Séance 2 – Enquêter sur les pratiques de gestion du risque

Management du risque (tronc commun)
EPITA 2025 – F. Giuliani

Enquêter sur le management du risque cyber

Management du risque cyber ≈ cybersécurité

- Cybersécurité :
  - Enjeu critique pour les organisations : viabilité des systèmes
  - Enjeu critique pour l'IT et les ingénieurs en IT
- Objectif de la présentation :
  - Clarifier l'importance de l'enquête
  - Expliquer le questionnaire
  - Fournir des conseils pour trouver des répondants et recueillir des données

EPITA

Pourquoi l'enquête de terrain est essentielle

EPITA
ÉCOLE D'INGENIEURS EN INFORMATIQUE

Exposition au danger provient souvent de l'interne

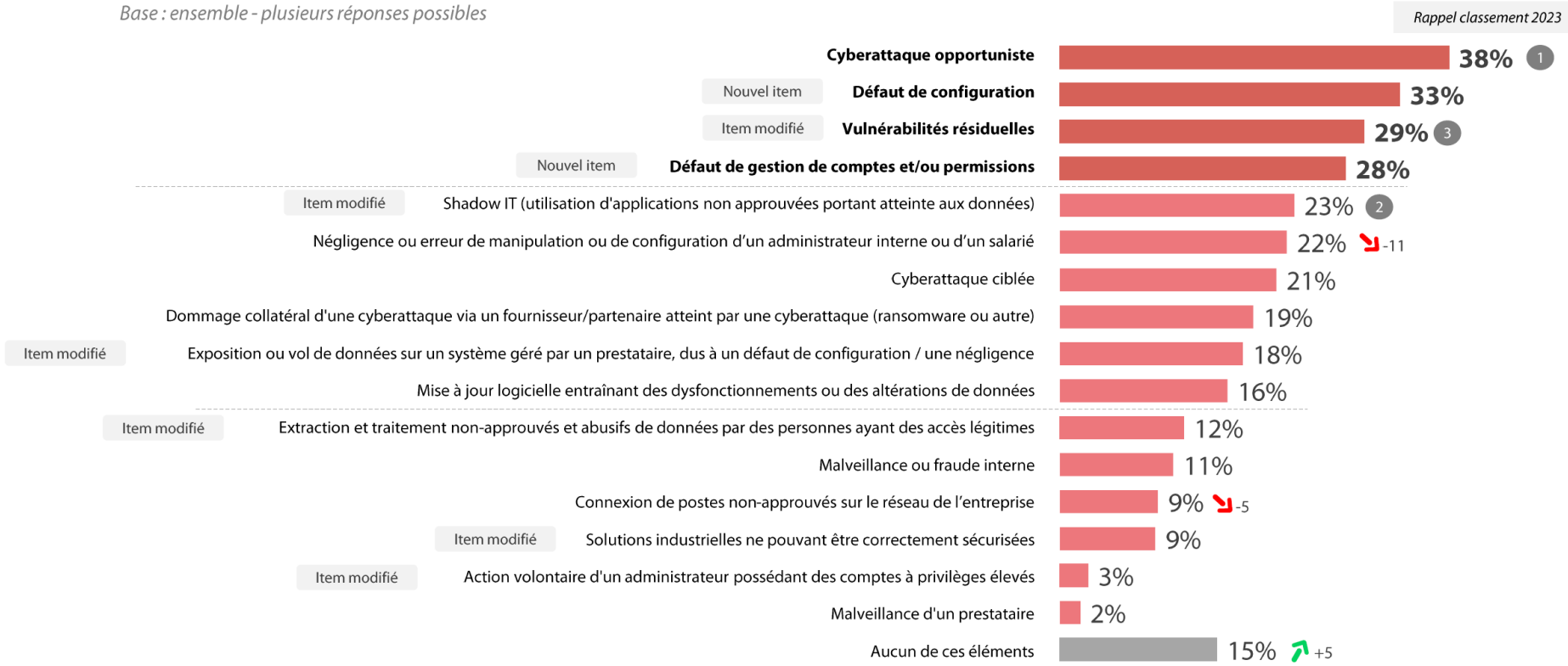
1. Pratiques informelles
2. Erreurs humaines
3. Transgressions volontaires de procédures

Les incidents de sécurité sont majoritairement causés par des opportunités laissées aux attaques : cyberattaque opportuniste, défaut de configuration, vulnérabilités résiduelles et défauts de gestion de comptes, reléguant alors le Shadow IT à la 5ème place cette année (vs 2ème l'année précédente).

