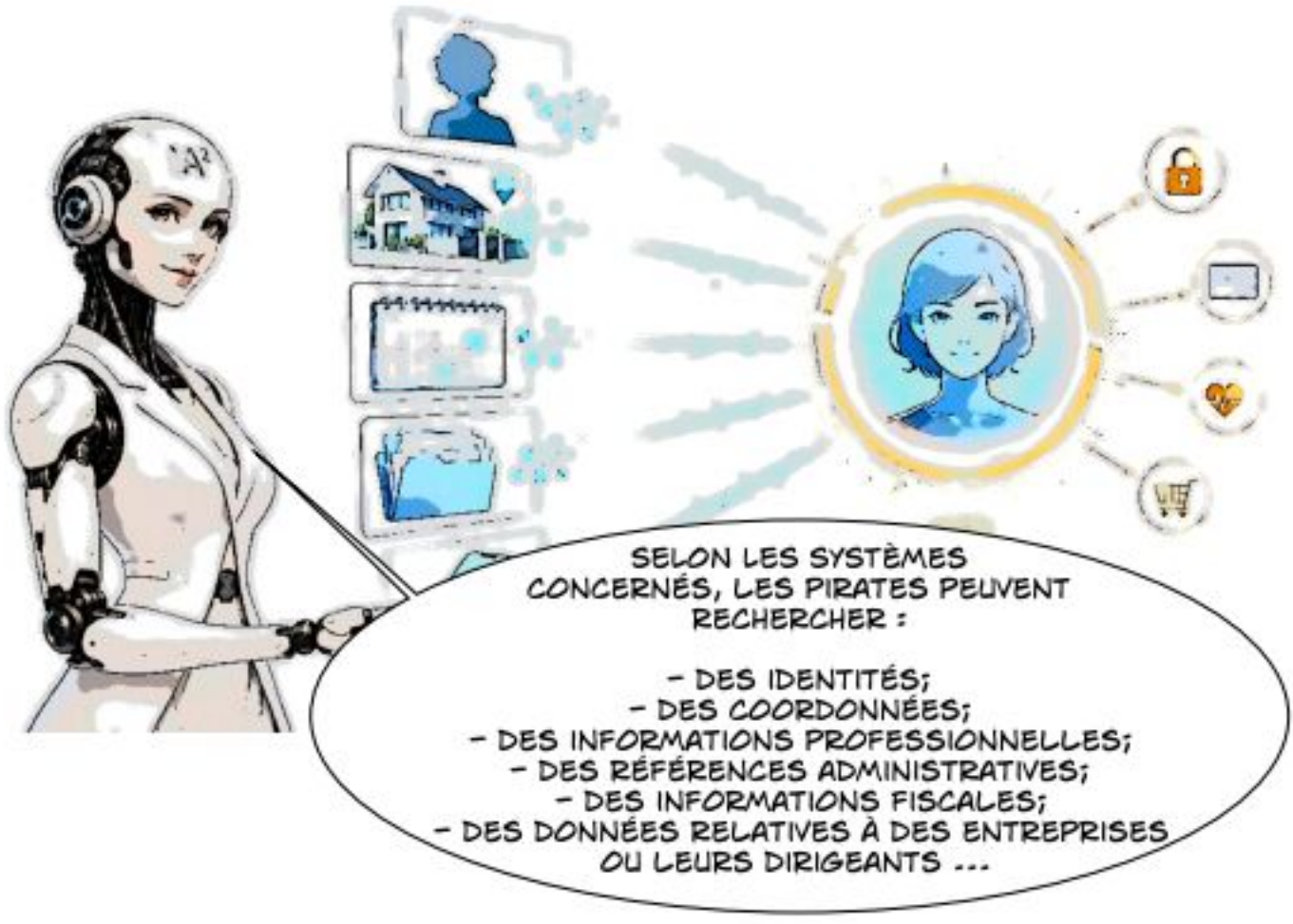
LA DIRECTION GÉNÉRALE DES FINANCES PUBLIQUES A COMMUNIQUÉ SUR DES ACCÈS ILLÉGITIMES À SON SYSTÈME D'INFORMATION...
CYBERATTAQUE À LA DGFiP
DES MILLIONS DE DONNÉES PERSONNELLES EXTRAITES

QUAND UNE ENTREPRISE EST PIRATÉE, ON DIT QU'ELLE EST VICTIME...
... MAIS LORSQU'IL S'AGIT D'UNE ADMINISTRATION QUI DÉTIENT LES DONNÉES DE MILLIONS DE PERSONNES, PEUT-ON SIMPLEMENT DIRE QU'ELLE EST VICTIME ?

