L'incident sans attaquant : le contournement devant la SEC

Le 11 mai 2026, une banque régionale de Pennsylvanie a déclaré au régulateur boursier américain un incident de cybersécurité « matériel » sans intrusion, sans rançon et sans panne. Des données clients avaient été traitées au moyen d'un outil d'intelligence artificielle non autorisé, ce que l'usage appelle désormais l'IA fantôme. Le droit boursier range l'événement parmi les incidents de sécurité. La théorie des contournements de Steven Alter le range parmi les adaptations du travail. L'article soutient que cet écart de classement décide de ce que l'organisation corrigera, et de ce qu'elle laissera intact.

Par Alexandre Berge · 13 octobre 2026 · 16 min de lecture · Chronique

Un incident matériel où rien n'a été forcé

CB Financial Services, société cotée au Nasdaq et maison mère de Community Bank, a déposé le 11 mai 2026 un formulaire 8-K (la déclaration d'événement courant que les sociétés cotées américaines doivent publier sous quelques jours) au titre de la rubrique 1.05, réservée aux incidents de cybersécurité jugés matériels. Le document, signé par son président-directeur général, tient en cinq paragraphes. Il expose que la banque a pris connaissance, le 5 mai, d'un incident interne portant sur le traitement d'informations clients non publiques au moyen d'une « unauthorized artificial intelligence-based software application » (une application logicielle d'intelligence artificielle non autorisée). La banque a sécurisé les informations concernées et ouvert une enquête interne avec des conseils extérieurs en cybersécurité. Le périmètre et la cause profonde de l'incident restent, à la date du dépôt, en cours d'examen.

Le texte précise ce qui ne s'est pas produit : aucune perturbation des opérations, de l'accès des clients à leurs comptes, des systèmes de paiement ni de l'infrastructure informatique centrale, aucun effet matériel attendu sur la situation financière consolidée. La société a pourtant jugé l'événement matériel le 7 mai, en raison du volume et de la nature sensible des informations en cause, parmi lesquelles figurent des noms, des numéros de sécurité sociale et des dates de naissance. Elle indique procéder aux notifications prévues par le droit fédéral et le droit des États, et se trouver en relation avec ses régulateurs bancaires.

Le document ne dit ni combien de clients sont concernés, ni quel outil a été employé, par qui,

ni pourquoi. Ce qui reste suffit à l'analyse : un événement **interne**, survenu **dans le traitement ordinaire** de données clients, au moyen d'un outil **non autorisé**, et qualifié de matériel sans qu'aucun système ait été pénétré. C'est ce que le titre appelle un incident sans attaquant.

L'IA fantôme désigne l'usage, par les salariés, d'outils d'intelligence artificielle que l'organisation n'a ni choisis ni validés. Très commenté, le phénomène apparaît rarement dans un document opposable : à la date du 18 octobre 2026, une recherche plein texte sur la base EDGAR de la SEC, limitée aux formulaires 8-K, ne renvoie pour l'expression « unauthorized artificial intelligence » qu'à ce seul dépôt.

> **Ce que dit le document, et ce qu'il ne dit pas**
>
> Le 8-K fixe trois dates : la découverte (5 mai 2026), la décision de matérialité (7 mai), le dépôt (11 mai), soit deux jours ouvrés après la décision, dans le délai réglementaire de quatre jours ouvrés. Il nomme trois catégories de données divulguées (noms, numéros de sécurité sociale, dates de naissance) et écarte quatre conséquences (opérations, accès clients, paiements, infrastructure). Il décrit la réponse en trois termes : renforcement des contrôles existants, ajout de contrôles, surveillance accrue. Il ne mentionne ni le nombre de personnes concernées, ni l'outil, ni le motif de son usage, ni l'existence d'un outil autorisé équivalent.

La catégorie d'incident a été écrite contre l'intrus, elle saisit désormais un geste de travail

La rubrique 1.05 procède d'une règle adoptée par la SEC le 26 juillet 2023 et entrée en vigueur le 5 septembre suivant. Son texte de présentation situe l'enjeu sans ambiguïté : multiplication des attaques, essor des rançongiciels, menaces étatiques, acteurs malveillants capables d'exploiter la moindre divulgation. La règle a été pensée face à un adversaire.