401 perso

Q6. Parmi les causes des incidents de sécurité rencontrées par l'entreprise, cyberattaques incluses, quelles sont celles auxquelles votre entreprise a été concrètement confrontée au cours des 12 derniers mois ?

Base : ensemble - plusieurs réponses possibles



Pourquoi les acteurs sociaux transgressent-il les normes de des organisations pour lesquelles ils travaillent ?

Mini-cas : groupe hôtelier français (1/2)

- Cas réel, rapporté par Yves Morieux (voir Morieux & Tollman, 2014)
- Contexte : milieu des années 2000-2010
- Un grand groupe hôtelier français voit sa rentabilité stagner et le cours de son action en bourse diminuer
- Plusieurs restructurations et plans de formation du personnel : aucun résultat tangible malgré investissements importants
- La DG missionne un cabinet de conseil pour comprendre la persistance des problèmes
- Après interview des cadres dirigeants du groupe hôtelier, le cabinet de conseil décide d'enquêter sur les pratiques des collaborateurs
    - Observations de terrain
    - Echanges directs

Mini-cas : groupe hôtelier français (2/2)

- Méthode d'observation « client mystère » : un consultant se fait passer pour un client
- Le client mystère arrive un dimanche soir à l'accueil d'un hôtel, et demande une chambre
  - Réponse du réceptionniste : « *je suis navré Monsieur, je n'ai plus de chambre à vous proposer, mais je vais appeler pour vous un autre hôtel de notre groupe, à seulement quelques minutes d'ici.* »
  - Le réceptionniste du deuxième hôtel déclare au téléphone ne plus avoir de chambre disponible.
  - Le premier réceptionniste propose d'appeler un troisième hôtel du groupe, à peine plus loin : son homologue affirme également ne plus avoir de chambre libre.
  - Accueil irréprochable (sourire, souci évident du service, empathie…)
- Analyse du CRM des hôtels ce soir-là
  - 2 chambres libres dans le premier hôtel
  - 1 chambre libre dans chacun des deux hôtels appelés par le réceptionniste

Pourquoi ?

Comportement : réponse rationnelle aux problèmes portés par le contexte

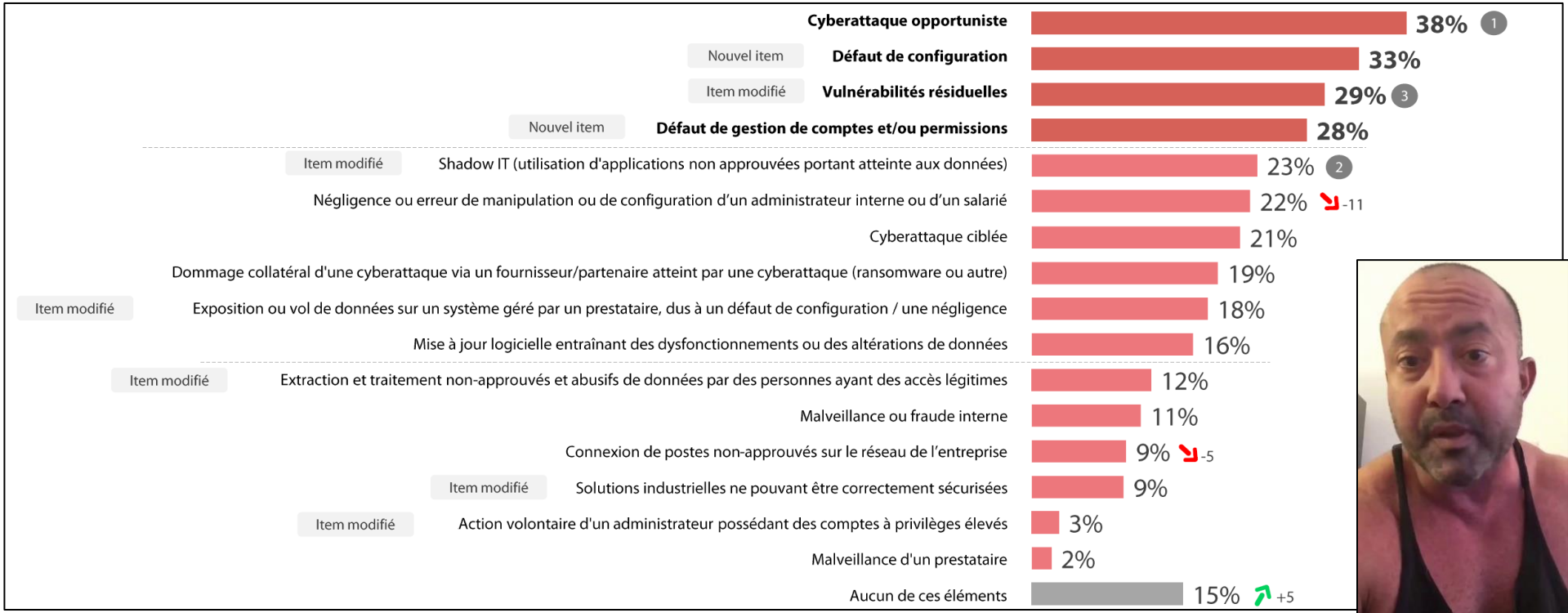
1. **Tout comportement est une solution face à un problème**
2. Tout comportement contient des indices sur…
    - Les ressources que peut mobiliser l'acteur
    - Les efforts fournis par les acteurs pour contourner ou minimiser leurs contraintes

