ÉDITION 2024

TECH-RADAR DU COURTAGE

Guide des solutions
et pratiques pour organiser
sa cyber-résilience

PLANETE CSCA

EURUS

SOMMAIRE

LAURENT DEVORSINE
Gérant Cabinet DEVORSINE
& Président du LAB' PLANETE CSCA

"

Avec la publication du 5e Livre Blanc en collaboration avec INTERMEDIUS en 2023, le LAB' PLANETE CSCA a bien compris les enjeux des risques cyber.

Notre ambition est de construire un Tech Radar, un outil novateur destiné à aider les courtiers membres de notre syndicat à renforcer leur résilience face aux risques cyber.

À travers ce Tech Radar, nous souhaitons non seulement continuer à soutenir nos adhérents, mais aussi inspirer nos confrères dans leur quête d'une cybersécurité renforcée. Nous espérons que cet outil vous aidera à naviguer dans un paysage de menaces en constante évolution.

"

ERWAN LOMENECH
Partner
EÜRUS

"

EÜRUS est profondément engagé sur les enjeux de transformation et les questions de résilience du courtage. EÜRUS possède notamment une expertise reconnue, en ce qui concerne DORA (Digital Operational Resilience Act).

En collaborant avec le LAB' PLANETE CSCA, EÜRUS souhaite apporter sa connaissance approfondie du secteur et son expérience stratégique pour contribuer activement à la protection et à la résilience des cabinets de courtage face aux cybermenaces.

Il nous importe fortement de contribuer à ce sujet dans un paysage numérique de plus en plus complexe et risqué.

"

Face à l'augmentation des cybermenaces, qui ciblent les entreprises du secteur financier avec une intensité 300 fois supérieure à celle observée dans d'autres secteurs[1], ainsi qu'à leur diversité, telles que les ransomware et le phishing, les courtiers d'assurances doivent impérativement renforcer leur cyber-résilience. L'impact financier des cyberattaques est désormais colossal, avec des coûts estimés à 6 000 milliards de dollars[2], ce qui place ces menaces au rang de la 3e économie mondiale.

La cyber-résilience est devenue une tendance incontournable, notamment d'un point de vue réglementaire. La mise en œuvre du Digital Operational Resilience Act (DORA) par l'Union Européenne souligne cette évolution, en établissant des normes strictes pour renforcer la résilience opérationnelle des entités financières. Même si la majorité des courtiers d'assurances de proximité ne sont pas directement assujettis à ces régulations, l'adoption de telles mesures reflète une prise de conscience croissante face à l'augmentation des risques cyber. Investir dans la cyber-résilience n'est donc plus une option, mais une nécessité pour se prémunir contre les menaces en constante évolution et garantir la continuité des activités.

LE LAB' PLANETE CSCA & EÜRUS CONSULTING S'ASSOCIENT POUR GUIDER LE COURTAGE DANS L'ORGANISATION DE SA CYBER-RÉSILIENCE.

En adoptant des mesures de prévention puis en investissant dans des systèmes de sécurité avancés pour limiter et gérer les cyberattaques, les courtiers peuvent non seulement protéger les informations sensibles de leurs clients, particulièrement ciblées par les commanditaires, mais aussi répondre à la réglementation. Les témoignages de la profession affluent. Leur préparation a permis d'éviter le pire. Pour autant, de nombreux acteurs demeurent parfois insuffisamment mobilisés pour se prémunir de ce risque. Cette impréparation appelle à un sursaut de la profession, alors que les attaques sont appelées à s'intensifier[3].

Dans ce contexte, des initiatives de place sont essentielles pour encourager l'échange de bonnes pratiques et l'identification de solutions technologiques pertinentes. Ces efforts permettront aux courtiers de surmonter les défis posés par la cybersécurité tout en tirant parti des opportunités offertes par la transformation numérique.

Lancé en 2020, le LAB' PLANETE CSCA vient renforcer les rôles de représentation et de défense de la profession en s'attaquant aux enjeux sans précédent de digitalisation du secteur.

EÜRUS accompagne le LAB' PLANETE CSCA pour accélérer ses activités depuis 2023. Reconnu pour son expertise dans le courtage, ainsi que son expérience en matière de digitalisation, EÜRUS anime régulièrement des réflexions regroupant tous les courants de la profession.

Le LAB' PLANETE CSCA et EÜRUS s'associent pour la réalisation de Tech Radar sur la cyber-résilience, dans la continuité des travaux 2023 du Think Tank INTERMEDIUS[4].