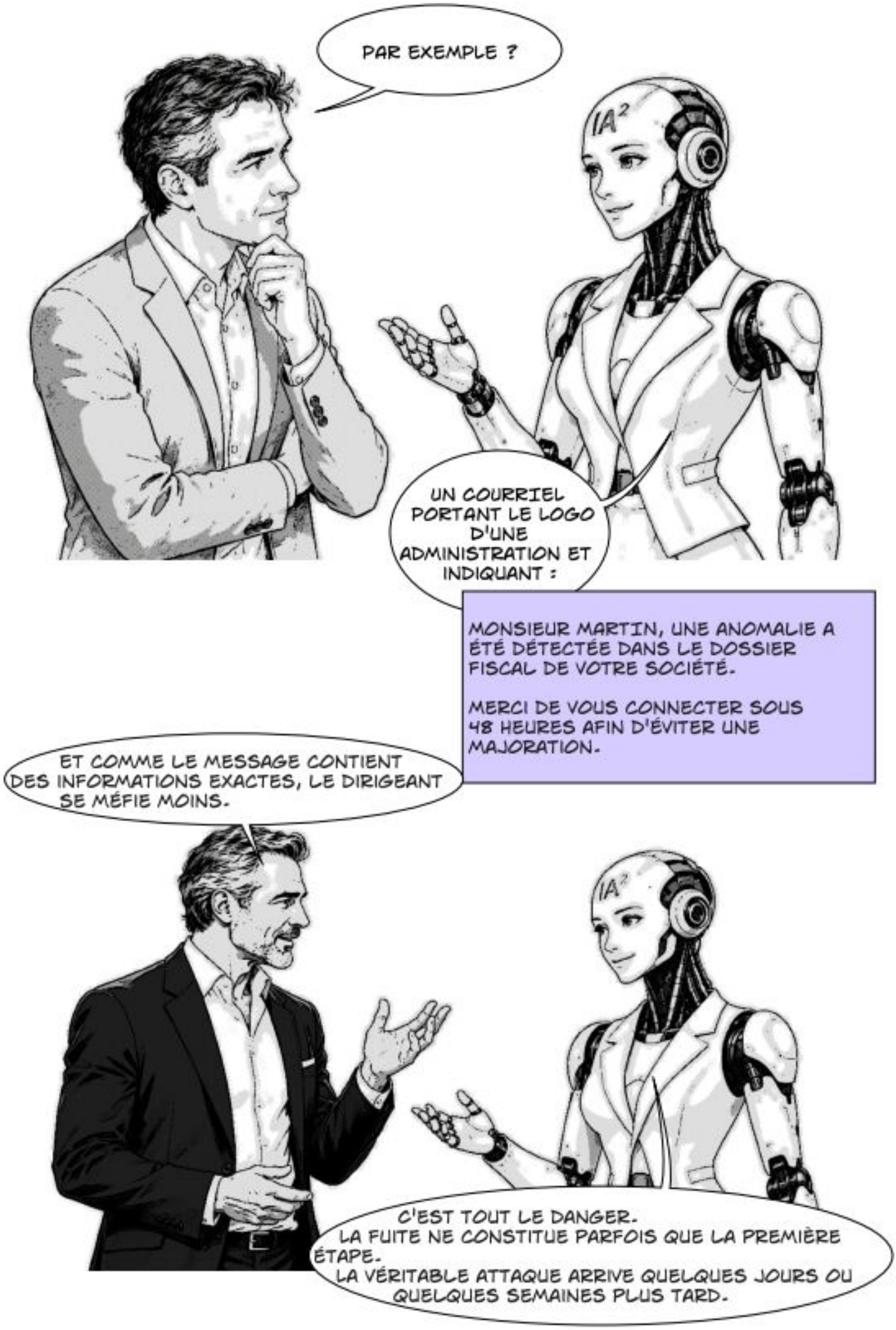
(1) INTELLIGENCE ASSURANTIELLE GESCO SA

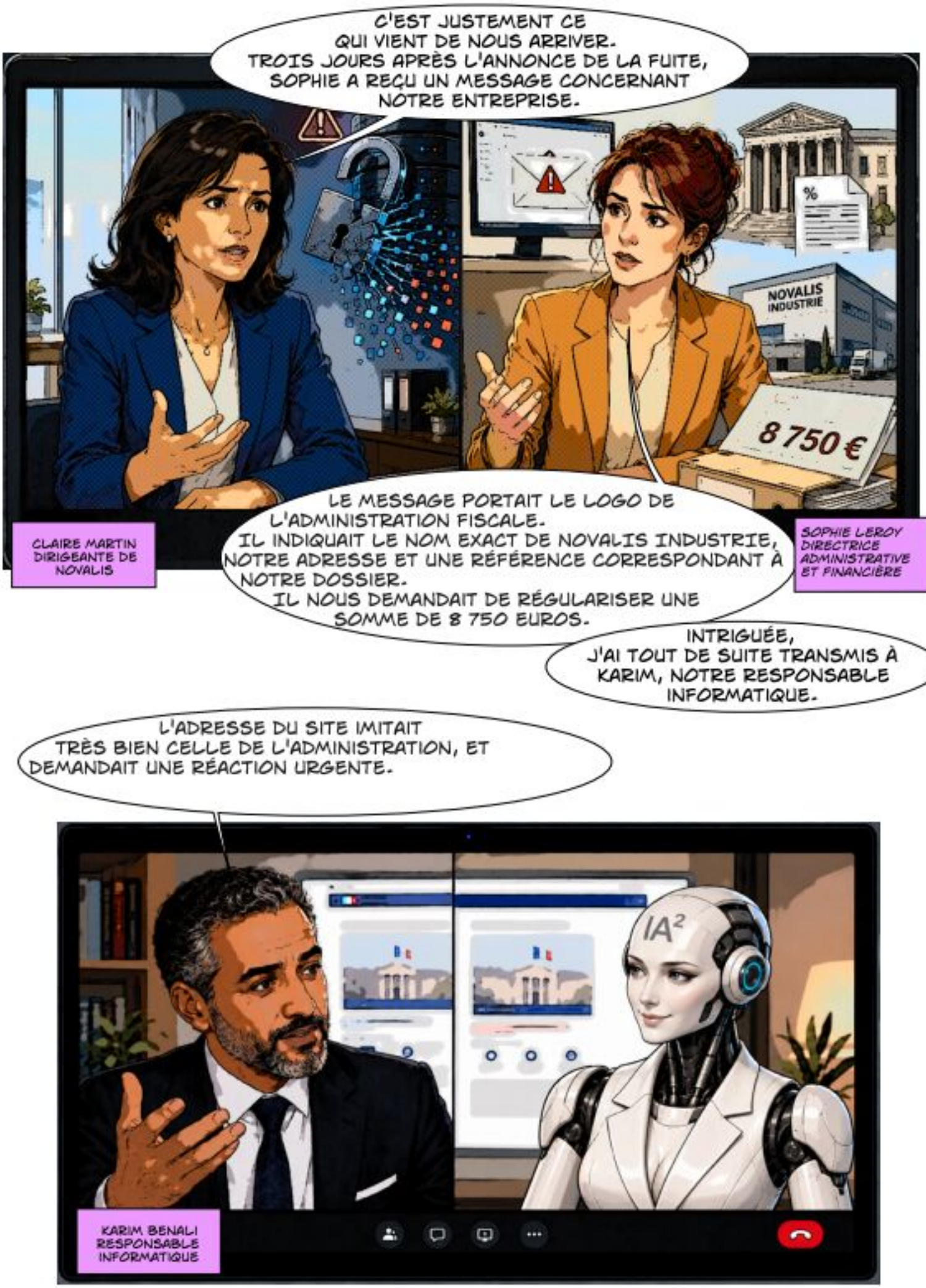
POURQUOI LES PIRATES S'INTÉRESSENT-ILS AUTANT AUX DONNÉES DÉTENUES PAR UNE ADMINISTRATION FISCALE ?


SELON LES SYSTÈMES CONCERNÉS, LES PIRATES PEUVENT RECHERCHER :
- DES IDENTITÉS;
- DES COORDONNÉES;
- DES INFORMATIONS PROFESSIONNELLES;
- DES RÉFÉRENCES ADMINISTRATIVES;
- DES INFORMATIONS FISCALES;
- DES DONNÉES RELATIVES À DES ENTREPRISES OU LEURS DIRIGEANTS ...