Sa définition, elle, n'en exige aucun. Le Regulation S-K (le corpus des obligations d'information des sociétés cotées) entend par incident de cybersécurité un événement non autorisé, survenu dans les systèmes d'information de l'émetteur ou conduit par leur intermédiaire, qui compromet la confidentialité, l'intégrité ou la disponibilité de ces systèmes ou des informations qu'ils contiennent. La Commission a précisé que le terme devait être interprété largement. Elle a ajouté que la matérialité ne se mesure pas seulement à l'aune financière : un vol d'informations peut être matériel par l'ampleur ou la nature du préjudice causé aux personnes, même lorsqu'aucun seuil comptable n'est franchi.

Le choix de la rubrique n'est pas neutre. En mai 2024, le directeur de la division du financement des entreprises de la SEC a rappelé que la rubrique 1.05 est réservée aux incidents que l'émetteur a lui-même jugés matériels, les autres pouvant être déclarés volontairement sous la rubrique 8.01, consacrée aux événements divers. En déposant sous la rubrique 1.05, la banque a donc reconnu la matérialité, et non simplement signalé un fait.

Une catégorie construite pour décrire l'action d'un adversaire s'applique, par la largeur de sa définition, à un usage interne d'outil. Une fois classé, l'événement est gouverné comme un événement de sécurité, jusque dans le vocabulaire de sa remédiation. Le classement n'est pas faux. Il est incomplet.

Ce que la sécurité nomme incident, la théorie du travail nomme contournement

La recherche en systèmes d'information dispose d'un cadre qui saisit le même événement depuis l'autre bord. Steven Alter, professeur à l'université de San Francisco, a proposé en 2014 une théorie intégrée des contournements, construite à partir de plus de trois cents articles couvrant la santé, les administrations, les centres d'appels et les progiciels de gestion.

> **Le contournement (*workaround*), selon Steven Alter (2014)**
>
> Dans « Theory of Workarounds » (*Communications of the Association for Information Systems*, vol. 34, art. 55, 2014), Alter définit le contournement comme une adaptation, une improvisation ou une modification d'un système de travail existant, orientée vers un but, destinée à surmonter, éviter ou atténuer des obstacles, des exceptions, des pratiques établies ou des contraintes perçues comme empêchant d'atteindre le niveau d'efficacité ou d'efficience recherché. Quatre conditions préalables en découlent : un processus ou une règle en place, un but de l'acteur, un obstacle perçu, la capacité d'imaginer et d'exécuter une autre voie. Deux exclusions comptent ici : les actes d'acteurs extérieurs au système de travail (attaques, sabotages) et les simples erreurs d'inattention ne sont pas des contournements.

La définition coupe exactement là où passe la catégorie boursière, mais de l'autre côté. Ce que le Regulation S-K englobe (tout événement non autorisé, quelle qu'en soit l'origine), Alter le scinde. L'attaque relève de la menace. L'erreur relève de l'accident. Le contournement relève du travail : il est le fait d'un participant légitime, qui poursuit un but de travail et rencontre un obstacle. Si l'usage décrit par le 8-K visait un but professionnel, il a la forme d'un contournement. Le document ne l'établit pas, et l'article ne le présume pas pour ce cas. Il examine le mécanisme que cette forme désigne, et qui est documenté ailleurs.

Alter résume sa démarche d'une formule : sa théorie « turns agency theory on its head » (prend la théorie de l'agence à rebours). Là où la théorie de l'agence cherche à aligner l'agent sur les buts du mandant, la théorie des contournements part de l'agent qui décide de suivre ou non la voie prescrite, y compris lorsque ses buts sont alignés sur ceux de l'organisation. Le modèle d'Alter fait intervenir plusieurs facteurs dans cette décision : l'architecture et les règles du système de travail, les objectifs de performance qui pèsent sur l'acteur, les obstacles de la situation, les connaissances disponibles, le système de récompense, et le système de surveillance, qui détermine la probabilité qu'un contournement contestable soit détecté. Parmi les effets directs recensés figure, explicitement, l'exposition

d'informations qui auraient dû rester privées.

La catégorie de sécurité demande ce qui a été compromis. La théorie des contournements demande quel obstacle a rendu l'autre voie préférable.

La réponse annoncée ne traite qu'une case du modèle

Le 8-K décrit les mesures prises en trois termes : renforcer les contrôles existants, en mettre en place de nouveaux, accroître la surveillance. Rapportées au modèle d'Alter, ces trois mesures agissent sur un seul facteur, le système de surveillance. Elles élèvent le coût perçu du contournement en augmentant sa probabilité de détection. Le document ne mentionne rien qui porte sur les autres facteurs : l'obstacle qui a rendu l'outil non autorisé attractif, les objectifs de performance de la fonction concernée, la disponibilité d'un outil autorisé équivalent.