[1] Zakrzewski et al. (2019), "Global Wealth 2019: Reigniting Radical Growth", Boston Consulting Group
[2] Sénat (2021), « La cyber sécurité des entreprises »
[3] FMI (2024), « L'intensification des cybermenaces suscite de grandes inquiétudes pour la stabilité financière »
[4] PLANETE CSCA / INTERMEDIUS (2023), « Risque Cyber » Livre Blanc

LES CONTRIBUTEURS DU PANORAMA

LAB' PLANETE CSCA

BERTRAND DE SURMONT
Président
PLANETE CSCA

LAURENT DEVORSINE
Gérant Cabinet DEVORSINE
& Président du LAB' PLANETE CSCA

JEAN-FRANÇOIS COUSIN
Président délégué
PLANETE CSCA

MAXIME BASTUCK
Chef de projet digital
O.M.A SAS

CHRISTOPHE HAUTBOURG
Directeur général
PLANETE CSCA

BENOIT BEAULIEU
Directeur Cybersécurité
DATTAK

EÜRUS

CAPUCINE BERNON
Directrice de la transformation digitale
Groupe CEA

ERWAN LOMENECH
Partner
EÜRUS

XAVIER THAMIN
Directeur du développement
ASQUA

ALEXANDRE GOMBAUD-SAINTONGE
Manager
EÜRUS

AMBININA IRIMANANA
Analyste
EÜRUS

NOTE DES AUTEURS

Le présent document s'inscrit dans un contexte actuel où la sécurité informatique et la résilience face aux cybermenaces sont des préoccupations majeures pour les entreprises.

Il est important de noter que ce domaine est en constante évolution, avec des risques cyber, des technologies et des approches qui se développent et se transforment rapidement.

Cette publication vise à fournir une vue d'ensemble accessible et informative sur le sujet, destinée à vulgariser les concepts clés et à partager des informations pertinentes. Cette publication a pour ambition de donner une première feuille de route aux courtiers s'interrogeant sur le sujet.

Les solutions présentées sont spécialisées, indépendantes, représentatives et adaptées au monde du courtage.

Cependant, le document ne prétend ni à l'exhaustivité ni à la complétude. Les solutions présentées ici ne doivent pas être interprétées comme des conseils personnalisés, et il est essentiel de considérer que les besoins et les contextes spécifiques de chaque courtier peuvent différer. Le LAB' PLANETE CSCA et EÜRUS souhaitent souligner que cette publication est un guide de référence et non une liste complète de recommandations. Les auteurs ne peuvent pas être tenus responsables des solutions technologiques mentionnées dans le présent guide et de leur exhaustivité.

Nous espérons que ce document vous sera utile pour mieux comprendre les enjeux de la cyber-résilience et les options disponibles, tout en gardant à l'esprit l'évolution perpétuelle au sein de ce domaine.

La cyber-résilience est un sujet complexe, faites-vous aider par des experts à vos côtés !

Pourquoi investir dans la cyber-résilience ?

95 %
des problèmes de cybersécurité seraient liés aux erreurs humaines.

Avec la digitalisation croissante des activités économiques, les entreprises sont de plus en plus exposées au risque de cyberattaque. Les assureurs et les courtiers sont visés au vu de la sensibilité et de la richesse de la donnée qu'ils détiennent. Selon IBM, 22 % des attaques dans le monde sont dirigées contre des banques et des assureurs ce qui en fait le deuxième secteur le plus exposé à ce risque[5]. Chaque année, les cyberattaques sont plus nombreuses, plus brutales et plus sophistiquées.

Également, selon le Global Risks Report, 95 % des problèmes de cybersécurité seraient liés aux erreurs humaines. Ainsi, l'information et la formation se retrouvent au cœur des enjeux de la cyber résilience. Investir dans la cyber-résilience n'est donc pas simplement une dépense, mais une protection essentielle pour l'avenir de votre entreprise. En effet, le coût moyen d'une cyberattaque en France est estimé à 59 000 € en 2022[6], en combinant les coûts directs et les coûts indirects.
Dans un contexte où les risques augmentent et où de nombreuses entreprises sont encore mal préparées, il est donc crucial d'agir.

Pour approfondir sur la question des risques cyber, nous vous invitons à consulter le 5e livre blanc de l'Institut INTERMEDIUS et PLANETE CSCA qui adresse cette préoccupation majeure.

UNE LARGE PALETTE DE MÉTHODES ACTIONNÉES PAR LES CYBERATTAQUANTS[7] :

PHISHING

Technique de fraude visant à obtenir des informations sensibles (comme des mots de passe) en se faisant passer pour une entité de confiance par email ou autres moyens de communication.

RANSOMWARE

Logiciel malveillant qui chiffre les données d'une victime et exige une rançon pour les déchiffrer.

ATTAQUE DDoS

Attaque par déni de service distribué, qui surcharge un serveur ou un réseau avec un trafic massif, le rendant inaccessible.

ATTAQUE ZERO-DAY

Attaque exploitant une vulnérabilité logicielle inconnue du fournisseur ou sans correctif disponible, exposant les systèmes à des risques avant que des mesures de protection puissent être mises en place.

MALWARE

Logiciel malveillant conçu pour infiltrer, endommager ou désactiver des ordinateurs, réseaux ou systèmes informatiques.

.... MAIS AUSSI les attaques par force brute, les injections SQL, les spywares, les attaques de l'homme du milieu (MitM).

