l'organigramme de l'organisation, chaque membre de l'équipe s'attribuant un rôle dans cet organigramme
2) Décrire les principaux workflows de l'organisation (base de leur Business Impact Analysis et d'une éventuelle approche par les événements pour une analyse de risque selon ISO27005)
3) Créer l'infrastructure IT de l'organisation.
4) Définir précisément le contexte interne et externe de l'organisation ainsi qu'un périmètre pour la suite de leur travail.
5) Mener une analyse de risque sur leur périmètre (ISO27005/EBIOS)
6) Décrire comment mettre en œuvre les 93 mesures de sécurités de l'annexe A de l'ISO27001
7) Ecrire un Plan de Continuité d'Activité (ISO22301)

Chaque équipe aura tiré au sort un type d'organisation (hôpital, école, administration, industrie, OIV, ...) qu'elle devra s'approprier. Afin de les aider dans la création de l'organigramme et de la prise en main du fonctionnement de l'organisation imposée, les grandes lignes des livrables attendus leurs sont fournis. Cette première partie, assez loin de ce à quoi sont confrontés les élèves ingénieurs en général, leur permet de prendre connaissance avec la réalité d'une entreprise, et des différnts rôles et interactions présents. Cela est nécessaire pour une analyse de risque intéressante.

Les étudiants avancent en équipe, nous les suivons, les aidons, les aiguillons... et les forçons à se confronter à des réalités qu'ils n'envisageaient pas. Tout ceci dans un jeu de rôle, que nous faisons attention à garder le plus réaliste possible.

Des livrables jallonent les différentes phases (rapports, vidéos, présentations) permettant aux équipes de finaliser leurs réflexions et d'avoir un retour, et pour nous d'évaluer in fine le travail réalisé.

### *B. La création et la mise en œuvre de l'exercice de gestion de crise*

ne fois la cible de l'exercice créée, chaque équipe fournit toutes les informations qu'elle a créées à une autre équipe, et reçoit à son tour le descriptif détaillé d'une équipe.

Les équipes ont maintenant un "rôle de consultant" pour une entité. Elles disposent :

- du descriptif détaillé de l'entreprise (nom, fonction, organigramme, organisation sociale, ...)
- de son infrastructure IT
- de son analyse de risque (sur un périmêtre donné)
- de sa politique de sécurité
- des informations pour la mise en application des mesures de sécurité liées à la gestion du SMSI
- du plan de continuité

A l'aide de tous ces documents, l'équipe va devoir construire un exercice de crise, comme devraient le faire des consultants sollicités par l'entreprise pour leur proposer un exercice permettant de tester sa sécurité et les mesures prises pour celle-ci.

Pour la construction de l'exercise de crise, l'équipe devra créer un scénario réaliste, avec l'ensemble des syllabi, la situation initiale, et le chronogramme. ce sont les livrables attendus, *a minima*.

Les contraintes suivantes sont imposées :

- L'exercice doit permettre à la cible d'activer une partie au moins de son PCA.
- Le scénario doit posséder des stimuli relevant du périmètre de l'analyse de risque mais non nécessairement traités par l'équipe cible.
- Le scénario doit évidemment contourner les 93 mesures de sécurité mises en place par l'équipe cible.
- Le scénario ne doit pas se focaliser sur un seul événement, il doit "faire du bruit" (ajout de stimuli sans rapport avec l'incident cyber) dans le périmètre de l'analyse de risque ou en dehors.
- Le scénario doit impacter largement les métiers, et sous couvert d'un incident technique avoir des

impacts stratégiques/humains (grèves, communication défaillante).
- L'exercice combine des stimuli projetés sur écran, des mails et messages sur messagerie instantanée ainsi que des stimuli téléphoniques pour une plus grande adaptation possible du scénario aux réactions de l'équipe de gestion de crise.

## III. Résultats obtenus

Les équipes sont très intéressées à "piéger" leur camarades et se prennent complètement au jeu. Les étudiants ont besoin d'aller chercher beaucoup d'informations, dans différents domaines, pour "créer" leur entreprise. Cela leur permet de mieux comprendre le fonctionnement de différentes entités, et les liens entre chaque.

Les équipes sont composées d'alternants et d'étudiants en formation initiale, l'apport de chacun est très intéressant.