Cette absence ne vaut pas reproche. La règle de la SEC demande la nature, l'étendue, le calendrier et l'impact de l'incident, et dispense expressément l'émetteur des détails techniques sur sa réponse qui gêneraient la remédiation. C'est précisément le point. **La catégorie qui saisit l'événement oriente le vocabulaire de sa correction, et ce vocabulaire ne contient pas le mot qui nommerait sa cause probable.**

Le discours dominant sur la gouvernance de l'IA en entreprise se formule en chartes d'usage, en listes d'outils approuvés et en dispositifs de détection. Il traite l'IA fantôme comme un écart à la règle. Ce qu'il ne formule pas, c'est que la demande qui produit l'écart survit à la règle. Alter rapporte une observation tirée d'une étude de projets : plus un système de contrôle se resserre, plus il peut produire de contournements et de données fausses destinées à le satisfaire.

Les mesures disponibles de cette demande émanent surtout d'éditeurs. L'étude annuelle de Microsoft et LinkedIn publiée le 8 mai 2024, conduite par Edelman Data & Intelligence auprès de 31 000 travailleurs du savoir dans 31 pays entre le 15 février et le 28 mars 2024, indique que 78 % des utilisateurs d'IA au travail y recourent avec des outils que leur organisation ne leur fournit pas, et que 68 % des répondants disent peiner face au rythme et au volume de travail. L'émetteur vend des outils d'IA aux entreprises et a intérêt à décrire une demande non servie. Le chiffre ne prouve rien à lui seul, mais il dessine le mécanisme : l'obstacle invoqué est la charge de travail, l'outil personnel en est le contournement.

En 2006, un analyste et un disque dur avaient déjà écrit le scénario

Le 3 mai 2006, le domicile d'un spécialiste informatique du département américain des Anciens combattants est cambriolé. Un ordinateur portable personnel et un disque dur externe sont emportés. Le disque contient vraisemblablement des extraits de bases de données portant sur environ 26 millions d'anciens combattants : noms, numéros de sécurité

sociale, dates de naissance. Les catégories de données sont celles du 8-K de 2026.

Le rapport de l'inspecteur général du département, publié le 11 juillet 2006, établit les faits avec une précision que le 8-K n'offre pas. L'agent avait un accès légitime à ces bases pour ses missions. Il n'avait ni besoin ni autorisation de les emporter chez lui. Il le faisait depuis 2003, sans en demander la permission, pour un projet d'analyse lié à l'activité du département, qu'il travaillait chez lui parce qu'il ne parvenait pas à y consacrer assez de temps au bureau. Il avait disposé en 2004 et 2005 d'un portable de service avec accès distant sécurisé. Après l'avoir restitué en janvier 2006, il a continué à travailler chez lui, avec son matériel personnel. Sa dernière évaluation lui attribuait la meilleure note du barème. Le matériel a été retrouvé intact le 28 juin, et les enquêteurs se sont déclarés très confiants dans l'absence de compromission des fichiers.

Tous les éléments du modèle d'Alter y figurent : un participant légitime, un but de travail, un obstacle (le temps disponible au bureau), un outil officiel retiré, une voie personnelle substituée. Le cambrioleur n'a été que l'occasion. L'exposition des données préexistait au vol.

Le rapport documente aussi l'aveuglement catégoriel. Le centre des opérations de sécurité du département a mis douze jours à conclure que l'affaire relevait de la protection de la vie privée plutôt que de la cybersécurité, et l'a renvoyée au correspondant qui la lui avait signalée. L'inspecteur général relève que les politiques prises en application du droit de la sécurité de l'information visaient à protéger les systèmes « from unauthorized intrusions and viruses » (contre les intrusions non autorisées et les virus). Il constate qu'aucune politique ne protégeait alors une information sortie des systèmes du département par la main d'un agent. Les six recommandations du rapport portent sur une politique unifiée de protection des données, la formation obligatoire, la classification des postes sensibles, les clauses contractuelles et les critères de signalement des incidents. Aucune ne porte sur la raison pour laquelle un analyste apprécié travaillait chez lui sur des fichiers nominatifs. Vingt ans séparent les deux cas. La structure est identique, et le registre de la correction aussi.