Récurrence forte

Récurrence moyenne

Récurrence faible

[5] Abadie, A. (2022), Le risque cyber augmente pour le secteur financier, L'Agefi
[6] Asterès (2023), « Les cyberattaques réussies en France : un coût de 2 Mds€ en 2022 »
[7] Les probabilités sont issues du baromètre CESIN (2022)

DES RISQUES DE CYBERATTAQUES EN HAUSSE :

Une hausse de la fréquence *des cyberattaques*

+ 30 % de ransomwares en 2023[8]

- 385 000 cyberattaques réussies en France en 2022[9]
- Une cyberattaque a lieu toutes les 39 secondes dans le monde[10]
- + 13 % de fréquentation de cybermalveillance.gouv.fr en 2023[11]

« La situation n'est pas bonne. La menace croit. Plus grand monde n'est à l'abri. »[12]

Guillaume Poupard, Ex-Directeur général de l'ANSSI

Une surface d'exposition *en hausse*

Plus de 8 millions de salariés en télétravail rien qu'en 2020[13]

- + 667 % en moyenne d'attaques sur les comptes Cloud en 2020[14]
- 47 % des entreprises françaises ont intégré le télétravail dans leur mode de fonctionnement en 2023 (INSEE)[15]

« Le niveau de cybersécurité des entreprises doit être rapidement et fortement augmenté avant l'explosion de l'internet des objets (IoT), qui va étendre de façon exponentielle la surface d'exposition aux risques cyber, de l'ordinateur quantique qui démultipliera les capacités d'intrusion, ou encore de l'Intelligence Artificielle. »[16]

Sénat

Une plus grande vulnérabilité *des TPE & PME...*

50 % des TPE-PME ne sécurisent pas leurs postes de travail et 1/3 n'utilisent pas d'antivirus [17]

- 40 % des ransomwares entre 2021 et 2022 étaient destinés aux TPE-PME[18]
- Seuls 38 % des PME mettent à jour régulièrement leurs logiciels[19]
- 60 % des PME n'ont aucun référent dédié à la cybersécurité[2]

[8] ANSSI (2023), « Panorama de la Cybermenace »
[9] Cybermalveillance.gouv.fr (2023), « Rapport d'activité et état de la menace »
[10] Cyber Cover (2023), « Cybercriminalité : 10 chiffres clés à connaître en 2023 »
[11] Cybermalveillance.gouv.fr (2023), « Rapport d'activité et état de la menace »
[12] Conférence de presse du 10 juin 2021
[13] Sénat (2021), « La cyber sécurité des entreprises »
[14] Sénat (2021), « La cyber sécurité des entreprises »
[15] Droit Travail France.fr (2023), « Télétravail en France : bilan 2023 et perspectives d'avenir pour les entreprises »
[16] Sénat (2021), « La cyber sécurité des entreprises »
[17] PLANETE CSCA / INTERMEDIUS (2023,) « Risque Cyber » Livre Blanc
[18] Les Grands Themas (2022), « Les chiffres clés signifiants de la cyber-résilience »
[19] Cyber Cover (2023), Cybercriminalité : 10 chiffres clés à connaître en 2023 [1]
[20] PLANETE CSCA / INTERMEDIUS (2023,) « Risque Cyber » Livre Blanc

...et notamment des cabinets de courtage *de proximité*

53 % des cabinets disent avoir été victime d'une attaque informatique, principalement sous forme de rançongiciels[21]

La moitié des cabinets n'investit pas dans la cybersécurité[22] par :

- Manque de temps (54 %)
- Manque de budget (41 %)
- Manque de prise de conscience (28 %)
- Manque de compétence (23 %)

« Les cabinets de proximité pensent encore, à tort, que seules les grandes entreprises sont touchées. »[23]

Jules Veyrat, CEO de Stoïk,
extrait du 5e Livre blanc PLANETE CSCA/INTERMEDIUS

Des impacts majeurs *pour les entreprises victimes*

80 % des entreprises ayant perdu leurs données informatiques suite à une cyberattaque font faillite dans les 12 mois[24]

- + 667 % en moyenne d'attaques sur les comptes Cloud en 2020[14]
- 47 % des entreprises françaises ont intégré le télétravail dans leur mode de fonctionnement en 2023 (INSEE)[15]

« Dans les mois qui suivent, ces coûts de gestion de crise se transforment en coûts de désorganisation, par exemple dus à la perte d'efficacité du fait de systèmes non fonctionnels, de processus internes défaillants, de clients mécontents, puis en coûts de reconstruction et de sécurisation du système d'information. » [27]

Sénat

[21] PLANETE CSCA / INTERMEDIUS (2023,) « Risque Cyber » Livre Blanc
[22] PLANETE CSCA / INTERMEDIUS (2023,) « Risque Cyber » Livre Blanc
[23] PLANETE CSCA / INTERMEDIUS (2023,) « Risque Cyber » Livre Blanc
[24] Sénat (2021), « La cyber sécurité des entreprises »
[25] Freelance.com (2023), « Cybersécurité dans les banques et assurances : Quels sont les enjeux et les leviers ? »
[26] Carrère, M. (2020), « 45 % des clients prêts à quitter leur assureur en cas de cyberattaque » L'Argus de L'Assurance
[27] Sénat (2021), « La cyber sécurité des entreprises »

DES COÛTS SUPPLÉMENTAIRES GÉNÉRÉS PAR LES CYBERATTAQUES :

EXEMPLE 1

Une attaque subie par un cabinet de 2 collaborateurs

Prenons l'exemple d'un cabinet qui réalise 200 000 € de commissions en s'appuyant sur deux collaborateurs pour 500 clients professionnels et particuliers.