Dans la première phase, "construction de leur entreprise", il "apprennent" la méthode EBIOS-RM, l'analyse de risque, le SMSI, le PCA, mais surtout, ils réalisent tous ces documents.

Les retours que nous avons eu de plusieurs étudiants qui ont fait leurs stages ensuite dans la gourvernance est "qu'ils l'avaient **déjà fait** à l'école", et qu'ils n'étaient ainsi plus des débutants !

La deuxième phase, "construction de l'exercice de crise", les oblige à se plonger dans des documents, comme ils auront à le faire ensuite dans leur entreprise. Ils sont obliger d'analyser, de comprendre, afin de trouver les failles. Ils doivent aussi faire des recherches sur les différentes attaques cyber pour se donner des idées, analyser les kill chain pour en construire une réaliste. Ils doivent aussi se renseigner sur différentes crises, pas forcément d'origine cyber, afin de corser leur scénario.

Enfin, lorsqu'ils "subissent" la crise préparée pour eux, ils se rendent compte "pour de vrai" de ce que signifie gestion de crise, et gestion du stress. Nous leur avions donné les informations théoriques à ce sujet, mais dans la gestion de crise encore plus que dans tout autre domaine, tant que l'on ne l'a pas vécu, on ne sait pas ce que c'est. Une simulation est le meilleur moyen de s'y préparer "pour de vrai".

Lors des exercices, nous sommes toujours présents, en tant qu'observateurs, et pour pouvoir réagir si besoin. Et surtout pour les aider à faire le RetEx ensuite, en les amenant à formuler les "bonnes pratiques".

Cette expérience, de "subir une crise", la première pour quasiment tous les étudiants est particulièrement formatrice et interessante pour chacun. Ils seront moins démunis lorsqu'ils se trouveront dans une situation de crise. Ce dernier aspect de notre proposition d'enseignement nous tient aussi particulièrement à coeur, notre rôle est aussi de les préparer à la société dans laquelle nous évoluons.

## IV. Conclusion

Pour conclure, la création d'un exercice de crise d'origine cyber dans son entièreté, permet de :

- Mobiliser la créativité et l'engagement des apprenants, de la création de la cible à la création et l'exécution de l'exercice de gestion de crise.
- Mettre en œuvre le bagage technique acquis dans la formation d'ingénieur par la mise en place d'une infrastructure IT réaliste et l'écriture d'un scénario techniquement plausible (incluant toutes les étapes de la kill chain par exemple). Cela permet de conserver une accroche technique et donc l'intérêt des apprenants de profil technique.
- Comprendre les enjeux d'une direction d'entreprise, dans la mesure où l'exercice implique une cellule de crise décisionnelle et non technique. La phase de création de la cible pousse à la prise de conscience des enjeux stratégiques d'une organisation et offre également une première approche de la façon dont cette organisation se structure et fonctionne.
- Intégrer les exigences de la GRC de façon pratique : En réalisant les études de GRC sur la cible que l'équipe crée. En construisant le scénario sur la cible qui leur est affectée, puisque ce scénario doit s'appuyer sur les éléments de GRC fournis sur la cible.

Les retours des étudiants, pendant et après, globalement très positifs, nous assurent de poursuivre dans cette voie.

La formation est appréciée, mais surtout permet un réel apprentissage par l'expérience de tous les aspects de la GRC rencontrés. Cela assure une réelle, solide, et durable montée en compétences des étudiants. Le travail en équipe, et la responsabilisation des étudiants dans leurs apprentissages permet aussi de fédérer la plupart d'entre eux, pour ne pas dire tous.

La posture de facilitateur dans laquelle nous nous mettons permet de favoriser les échanges enseignants-étudiants, de valoriser leurs qualités, de leur donner encore plus confiance en eux, bref de remplir pleinement notre rôle d'enseignant en les aidant à se construire en tant qu'adulte responsable, éthique, et utile pour la société.

## References


[1] D.A. Kolb, "Experiential Learning: Experience as the Source of Learning and Development", Englewood Cliffs, NJ, Prentice Hall, 1984.

[2] L. Johnson, S. Adams Becker, V. Estrada and A. Freeman, "NMC Horizon Report: 2014 Higher Education Edition", Austin, Texas: The New Media Consortium, 2014.

[3] J.Rancière, "Le Maître ignorant : Cinq leçons sur l'émancipation intellectuelle", Paris : Fayard, 1987.