Les conditions qui font d'un contournement un incident

Une chronique antérieure lisait l'IA fantôme des collectivités comme une innovation ordinaire, au sens de Norbert Alter. Le cas présent déplace la question vers ce que la catégorie qui saisit l'usage clandestin fait de lui.

Le mécanisme se formule sans nom d'organisation : **lorsqu'un participant légitime contourne l'outil officiel pour atteindre un but de travail, et que la voie choisie fait sortir des données sensibles, l'événement est saisi par une catégorie de sécurité conçue contre l'intrus, et la réponse qu'elle appelle porte sur la détection plutôt que sur l'obstacle.** Trois conditions en rendent la reproduction probable dans n'importe quelle organisation.

La première est un écart d'effort : pour la tâche réelle, au guichet ou au service de gestion, l'outil autorisé coûte plus de temps que l'outil grand public disponible sur tout téléphone. Il suffit que l'écart soit perçu et répété.

La deuxième est la présence de données sensibles dans le flux ordinaire de la tâche. Un contournement portant sur des documents publics ne produit pas d'incident, celui qui porte sur des dossiers clients en produit un dès qu'il quitte le périmètre. Les organisations dont le cœur de métier consiste à traiter des données personnelles (banques, assureurs, mutuelles, établissements de santé, organismes de protection sociale) remplissent donc la condition par construction.

La troisième est une catégorie de déclaration à la fois orientée vers l'intrus et définie assez largement pour absorber l'événement après coup. Le droit européen présente cette propriété. Le règlement général sur la protection des données vise, dans son considérant 83, les destructions, pertes, altérations et divulgations non autorisées survenues de manière accidentelle ou illicite, et son considérant 85 rappelle l'obligation de notifier l'autorité de contrôle dans les 72 heures lorsque c'est possible. Une organisation française se trouverait dans la même position : un événement de travail, déclaré dans une catégorie de sécurité, corrigé dans le vocabulaire du contrôle.

Le mécanisme devient visible à quelques signes : un nombre d'interdictions d'outils qui croît plus vite que le nombre d'outils fournis, des alertes de fuite de données concentrées sur quelques fonctions sous forte pression de production, des incidents classés en sécurité dont aucune analyse ne remonte jusqu'à l'organisation du travail.

> **Grille de lecture**
>
> 1. Pour les trois tâches les plus fréquentes d'une fonction qui manipule des données clients, le temps d'exécution avec l'outil autorisé a-t-il été mesuré et comparé à celui d'un outil grand public ?
> 2. Les mesures prises après le dernier incident lié à un usage non autorisé portent-elles uniquement sur la détection et la sanction, ou aussi sur l'outil mis à disposition et la charge de la fonction concernée ?
> 3. Le registre des incidents permet-il de distinguer une attaque, une erreur et un contournement, ou range-t-il les trois dans la même catégorie ?
> 4. La dernière extension de la liste des outils interdits a-t-elle été accompagnée d'une extension de la liste des outils fournis ?

Conclusion : le prochain incident sans attaquant dira si la leçon a changé de case

L'incident sans attaquant n'est pas une curiosité réglementaire. Il est le point où deux lectures d'un même geste se rencontrent dans un document opposable : celle de la sécurité, qui voit

une compromission, et celle du travail, qui voit un contournement. Seule la première dispose d'une catégorie, d'un délai et d'un vocabulaire dans les formats de déclaration. Tant que le contournement n'est lu qu'à travers la catégorie de l'incident, sa correction porte sur la case de la surveillance et laisse les autres cases du modèle intactes.

L'hypothèse se vérifie de l'extérieur. Si le mécanisme décrit est général, la recherche plein texte EDGAR sur l'expression « unauthorized artificial intelligence » et ses variantes renverra, au 31 octobre 2027, au moins deux autres émetteurs ayant déposé un 8-K au titre de la rubrique 1.05 pour un incident de même nature, et leurs paragraphes de remédiation seront rédigés, comme celui de 2026, dans le seul vocabulaire du contrôle et de la surveillance. Un second indicateur arrivera plus tôt : le rapport annuel 10-K de CB Financial Services pour l'exercice 2026, attendu au premier trimestre 2027, dont la rubrique consacrée à la gestion des risques de cybersécurité dira si l'usage des outils d'IA y est décrit comme un risque d'intrusion ou comme une question d'équipement du travail. La question plus large reste ouverte : à quoi ressemblerait une déclaration d'incident qui décrirait le système de travail, et pas seulement le système d'information ?