Ce courtier subit une cyberattaque lui causant une interruption d'activités de 5 jours et nécessitant le recours à un prestataire externe pour résoudre l'incident (1 ETP). Les coûts générés par l'incident peuvent s'élever entre 25 000 € et 30 000 € soit 15 % de ses commissions. Cette estimation de coûts se décomposerait de la manière suivante :

Veuillez noter que les symboles «€, €€, et €€€» utilisés dans la colonne «Importance des Coûts» indiquent le poids relatif des coûts par rapport au montant des commissions perçues par l'acteur.

TYPOLOGIES DE COÛTS	IMPORTANCE DES COÛTS[28]	ILLUSTRATION DE L'IMPACT
Réponse à l'incident et à la récupération	**€€**	**5 000 €** 1 000 € x 5 jours x 1 ETP
Perte de revenus durant l'interruption d'activité	**€€**	**4 600 €** 200 000 € x (5 jours/220 jours)
Frais de notification aux clients	**€€**	**6 000 €** 12 € de traitement du LRAR x 500 clients
Frais de gestion administrative de l'incident et relation client	**€€**	**5 000 €** 1 000 € x 5 jours x 1 ETP
Enquête et audits	**€€** (Coûts indirects)	**Entre 5 000 € et 8 000 €** Fourchette de prix d'un audit de sécurité
Amendes réglementaires	**€€€** (Coûts indirects)	Amende non-conformité à la RGPD
Atteinte à la réputation et à la confiance des clients et prospects	**€€** (Coûts indirects)	Perte potentielle de clients et prospects
Atteinte à la réputation et à la confiance des assureurs	**€€€** (Coûts indirects)	Perte de la délégation d'encaissement
Augmentation des primes d'assurance cyber	**€** (Coûts indirects)	**400 €** 200 € de primes avant augmentation + 200 %[29]
Exemple de coût total	**Entre 25 000 € et 30 000 €**	

[28] Par rapport aux commissions

[29] Deloitte (2022), « Beneath the surface of a cyberattack: A deeper look at business impacts »

EXEMPLE 2

Une attaque subie par un cabinet de 8 collaborateurs

Prenons maintenant l'exemple d'un autre cabinet qui réalise 1 M€ de commissions en s'appuyant sur huit collaborateurs avec 1 500 clients.
Ce courtier subit une cyberattaque lui causant une interruption d'activités de 5 jours et nécessitant le recours à un prestataire externe pour résoudre l'incident (1 ETP). Les coûts générés par l'incident peuvent s'élever entre 50 000€ et 55 000€ soit environ 6 % de ses commissions. Cette estimation de coûts se décomposerait de la manière suivante :

TYPOLOGIES DE COÛTS	IMPORTANCE DES COÛTS[30]	ILLUSTRATION DE L'IMPACT
Réponse à l'incident et à la récupération	€	**5 000 €** 1 000 € x 5 jours x 1 ETP
Perte de revenus durant l'interruption d'activité	€€	**23 000 €** 1 M € x (5 jours/220)
Frais de notification aux clients	€€	**18 000 €** 12 € de traitement du LRAR x 1 500 clients
Frais de gestion administrative de l'incident et relation client	€	**5 000 €** 1 000 € x 5 jours x 1 ETP
Enquête et audits	€	**Entre 5 000 € et 8 000 €** Fourchette de prix d'un audit de sécurité
Amendes réglementaires	€€€ (Coûts indirects)	Amende non-conformité à la RGPD
Atteinte à la réputation et à la confiance des clients et prospects	€€ (Coûts indirects)	Perte potentielle de clients et prospects
Atteinte à la réputation et à la confiance des assureurs	€€€ (Coûts indirects)	Perte de la délégation d'encaissement
Augmentation des primes d'assurance cyber	€ (Coûts indirects)	**2 000 €** 1 000 € de primes avant augmentation + 200 %[31]
Exemple de coût total	**Entre 55 000 € et 60 000 €**	

[28] Par rapport aux commissions
[29] Deloitte (2022), « Beneath the surface of a cyberattack: A deeper look at business impacts »

tous ciblés, *tous vulnérables !*

Cas du cabinet Devorsine 1
Laurent Devorsine

« Notre cabinet travaille sur plusieurs pôles et notamment un, celui de l'immobilier, qui génère de nombreux échanges, souvent en urgence, avec les syndicats d'immeuble. Aussi, malgré un niveau d'information important sur les risques cyber des équipes du cabinet, une assistante a ouvert un lien dans un mail nous demandant un devis, et provoquant immédiatement l'ouverture d'un pop-up semblable à Outlook, l'invitant à rentrer ses codes d'accès.