Un acteur a toujours des raisons de se comporter comme il le fait, même si son comportement n'est pas raisonnable du point de vue d'autres acteurs

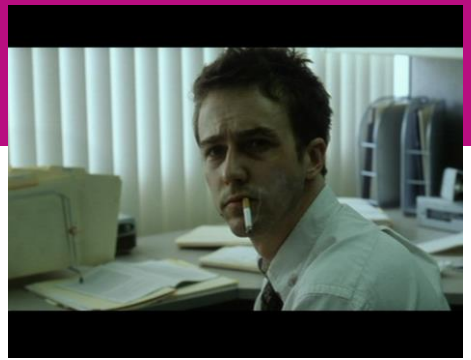
Dans le cas du groupe hôtelier français

- Service maintenance fermé à partir de 20h : pas de techniciens disponibles entre 20h et 6h
- Agents d'entretiens ne rapportent pas les pannes / problèmes constatés lors du ménage
- Si un problème survient après 20h (clim déréglée, télé HS, chasse d'eau bouchée etc.), pas d'autre solution pour le réceptionniste que de proposer au client une nouvelle chambre
- **Nécessité de garder en permanence une ou deux chambres libres**
    - Objectif : ne pas affronter la colère du client

Négligences, difficultés et transgressions sont des phénomènes tabous… et normaux !



Travail prescrit Vs travail réel



Travail prescrit

- Contenu des tâches décrit dans les fiches de postes et les procédures
- Conception scientifique / optimisatrice
- Produit d'analyse sur les modes d'action et les durées
- Objectif : tendre vers la plus grande productivité
- Cadre théorique

Travail réel

- Contenu des tâches effectivement mis en œuvre par les opérateurs
- Multitudes de petites décisions et d'initiatives fondées sur la connaissance empirique des postes de travail
- Mobilise des connaissances, savoir-faire et savoir-être tirés de l'expérience
- Rend opérationnel le travail prescrit

Enquête de terrain

EPITA
ÉCOLE D'INGENIEURS EN INFORMATIQUE

Objectifs et structure du questionnaire

- Quatre axes :
  - Gouvernance (politiques, organisation)
  - Risques (identification, analyse, impacts)
  - Stratégies de protection (mesures, budgets, assurance)
  - Culture et formation (sensibilisation, adhésion)
- Visées
  1. Déterminer le la maturité cyber de l'organisation
  2. Explorer les arbitrages entre sûreté, coûts et délais
- Réponses seront analysées quantitativement (statistiques) et qualitativement (exemples concrets)

Cibler des répondants pertinents

- Fonctions clé : RSSI, DSI, responsables IT…
- Idéalement, dans une industrie / une entreprise qui vous intéresse
- Recherche via LinkedIn (recherche par intitulé, groupes spécialisés), réseaux professionnels, cercles alumni…
- Envoyez un message court et personnalisé :
  - Précisez votre statut étudiant, l'objet de l'étude et raison de l'intérêt
- Taux de réponse
  - Message impersonnel : 1-2% de réponses en marketing → à éviter
  - Message personnalisé : 20-25% → à privilégier