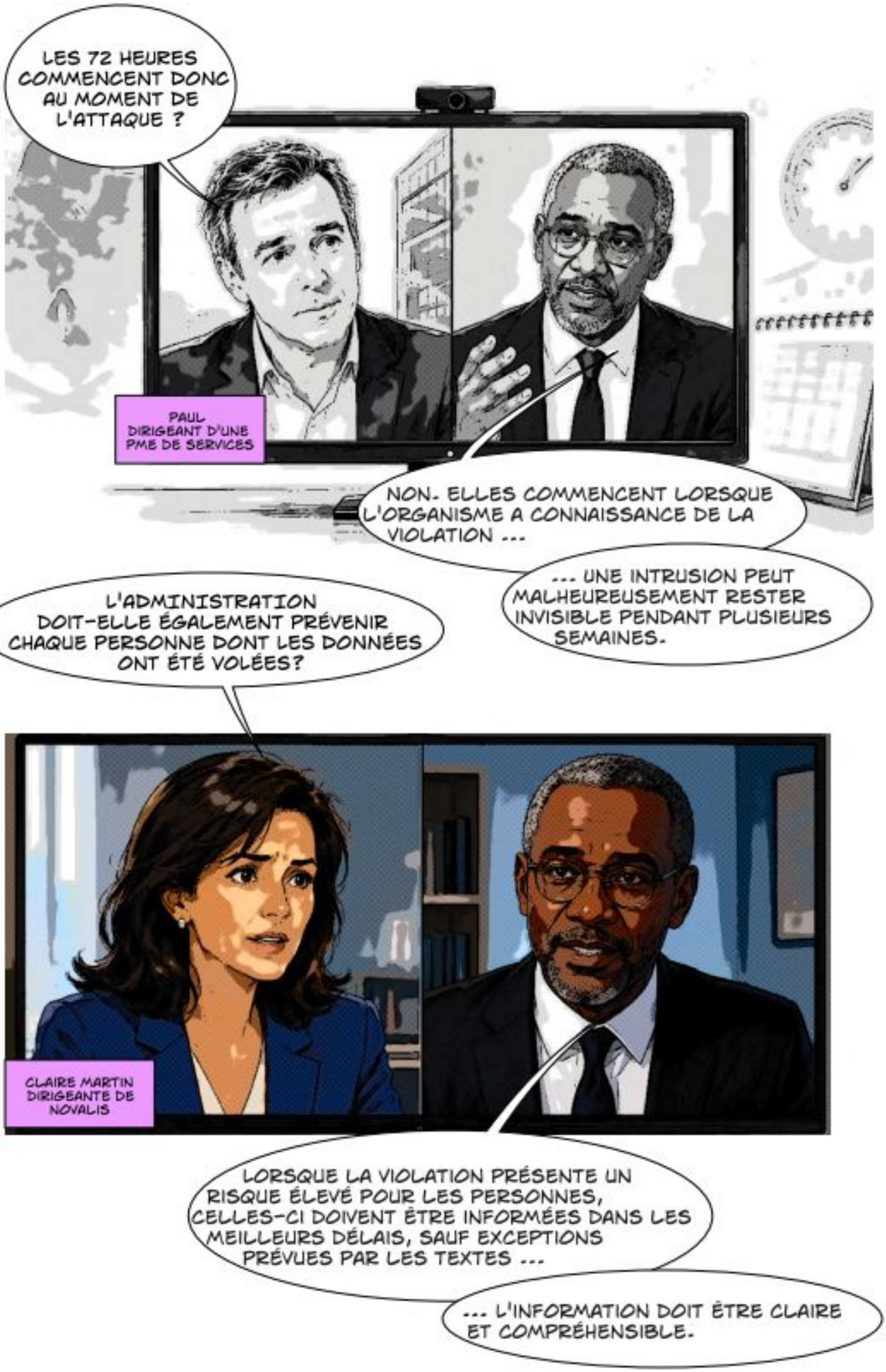
UN NOM, UNE ADRESSE, ET UNE RÉFÉRENCE ADMINISTRATIVE PEUVENT SUFFIRE POUR FABRIQUER UNE ATTAQUE EXTRÊMEMENT CRÉDIBLE...
IA²