Dans le même temps, un administrateur système a été victime de la même tentative. Nous avons contacté notre client qui nous indiquait s'être fait pirater. Notre prestataire est intervenu immédiatement, et tout a pu être réglé en 20 minutes. Cet exemple démontre que malgré une certaine maturité sur ces sujets, la qualité des mails pirates atteint un tel niveau, que la prévention de suffit plus, mais qu'il est nécessaire de disposer d'une protection renforcée.

Même quelqu'un de très informé peut se faire piéger. Ce qui nous a notamment sauvé, c'est la double authentification nécessaire à l'accès de nos systèmes. Si cela nous était arrivé il y a ne serait-ce que 2 ans, cela aurait pu être dramatique.[32] »

Extrait du 5e Livre Blanc de PLANETE CSCA/ INTERMEDIUS

Cas d'AssurOne
Paul-Henri Chabrol, DSI d'AssurOne

2

« AssurOne est un courtier grossiste employant 400 salariés et ayant un modèle de distribution multicanal[33]. En tant que société financière, nous sommes particulièrement exposés au risque cyber, qui devient de plus en plus protéiforme. Nous nous faisons attaquer tous les jours par des attaques toujours plus sophistiquées et insidieuses dont l'élément déclencheur est souvent humain. Comme nous avons une grande variété d'utilisateurs de nos solutions (courtiers, partenaires, utilisateurs internes), l'origine des attaques est vaste.

Nous avons connu une cyberattaque fin 2022. Celle-ci n'a pas induit d'incidents opérationnels mais a créé une prise de conscience encore plus forte d'AssurOne et de ses actionnaires sur le besoin d'investir massivement dans la gestion de la sécurité de l'information, car le risque cyber doit être suivi avec le même niveau d'attention que tous les autres risques d'entreprise. Nous avons donc investi dans des technologies, de l'expertise en interne et mis en place des processus pour mieux nous protéger et devenir plus résilients quand une attaque intervient.

Plus concrètement, nous avons mené un plan de transformation sécurité. D'une part, nous avons sensibilisé toutes nos parties prenantes à ce risque et pas uniquement nos salariés. D'autre part, nous avons mis en place un arsenal de solutions au cœur de notre SI pour détecter des incidents potentiels (Endpoint Detection and Response [EDR], Security operations center [SOC], Security Information and management [SIEM], outils IA d'analyse de menaces…) et mis en place un système de management de la Sécurité de l'Information (SMSI) qui crée un cadre robuste de gouvernance pour ancrer ces pratiques dans nos opérations. »

[32] Témoignage du 21 juin 2023

[33] Vente directe auprès de comparateurs, réseau de courtage et délégation de gestion et de souscription pour des constructeurs automobiles

Cas du groupe ASQUA
Xavier Thamin, Directeur du Développement du Groupe ASQUA

3

« En février 2021, nous avons été victime d'une cyber-attaque ciblant nos systèmes. À la fin du mois le service administratif a reçu une facture semblant être une facture Orange en bonne et due forme mais c'était une fausse... L'ouverture de ce faux mail a conduit à la compromission temporaire de notre réseau informatique.

À la suite de cette tentative de fraude, nous avons dû immédiatement bloquer l'accès à tous nos ordinateurs pendant 24 heures afin d'évaluer l'ampleur des dommages potentiels. Heureusement, grâce aux leçons tirées d'une précédente cyber-attaque en 2018, nous disposions de mesures de protection renforcées. L'impact de cette attaque a été limité, principalement en raison de la mise en place d'un véritable système de sauvegarde (backup), qui nous a permis de redémarrer rapidement nos activités sans perte significative de données.

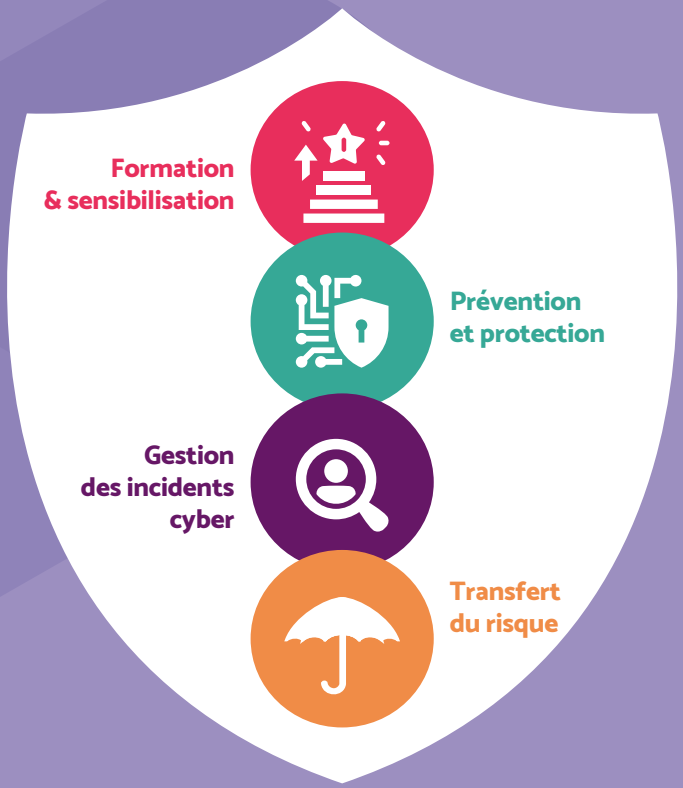
Pendant l'attaque, la priorité a été de bloquer l'accès aux systèmes pour limiter la propagation de la menace. Les équipes informatiques ont travaillé intensément pour analyser l'origine et l'ampleur de l'intrusion. Post-attaque, nous avons immédiatement renforcé nos dispositifs de sécurité en introduisant des mesures supplémentaires, notamment :