Maximiser le taux de réponse

- **Accroche :** mentionnez la durée de l'entretien, l'objectif précis, le bénéfice pour le répondant.
- **Expliquer l'intérêt de l'enquête :** partage de bonnes pratiques, possibilité de recevoir les conclusions de l'enquête
- **Expliquer votre intérêt pour le répondant :** entreprise innovante, secteur d'activité intéressant pour vous, profil actif sur les réseaux sociaux etc.
- **Adapter le ton :** formel pour un contact inconnu, chaleureux avec un alumni ou via recommandation
- **Relancez au bout de 5-7 jours**, en rappelant brièvement votre demande et l'utilité de sa participation.

Administrer l’enquête

- **Rendez-vous court (30-45 min, 1h si l’interlocuteur est bavard)**
- **Introduction :** expliquer la finalité de l’enquête, garantir la confidentialité et l’usage pédagogique des données
- **Pendant l’entretien :** suivez la trame du questionnaire, posez des questions ouvertes et reformulez-les si besoin
- **Saisissez les réponses en direct dans le formulaire Microsoft Forms**

Bonnes pratiques en entretien

- **Soyez ponctuel et professionnel :** présentez brièvement le projet, puis suivez la grille de questions.
- **Privilégiez les questions ouvertes :** « *Comment cela se fait-il ?* », « *Pourquoi ?* », « *Pouvez-vous donner un exemple ?* »
- **Écoute active :** prenez des notes, demandez des précisions, reformulez (« *si je comprends bien…* »)
- **Respectez la durée annoncée :** recentrez le propos si nécessaire, mais laissez le répondant exprimer ses idées.
- **Terminez par un remerciement** et rappelez que vous partagerez une synthèse des résultats si le répondant le souhaite

EPITA

Déroulé

EPITA
ÉCOLE D'INGENIEURS EN INFORMATIQUE

Informations pratiques

1. Kick-off : maintenant
2. Enquête :
    1. Guide d'entretien disponible sur Moodle
    2. Collecte des résultats via Microsoft Forms
        - Auto-inscription par groupe de 5
        - 1 questionnaire par groupe
3. Besoin de conseil pour trouver un répondant / pour vous préparer à l'entretien ?
    1. **Possibilité d'avoir un call de coaching 30 minutes**
    2. Si vous êtes inscrit à Epita Paris : réservation directe via https://calendly.com/mukaconseil/module-management-risques-epita
    3. Si vous êtes inscrit à Epita Lyon et Toulouse : écrire un mail à fabien1.giuliani@epita.fr

Coaching – conseil

Objectif : vous assister **à votre demande** (facultatif) dans la conduite de votre enquête de terrain

Epita Paris : Yann Kasay

- Spécialiste intelligence économique
- Consultant en intégration IA sur business existant
- Prise de RDV : https://calendly.com/mukaconseil/module-management-risques-epita

Epita Lyon et Toulouse : Fabien Giuliani

- Votre enseignant (préféré)
- Chargé de cours en gestion des risques et management
- Prise de RDV : fabien1.giuliani@epita.fr

Rappel modalité d'évaluation

- 50% note finale : QCM en ligne portant sur les concepts clés du cours (cadres normatifs, stratégies de gestion du risque, typologies de risques, outils de contrôle…)
- 50% de la note finale : réalisation de l'enquête de terrain auprès d'un RSSI ou poste jugé équivalent
  - Critères d'évaluation : intégralité des questions traitées, réponses explicites aux questions ouvertes
  - Preuves demandées :
    - Courte preuve d'échange : un snapshot / une photo de la réponse à votre prise de rdv (par mail, LinkedIn etc.)
    - Courte preuve d'entretien : un snapshot / une photo de votre entretien
    - Un mail de remerciement sera envoyé par Epita à chaque participant

Questions ?

Au besoin…

- Fabien1.giuliani@epita.fr (réponse sous 2-3 jours)
- +33 6 48 62 11 43 (besoin réponse rapide)
- Il n’y a pas de question idiote