Les grandes fonctions de l'entreprise
Les systèmes d'information (SI)
Transcription vidéo – Séquence 8

Ce cours vous est proposé par Jean-Fabrice LEBRATY, Professeur agrégé des Universités, Université Jean Moulin Lyon3, et AUNEGe, l'Université Numérique en Économie Gestion.

Diapo 3
Dans cette séquence nous aborderons la question de la résilience des SI et des technologies qui la sous-tendent. Pour cela nous mettrons en avant 2 technologies et systèmes contribuant à la résilience des SI. Puis nous donnerons des catégories de situations éprouvant la résilience ainsi que des exemples. Enfin nous proposerons quelques pistes pour faire face.

Diapo 4
Quand un SI est développé et mis en œuvre dans une organisation, celle-ci se trouve dans un certain contexte. Puis, les SI évoluent, les contextes aussi, mais pas forcément au même rythme.
Par exemple, une banque ayant un SI développé il y a 30 ans, avant Internet, fait évoluer son SI pour s'adapter à l'Internet. Durant cette évolution, une crise informatique, comme un virus de grande ampleur, peut apparaître alors que la transition numérique de la banque n'est pas totalement accomplie.

Il y a plusieurs types de contexte et notamment des situations dans lesquelles il est possible de prévoir ce qui arrive et dans lesquelles le management contrôle la situation. Il y a aussi des contextes extrêmes qui restent toujours contrôlés mais qui sont plus délicat à gérer. Enfin il peut y avoir des crises dans lesquelles le contrôle est perdu.

Une des grandes finalités du SI est de contribuer à la résilience globale de l'organisation, mais pour cela il faut qu'il soit lui-même résilient.

La résilience c'est la capacité à conserver une structure cohérente après une crise. Les causes de la crise peuvent être internes ou externes, naturelles ou provoquées.

Diapo 5
La première technologie contribuant à la résilience est la blockchain. Proposée en 2008, cette technologie peut être comprise comme un protocole décentralisé permettant d'assurer un stockage fiable et pérenne des données de transactions. De nombreuses blockchain ont été créées.

Avec l'apparition de la blockchain Ethereum imaginée par Vitalik Buterin, il est devenu possible d'effectuer des opérations automatiques sur ces données, on parle de « smart contract ». L'idée sous-tendant un grand nombre de blockchain est la décentralisation. Ce protocole décentralisé s'étend et on parle de Web3.

Diapo 6

Il existe un très grand nombre d'applications de la blockchain. La plus connue se sont les cryptomonnaies avec notamment le « Bitcoin ». Mais le protocole Web3 étendu aux activités financières a donné la finance décentralisée ou DeFi. Les NFT, de l'anglais « non fungible token », offrent la possibilité d'attribuer de manière certaine une identité à un actif immatériel : code, fichier ou logiciel. Cela constitue une avancée majeure.

Diapo 7

La seconde technologie est représentée par le déploiement de l'accès à l'Internet via une flotte de satellites à basse orbite. Le réseau Starlink mis en œuvre par la société d'Elon Musk et suivi par d'autres projets change la donne en matière d'accès au cyberespace.
Aujourd'hui, plus de 5000 satellites permettent, aussi bien à des bateaux industriels qu'à des particuliers isolés, d'être connectés. Il devient alors plus faisable pour une zone dévastée par un ouragan par exemple, de retrouver un accès Internet et donc de coordonner les secours.
Cette technologie favorise aussi de nouveaux usages et fait entrer des acteurs dans le marché.

Diapo 8

Il existe de nombreuses catastrophes naturelles qui ont comme conséquence d'empêcher l'accès physique ou virtuel aux ressources du SI. Dans certains cas, un incendie par exemple, ces données peuvent être détruites à jamais.
Souvent les salles de serveurs informatiques ont été construites en sous-sol, notamment pour des questions de poids et d'accès électriques. Ces salles peuvent alors être inondées lors de crues inédites. La ville de Paris, notamment se prépare dans l'hypothèse d'une crue centenaire.

Diapo 9

Malheureusement, les conflits n'ont pas disparu. Dans le cas d'attaques, les SI constituent une cible souvent prioritaire puisqu'ils contribuent à assurer la coordination des défenseurs et à prendre des décisions. Les serveurs informatiques et tous les moyens qui assurent leur fonctionnement sont source d'intérêt pour les adversaires. Ces attaques peuvent être physiques, en coupant le réseau électrique par une bombe, ou informatique. On parle de cyberattaque.

Diapo 10

Quels enseignements pouvons-nous tirer de ce besoin de résilience ?
Il existe deux grands types de causes qui peuvent conduire à des crises pour les SI.

Il y a des causes naturelles et donc il est important de mettre en place une sécurité du SI. Il y a aussi des causes provoquées, des attaques délibérées, et dans ce cas, il faut des mesures de sûreté.
Pour la sécurité des SI, il est important de disposer de matériels et de logiciels fiables, non « bugués », et en nombre suffisant pour faire face aux pannes.
Mais il faut aussi anticiper les crises et donc chercher à les préparer au travers notamment de deux types de plans : les plans de continuité d'activité et ceux de reprise d'activité.
Enfin, la perception du financement du SI s'avère déterminante et conditionne tout. Si le SI est perçu comme un coût, il sera tentant de minimiser ce coût. Des tensions sur les matériels et logiciels favoriseront alors les risques de crise. Alors que si le SI est vu comme un investissement, il s'agira de maximiser cet investissement en se donnant les moyens d'éviter les problèmes.

Pour la sureté, la gestion des accès au SI est un élément primordial.
Il s'agit par exemple de vérifier les accès quand une politique de télétravail est mise en place et donc que le SI s'ouvre hors les murs de l'entreprise.
Il est aussi important de mettre à jour très fréquemment les systèmes. Il suffit de voir la grande fréquence des mises à jour des applications de réseau sociaux sur les smartphones pour bien comprendre cette « criticité » perçue par les éditeurs de ces applications.
Il faut aussi, en interne, disposer d'équipes très réactives pour la sécurité, comme pour la sureté. Ces équipes doivent pouvoir intervenir 24 heures sur 24 et 7 jours sur 7. Les membres des équipes doivent posséder des qualités spécifiques. D'ailleurs l'ensemble des membres de l'organisation doit avoir au moins des bases numériques pour limiter les risques.
Enfin, l'étendue des connaissances en SI étant immense, il est important que l'entreprise noue des liens avec des acteurs institutionnels comme l'ANSSI par exemple. Mais aussi avec des communautés privées comme des groupes de développeurs de langages qui sont utilisés dans l'entreprise afin de bénéficier d'un appui pour la résolution de problèmes.

Références

Comment citer ce cours ?

Les grandes fonctions de l'entreprise – SI, Jean-Fabrice LEBRATY, AUNEGe (http://aunege.fr), CC – BY NC ND (http://creativecommons.org/licenses/by-nc-nd/4.0/).