- La double authentification pour tous les accès aux systèmes critiques,
- Une sensibilisation renforcée et continue des collaborateurs aux risques cyber, incluant des formations spécifiques sur la détection des tentatives de phishing et autres formes d'attaques.

Depuis cet incident, le Groupe ASQUA a renforcé sa stratégie de cybersécurité en intégrant des solutions plus robustes et en effectuant des mises à jour régulières des protocoles de sécurité. Des tests de vulnérabilité sont également menés régulièrement pour s'assurer que nos systèmes restent résilients face aux nouvelles menaces. L'engagement envers la formation des collaborateurs a été également renforcé, avec des sessions régulières pour les sensibiliser aux bonnes pratiques de sécurité informatique. »

LES 4 PILIERS *de la cyber-résilience*

Pour atteindre vos objectifs de cyber-résilience, nous avons identifié quatre piliers : la formation et la sensibilisation des collaborateurs, la prévention et la protection face aux risques cyber, la gestion des incidents et le transfert du risque. Ces quatre piliers couvrent l'essentiel des meilleures pratiques en matière de cyber-résilience. En les adoptant, vous pouvez atteindre les standards les plus élevés de résilience opérationnelle et protéger vos actifs et vos clients face aux cybermenaces.



PILIER 1

La sensibilisation et la formation des collaborateurs à la cyber-résilience visent à informer et entraîner les employés sur les bonnes pratiques de sécurité informatique et de gestion des cyber-attaques. Faire prendre conscience qu'ils sont quotidiennement exposés à ces risques et qu'ils doivent adopter quelques réflexes simples pour élever collectivement le niveau de protection de l'entreprise.

- Programmes de sensibilisation et de formation
- Politique de sécurité claire, connue de tous et mise à jour régulièrement
- Simulations de phishing (mises en situation concrète)

PILIER 2

La prévention et la protection des risques cyber englobent l'ensemble des mesures et stratégies mises en place pour anticiper, détecter et contrer les cybermenaces.

- Évaluation des risques
- Contrôles d'accès
- Sécurisation des systèmes
- Sécurisation des données
- Sauvegarde et restauration
- Mise à jour et gestion des correctifs

PILIER 3

La gestion des incidents cyber consiste à identifier, analyser, contenir et remédier aux cyberattaques pour minimiser les impacts sur les données, les opérations, les finances ou encore sur la réputation.

- Détection des incidents
- Plan d'intervention et de réponse aux incidents / Plan de Continuité des Activités et Plan de Reprise des activités
- Équipe de réponses aux incidents (IRT)
- Mise à jour et gestion des correctifs

PILIER 4

Le transfert du risque cyber via des solutions assurantielles consiste à utiliser des polices spécifiques pour couvrir les coûts engendrés par les cyberattaques et incidents de sécurité. Il existe différentes natures de garanties et les assureurs ont des attentes vis-à-vis des entreprises couvertes.

LES 3 NIVEAUX *de cyber-résilience à franchir*

Le transfert du risque cyber via des solutions assurantielles consiste à utiliser des polices spécifiques pour couvrir les coûts engendrés par les cyberattaques et incidents de sécurité. Il existe différentes natures de garanties et les assureurs ont des attentes vis-à-vis des entreprises couvertes.

LES MESURES DU PANORAMA SONT CLASSÉES EN FONCTION DE VOS AMBITIONS DE CYBER-RÉSILIENCE :

Risque identifié

CEINTURE JAUNE

Les 9 mesures fondamentales à adopter immédiatement pour une première ligne de défense à court terme ;

Risque maîtrisé

CEINTURE BLEUE

les 5 mesures complémentaires, essentielles pour atteindre un niveau de résilience maîtrisé ;

Risque limité

CEINTURE NOIRE

les 5 mesures avancées pour vous permettre d'atteindre un haut niveau de résilience.

QUELLE CEINTURE VISER POUR VOTRE ACTIVITÉ ?

La ceinture jaune est indispensable !
Nous recommandons une mise en place rapide de ces mesures simples et peu coûteuses, qui peuvent protéger votre activité du pire.

Cependant, **bien que nécessaire, elle ne suffit pas à elle seule** : seule la ceinture bleue vous permettra d'atteindre un niveau de cyber-résilience adapté aux risques actuels. Enfin, en atteignant le niveau de la « ceinture noire », vous pourrez considérer avoir réduit de manière optimale le risque cyber.