... ET VOUS ENVOYER UN MESSAGE QUI SEMBLE PARFAITEMENT AUTHENTIQUE !
IA²


PAR EXEMPLE ?
IA²
UN COURRIEL PORTANT LE LOGO D'UNE ADMINISTRATION ET INDIQUANT :
MONSIEUR MARTIN, UNE ANOMALIE A ÉTÉ DÉTECTÉE DANS LE DOSSIER FISCAL DE VOTRE SOCIÉTÉ.
MERCI DE VOUS CONNECTER SOUS 48 HEURES AFIN D'ÉVITER UNE MAJORATION.
ET COMME LE MESSAGE CONTIENT DES INFORMATIONS EXACTES, LE DIRIGEANT SE MÉFIE MOINS.
IA²
C'EST TOUT LE DANGER.
LA FUITE NE CONSTITUE PARFOIS QUE LA PREMIÈRE ÉTAPE.
LA VÉRITABLE ATTAQUE ARRIVE QUELQUES JOURS OU QUELQUES SEMAINES PLUS TARD.


C'EST JUSTEMENT CE QUI VIENT DE NOUS ARRIVER. TROIS JOURS APRÈS L'ANNONCE DE LA FUITE, SOPHIE A REÇU UN MESSAGE CONCERNANT NOTRE ENTREPRISE.
NOVALIS INDUSTRIE
8 750 €
LE MESSAGE PORTAIT LE LOGO DE L'ADMINISTRATION FISCALE. IL INDIQUAIT LE NOM EXACT DE NOVALIS INDUSTRIE, NOTRE ADRESSE ET UNE RÉFÉRENCE CORRESPONDANT À NOTRE DOSSIER. IL NOUS DEMANDAIT DE RÉGULARISER UNE SOMME DE 8 750 EUROS.
CLAIRE MARTIN DIRIGEANTE DE NOVALIS
SOPHIE LEROY DIRECTRICE ADMINISTRATIVE ET FINANCIÈRE
INTRIGUÉE, J'AI TOUT DE SUITE TRANSMIS À KARIM, NOTRE RESPONSABLE INFORMATIQUE.
L'ADRESSE DU SITE IMITAIT TRÈS BIEN CELLE DE L'ADMINISTRATION, ET DEMANDAIT UNE RÉACTION URGENTE.
IA²
KARIM BENALI RESPONSABLE INFORMATIQUE

REVENONS À LA FUITE INITIALE ...
... LORSQU'UNE ADMINISTRATION DÉCOUVRE QU'UN PIRATE A PU ACCÉDER À SES DONNÉES, QUE DOIT-ELLE FAIRE ?
COMME TOUT RESPONSABLE DE TRAITEMENT DE DONNÉES PERSONNELLES, ELLE DOIT DABORD ÉVALUER L'INCIDENT...
MAÎTRE ANTOINE VAUTRIN, AVOCAT SPÉCIALISÉ EN PROTECTION DES DONNÉES
ELLE DOIT NOTAMMENT :
- IDENTIFIER LES SYSTÈMES ET LES DONNÉES CONCERNÉS
- CONTENIR L'INTRUSION
- PRÉSERVER LES ÉLÉMENTS NÉCESSAIRES À L'ENQUÊTE
- DOCUMENTER LA VIOLATION
- ÉVALUER LES CONSÉQUENCES POSSIBLES POUR LES PERSONNES.
72 H
DOIT-ELLE PRÉVENIR LA CNIL ?
LORSQUE LA VIOLATION EST SUSCEPTIBLE DE PRÉSENTER UN RISQUE POUR LES DROITS ET LIBERTÉS DES PERSONNES, ELLE DOIT ÊTRE NOTIFIÉE À LA CNIL DANS LES MEILLEURS DÉLAIS ET, SI POSSIBLE, DANS LES 72 HEURES SUIVANT SA DÉCOUVERTE.