Note méthodologique

L'analyse s'appuie principalement sur le 8-K de CB Financial Services, la règle de la SEC de juillet 2023 et sa définition codifiée, le rapport de l'inspecteur général du département des Anciens combattants de 2006 et l'article de Steven Alter. L'affirmation d'unicité du dépôt est bornée à une recherche plein texte EDGAR sur l'expression exacte « unauthorized artificial intelligence », limitée aux formulaires 8-K et effectuée le 18 octobre 2026. Les affirmations d'absence sur les mesures annoncées sont bornées au texte du 8-K. Le motif de l'usage, non public en 2026, n'est pas présumé, le mécanisme étant établi par le cas de 2006. La théorie des contournements est retenue comme cadre central plutôt que l'innovation ordinaire de Norbert Alter, déjà mobilisée dans une chronique antérieure, parce qu'elle seule permet de rapporter la réponse annoncée aux facteurs de la décision de contourner. L'étude Microsoft et LinkedIn est présentée comme une étude d'éditeur et n'appuie aucune affirmation structurante à elle seule. Recherche de sources, croisement des données et structuration du raisonnement s'appuient sur une assistance par intelligence artificielle. Le choix de l'angle et du cadre théorique, la vérification des sources, les arbitrages et l'établissement du texte final relèvent de l'auteur.

Sources

Documents des organisations et textes officiels

- CB Financial Services, Inc., Form 8-K, Item 1.05 « Material Cybersecurity Incidents », date de l'événement le plus ancien déclaré : 7 mai 2026, signé le 11 mai 2026. https://

www.sec.gov/Archives/edgar/data/1605301/000160530126000021/cbfv-20260507.htm

- Securities and Exchange Commission, « Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure », Release Nos. 33-11216 et 34-97989, adoptée le 26 juillet 2023, publiée au Federal Register le 4 août 2023 (88 FR 51896). https://www.sec.gov/files/rules/final/2023/33-11216.pdf
- 17 CFR 229.106 (Regulation S-K, Item 106, Cybersecurity), version consolidée eCFR, consultée le 18 octobre 2026. https://www.ecfr.gov/current/title-17/chapter-II/part-229/subpart-229.100/section-229.106
- Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 (règlement général sur la protection des données), Journal officiel de l'Union européenne L 119 du 4 mai 2016, considérants 83 et 85. https://eur-lex.europa.eu/legal-content/FR/TXT/HTML/?uri=CELEX:32016R0679

Décisions et déclarations d'autorités

- Erik Gerding, directeur de la Division of Corporation Finance, Securities and Exchange Commission, « Disclosure of Cybersecurity Incidents Determined To Be Material and Other Cybersecurity Incidents », déclaration du 21 mai 2024. https://www.sec.gov/newsroom/speeches-statements/gerding-cybersecurity-incidents-05212024
- Securities and Exchange Commission, EDGAR Full-Text Search, requête « unauthorized artificial intelligence » limitée aux formulaires 8-K, consultée le 18 octobre 2026. https://efts.sec.gov/LATEST/search-index?q=%22unauthorized%20artificial%20intelligence%22&forms=8-K

Études et statistiques

- Microsoft et LinkedIn, « AI at Work Is Here. Now Comes the Hard Part », 2024 Work Trend Index Annual Report, 8 mai 2024 (enquête Edelman Data & Intelligence, 31 000 répondants, 31 pays, 15 février au 28 mars 2024, étude d'éditeur). https://www.microsoft.com/en-us/worklab/work-trend-index/ai-at-work-is-here-now-comes-the-hard-part

Cadres théoriques

- Steven Alter, « Theory of Workarounds », *Communications of the Association for Information Systems*, vol. 34, art. 55, p. 1041-1066, mars 2014 (mise en ligne le 2 mars 2014), DOI 10.17705/1CAIS.03455. https://aisel.aisnet.org/cais/vol34/iss1/55/

Parallèle historique

- Department of Veterans Affairs, Office of Inspector General, « Review of Issues Related to the Loss of VA Information Involving the Identity of Millions of Veterans », rapport n° 06-02238-163, 11 juillet 2006. https://vaoig.gov/sites/default/files/reports/2006-07/

VAOIG-06-02238-163.pdf