COMMENT FONCTIONNE CE SYSTÈME ?

Les ceintures vous fournissent à la fois une liste de mesures à mettre en œuvre pour améliorer vos pratiques actuelles. Elles vous permettent également d'évaluer vos mesures existantes, d'identifier les lacunes et les points d'amélioration.

ceinture jaune, *les pratiques essentielles*

LA CEINTURE JAUNE, REPRÉSENTATIVE D'UN NIVEAU MINIMAL DE CYBERSÉCURITÉ, EST OBTENUE APRÈS LA RÉALISATION DES 9 MESURES INDISPENSABLES.

Risque identifié

Chacune des mesures est affiliée aux piliers suivants :

Formation et sensibilisation

Prévention et protection

Gestion des incidents cyber

Pour obtenir la ceinture jaune, il est crucial de valider ces mesures fondamentales :

MESURE #1 - Sélectionner un prestataire pour gérer au quotidien les SI

MESURE #2 – Sensibiliser & former les collaborateurs à la cybersécurité

MESURE #3 - Mettre en place une politique de sécurité informatique claire et diffusable

MESURE #4 - Utiliser des antivirus & firewall

MESURE #5 - Maintenir les équipements et logiciels à jour

MESURE #6 - Adopter des pratiques de mot de passe rigoureuses

MESURE #7 - Faire des sauvegardes régulières des données de l'entreprise et tester les sauvegardes

MESURE #8 - Utiliser des VPN[1] et/ou RDP[2]

MESURE #9 - Contrôler les accès et les privilèges

[1] VPN (Virtual Private Network) est un service qui permet de créer une connexion sécurisée et cryptée entre l'appareil et le serveur distant

[2] RDP (Remote Desktop Protocol) est un protocole développé par Microsoft qui permet de se connecter et de contrôler à distance un autre ordinateur via une interface graphique, facilitant ainsi le travail à distance

MESURE #1
GESTION DES INCIDENTS CYBER

Temps ●○○
Coût ●○○
Impact ●●○

Sélectionner un prestataire
pour gérer au quotidien les SI

Quel enjeu pour moi, courtier ?

Assurer la gestion des SI par des professionnels expérimentés pour :

- Gérer les risques de manière proactive
- Garantir une réponse rapide et efficace en cas d'incident
- Se concentrer sur ses activités principales
- Optimiser les coûts de gestion des SI

Que faire ?

En nous basant sur l'ANSSI, la CNIL et le site de Cybermalveillance.gouv.fr, nous préconisons de :

1. **Identifier les besoins récurrents en gestion des SI (maintenance, support, sécurité, développement, etc.)**
2. **Rechercher et identifier les prestataires potentiels**
3. **Réaliser une évaluation préliminaire des prestataires sur la base des critères de sélection** *(cf. partie droite de la fiche)*
4. **Sélectionner le prestataire le mieux adapté**
5. **Négocier le contrat**
   - Établir les niveaux de service attendus
   - Établir les responsabilités en matière de sécurité
   - Établir les modalités de réponse en cas d'incident
6. **Mettre en place le service**
7. **Intégrer le prestataire dans les opérations quotidiennes**

Quels critères de sélection ?

Sélectionner des prestataires informatiques fiables et compétents est un enjeu crucial pour renforcer sa cyber-résilience. Pour assurer la sélection des prestataires, la due diligence est basée sur certains critères dont :

- Modules de formation interactifs
- Réputation et expérience
- Conformité règlementaire et certifications
- Compétences techniques
- Infrastructure et fiabilité
- Capacité de gestion des incidents
- Transparence et communication
- Régularité des audits et évaluations
- Évolutivité et flexibilité

Quel budget de mise en œuvre ?

Prix moyen (par mois et par collaborateur) :

25 € en moyenne par mois et par collaborateur
soit environ 300 € par an par collaborateur

20 € — 30 €

pour les fonctionnalités essentielles — pour les options supplémentaires

MESURE #2
FORMATION ET SENSIBILISATION

Temps ●●○
Coût ●○○
Impact ●●●

PRÉREQUIS ASSURANCE CYBER

Sensibiliser & former
les collaborateurs à la cybersécurité !

Quel enjeu pour moi, courtier ?

Les actions humaines sont au cœur des enjeux de cyber-résilience. Selon le Global Risk Report, 95 % des problèmes de cybersécurité y seraient attribuables. Sensibiliser et former les collaborateurs dans le but de :

- Constituer une première ligne de défense pour :
  - Réduire les risques d'erreur
  - Assurer une continuité opérationnelle avec les collaborateurs aptes à identifier et à réagir efficacement

Que faire ?

En nous basant sur l'ANSSI et la CNIL, nous préconisons de :

1. Établir un programme de formation

- Créer des modules de formation adaptés ou sélectionner un organisme de formation
- Définir un calendrier de formations régulières

2. Réaliser les formations sous les formats les plus adaptés

- Organiser des sessions en présentiel et en ligne
- S'assurer que les sessions sont interactives

3. Diffuser les bonnes pratiques

- Développer des politiques de sécurité claires et accessibles à tous les employés
- Concevoir des fiches pratiques et des guides

Quel budget de mise en œuvre ?