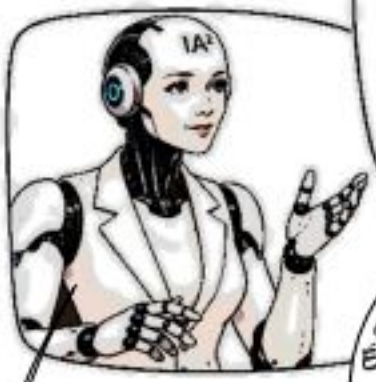

LES 72 HEURES COMMENCENT DONC AU MOMENT DE L'ATTAQUE ?
PAUL DIRIGEANT D'UNE PME DE SERVICES
NON. ELLES COMMENCENT LORSQUE L'ORGANISME A CONNAISSANCE DE LA VIOLATION ...
... UNE INTRUSION PEUT MALHEUREUSEMENT RESTER INVISIBLE PENDANT PLUSIEURS SEMAINES.
L'ADMINISTRATION DOIT-ELLE ÉGALEMENT PRÉVENIR CHAQUE PERSONNE DONT LES DONNÉES ONT ÉTÉ VOLÉES?
CLAIRE MARTIN DIRIGEANTE DE NOVALIS
LORSQUE LA VIOLATION PRÉSENTE UN RISQUE ÉLEVÉ POUR LES PERSONNES, CELLES-CI DOIVENT ÊTRE INFORMÉES DANS LES MEILLEURS DÉLAIS, SAUF EXCEPTIONS PRÉVUES PAR LES TEXTES ...
... L'INFORMATION DOIT ÊTRE CLAIRE ET COMPRÉHENSIBLE.

QUE DEVRAIT CONTENIR CETTE INFORMATION ?

ELLE DEVRAIT NOTAMMENT PRÉCISER :
- LA NATURE DE L'INCIDENT,
- LES CATÉGORIES DE DONNÉES CONCERNÉES,
- LES CONSÉQUENCES POSSIBLES,
- LES MESURES DÉJÀ PRISES,
- LES PRÉCAUTIONS RECOMMANDÉES,
- UN POINT DE CONTACT PERMETTANT D'OBTENIR DES RENSEIGNEMENTS.

INFORMER TROP VITE NE RISQUE-T-IL PAS D'INQUIÉTER INUTILEMENT LES CITOYENS ?

ET INFORMER TROP TARD PEUT EMPÊCHER LES VICTIMES DE SE PROTÉGER.



TOUT L'ENJEU EST LÀ. LA COMMUNICATION DE CRISE DOIT ÉVITER DEUX ÉCUEILS :
- MINIMISER UN INCIDENT SÉRIEUX
- ANNONCER COMME CERTAINES DES INFORMATIONS ENCORE NON VÉRIFIÉES.

UNE BONNE COMMUNICATION PEUT DIRE :
« VOICI CE QUE NOUS SAVONS. VOICI CE QUE NOUS NE SAVONS PAS ENCORE. VOICI CE QUE NOUS FAISONS. ET VOICI CE QUE VOUS POUVEZ FAIRE DÈS MAINTENANT. »

C'EST DONC UNE FORME DE TRANSPARENCE ORGANISÉE.

OUI. LA TRANSPARENCE NE CONSISTE PAS À TOUT ANNONCER DANS LA PRÉCIPITATION. ELLE CONSISTE À COMMUNIQUER RÉGULIÈREMENT DES INFORMATIONS EXACTES ET UTILES.

SI MON ENTREPRISE EST VICTIME D'UNE ATTAQUE CONSÉCUTIVE À CETTE FUITE, MON ASSURANCE CYBER INTERVIENDRA-T-ELLE ?

CELA DÉPEND DU CONTRAT QUE VOUS AVEZ SOUSCRIT.

L'ASSURANCE CYBER N'EST PAS SIMPLE.
EXEMPLE :
- SI L'ENTREPRISE EFFECTUE UN VIREMENT POUR LE COMPTE D'UN ESCROC, LA FRAUDE FINANCIÈRE N'EST PAS AUTOMATIQUEMENT COUVERTE.
- ELLE PEUT RELEVER D'UNE GARANTIE FRAUDE/TRANSFERT DE FONDS SPÉCIFIQUE.

D'OÙ VOTRE INTÉRÊT À CONSULTER UN SPÉCIALISTE EN CYBERRISQUES...

... VOILÀ POURQUOI GESCO A CRÉÉ UN NOUVEAU SITE SPÉCIALISÉ, ET S'EST DOTÉ D'UNE IA2
CyberRisques
UNE INITIATIVE ASSURANCES GESCO
L'ASSURANCE CYBERRISQUES SANS FAILLE
IA²
POUR ÊTRE CONSEILLÉ : 01 48 37 68 68
https://cyberrisques-assurances-gesco.fr/
01 48 37 68 68