Prix moyen (par mois et par collaborateur) :

3 € en moyenne par mois et par collaborateur
soit environ 35 € par an par collaborateur

2 €	4 €
pour les fonctionnalités essentielles	pour les options supplémentaires

Quelles solutions technologiques utilisées par le courtage ?

Gophish · HOOK SECURITY · PHISHED · sosafe · TitanHQ SafeTitan · phishingbox · Cyber Guru · HOXHUNT · caniphish

Votre entreprise connait-elle vraiment les dernières menaces en cybersécurité et les bonnes pratiques pour les contrer ?

La formation continue est essentielle, mais elle peut être difficile à maintenir. Les plateformes de formation en cybersécurité offrent des modules interactifs, des simulations d'attaques réelles et des mises à jour régulières. Elles permettent de garder vos collaborateurs informés et vigilants, renforçant ainsi votre première ligne de défense contre les cybermenaces. Transformez chaque membre de votre équipe en un acteur clé de votre résilience cyber !

Principales fonctionnalités :

- Modules de formation interactifs
- Exercices de mise en pratique
- Personnalisation des parcours
- Options supplémentaires : simulations de phishing, suivi des progrès, etc.

Les solutions de sensibilisation et de formation intègrent des fonctionnalités premium de contrôle de connaissances. Il s'agit donc des mêmes solutions.

La plateforme en ligne de formation continue PLANETE CSCA RH propose une dizaine de modules sur la sécurité informatique ▸

PLANETE CSCA propose également une formation Prévention cybersécurité de PLANETE CSCA RH avec Eurocybergroup (5h) ainsi que d'autres formations organisées tout au long de l'année.

MESURE #3

FORMATION ET SENSIBILISATION

Temps ●○○
Coût ○○○
Impact ●●●

PRÉREQUIS ASSURANCE CYBER

Mettre en place une politique de sécurité *informatique claire et diffusable*

Quel enjeu pour moi, courtier ?

I Uniformiser les pratiques de sécurité pour :

- Réduire le risque d'erreurs humaines et d'incidents de sécurité
- Éduquer et sensibiliser les employés aux bonnes pratiques de sécurité
- Définir les principes à appliquer
- Améliorer la rapidité et l'efficacité de la réponse aux incidents de sécurité

Que faire ?

En nous basant sur l'ANSSI et le site de Cybermalveillance.gouv.fr, nous préconisons de :

1. **Désigner un responsable de la politique qui sera chargé d'en définir le contenu et de le rédiger**
2. **Identifier les rôles et responsabilités des acteurs impliqués**
3. **Définir les objectifs de sécurité internes et les besoins opérationnels de l'entreprise**
4. **Déterminer le périmètre et le domaine d'application**
5. **Définir les règles et les référentiels de sécurité à respecter**
6. **Déterminer les moyens nécessaires (matériels et humains)**
7. **Assurer un suivi et une mise à jour et révision régulières de la politique**
   - I Au moins annuellement
   - I Lors d'un changement important

Quel document ou politique ?

Une politique de sécurité informatique est un ensemble de directives et de procédures établies par votre organisation pour protéger vos systèmes informatiques, vos réseaux et vos données contre les menaces et les cyberattaques.

Elle définit les responsabilités des collaborateurs, les mesures de protection des informations, les protocoles de gestion des accès et des identités, ainsi que les procédures à suivre en cas d'incident de sécurité.

Plan :

A I Objectifs de la politique

B I Les périmètres d'application

C I Le cadre réglementaire

D I Comitologie

E I La déclinaison opérationnelle (processus, outils)

F I Communication de la politique

G I Révision

Cliquez pour accéder au modèle de politique de sécurité de PLANETE CSCA !

Pour un diagnostic de cybersécurité gratuit conçu pour les TPE/PME par l'ANSSI, cliquez ici !

TECH RADAR DU COURTAGE - Cyber-résilience
Édition 2024

EÜRUS Consulting
24 Rue de Londres, 75009 Paris

www.eurus-consulting.com/fr
erwan.lomenech@eurus-consulting.com / +33 (0)7 64 01 79 81

PLANETE CSCA
10 Rue Auber, 75009 Paris

www.planetecsca.fr
01 48 74 19 12

À DÉCOUVRIR ÉGALEMENT :
LE PANORAMA DES SOLUTIONS MÉTIERS
dédiées aux courtiers

En 2023, le LAB' PLANEÈTE CSCA et EÜRUS ont réalisé un Tech Radar des solutions métiers dédiées aux courtiers de proximité. Celui-ci présente de nombreux outils qui vous permettront d'accélérer la digitalisation de votre activité et de gagner en efficacité, actionnables sur les différentes étapes de la chaîne de valeur.

Pour consulter ce panorama, scannez ce QR code !

EURUS

expert des métiers de l'assurance

Stratégie
Transformation
Risques & Résilience
Technologies

www.eurus-consulting.com