Culture de la cybersécurité dans l’aviation civile

Publié sous l’autorité du Secrétaire général

Janvier 2022

Organisation de l’aviation civile internationale

1. Introduction

1.1 Les présentes orientations cadrent avec la Stratégie[1] pour la cybersécurité de l'aviation de l'OACI et le Plan d'action[2] pour la cybersécurité, dont la mesure CyAP7.1 recommande de définir et de promouvoir la culture de la cybersécurité dans l'aviation civile.

2. Portée

2.1 Les présentes orientations visent à aider les États membres et les parties prenantes à concevoir et à mettre en œuvre une solide culture de la cybersécurité dans leurs organisations. L'objectif ultime est d'appuyer la sûreté et la résilience de l'aviation civile face aux cybermenaces et cyberrisques.

3. Définition, objectifs généraux et avantages de la culture de la cybersécurité

3.1 Aux fins des présentes orientations, la culture de la cybersécurité est généralement considérée comme un ensemble d'idées, d'attitudes, de croyances, de comportements, de normes, de perceptions et de valeurs qui sont inhérents au fonctionnement quotidien d'une organisation et qui transparaissent dans les actions et les comportements de toutes les composantes et de tout le personnel lors de leurs interactions avec les actifs numériques.

3.2 Une culture positive de la cybersécurité vise à intégrer les considérations de cybersécurité dans les habitudes, les comportements et les processus de l'organisation, en les ancrant dans les opérations quotidiennes, comme en témoignent les actions et les comportements de l'ensemble du personnel.

3.3 L'instauration d'une culture solide et efficace de la cybersécurité, en tant que partie intégrante d'une culture organisationnelle, aide les organisations à améliorer leur performance globale grâce à la détection précoce des cyberrisques potentiels.

3.4 La culture de la cybersécurité dans l'aviation civile s'appuie sur l'expérience acquise, les efforts consentis et les succès remportés par le secteur dans la mise en œuvre de cultures solides de sécurité et de sûreté de l'aviation, et partage avec ces cultures un grand nombre d'éléments fondamentaux. De par son caractère transversal, la culture de la cybersécurité conduit non seulement à une amélioration de l'état de la cybersécurité, mais aussi à des retombées positives dans les trois domaines en favorisant la promotion et le renforcement de cultures positives de la sécurité, de la sûreté et de la cybersécurité.

3.5 En résumé, la culture de la cybersécurité permet à chaque membre de l'organisation, peu importe son rôle, d'améliorer sa performance dans l'environnement numérique. Parmi les exemples d'avantages procurés par la conception et la mise en œuvre d'une culture de la cybersécurité efficace et solide, on peut citer les suivants :

a) accroissement du niveau de maturité en cybersécurité de l'organisation ;

b) traitement approprié des informations par l'ensemble du personnel ;

c) amélioration de l'état de la cybersécurité qui favorise l'efficacité et l'efficience de l'organisation en matière d'atténuation des cyberrisques ;

d) amélioration de la sensibilisation de tous les membres du personnel aux cyberrisques et au rôle que joue chacun dans la détection et l'atténuation de ces risques ;

---

[1] https://www.icao.int/cybersecurity/Pages/Cybersecurity-Strategy.aspx
[2] Lettre 2020/114 de l'OACI.

e) disposition à signaler les oublis personnels dans l'application des processus et procédures de cybersécurité de l'organisation ainsi que les cyberactivités suspectes, d'où une proactivité et une meilleure détection des cyberrisques.

3.6 Les sections ci-après des présentes orientations décrivent les éléments fondamentaux d'une culture organisationnelle efficace de la cybersécurité aérienne. Toutefois, bien que ces éléments fondamentaux soient bien définis, la culture de la cybersécurité devrait être conçue de manière unique dans chaque organisation. Elle devrait prendre en compte différents aspects, notamment le niveau de maturité de la cybersécurité, les cultures et valeurs actuelles, et le paysage global des menaces pour la cybersécurité dans l'organisation.

3.7 Les éléments fondamentaux d'une culture solide et efficace de la cybersécurité dans l'aviation civile sont les suivants :

a) rôle moteur ;
b) liens transversaux ;
c) communication ;
d) sensibilisation, formation et éducation ;
e) systèmes de rapports ;
f) examen et amélioration continus ;
g) environnement de travail positif.

4. Rôle moteur

4.1 Une culture de cybersécurité efficace dépend de l'engagement de chaque membre de l'organisation, à commencer par les cadres supérieurs. Ces derniers devraient s'engager pleinement en faveur de la culture de la cybersécurité, en tout temps et pour l'ensemble des activités, stratégies, politiques et objectifs de l'organisation.

4.2 Les membres de la haute direction devraient se conformer aux politiques de cybersécurité, montrer l'exemple et devenir des modèles pour les cadres et le personnel de l'organisation. Ils devraient aussi défendre la cybersécurité en tant que valeur organisationnelle et personnelle, tout en s'efforçant de la même manière d'aligner leurs comportements sur cette valeur.

4.3 À cet égard, les cadres supérieurs devraient :

a) s'efforcer d'améliorer leurs connaissances en matière de cybersécurité dans l'aviation civile ;

b) se conformer en permanence aux règles, aux processus et aux procédures de cybersécurité et montrer l'exemple ;

c) inscrire clairement la cybersécurité parmi les priorités de l'organisation ;

d) inscrire la cybersécurité aérienne dans les politiques écrites de l'organisation pour qu'elle fasse partie intégrante du plan de gestion de l'entreprise ;

e) fournir un soutien visible à la mise en œuvre de la culture de la cybersécurité ;

f) assurer et appuyer la formation à la cybersécurité et le renforcement des capacités de l'ensemble du personnel ;

g) assurer le traitement des rapports de cybersécurité en temps utile et veiller à la mise en œuvre rapide de toute action corrective et préventive requise ;

h) intervenir de manière appropriée chaque fois que la cybersécurité est compromise ;

i) suivre l'évolution de l'état de la cybersécurité de l'organisation, de la culture de la cybersécurité et des mesures et ressources destinées à appuyer l'amélioration continue de l'adoption de la culture de la cybersécurité à l'échelle de l'organisation.

4.4 Sous l'impulsion de la haute direction, les échelons hiérarchiques de l'organisation devraient également s'efforcer d'adopter les mesures prévues au § 4.3, en fonction de leurs responsabilités et de leur champ d'action, afin de généraliser l'engagement en faveur d'une culture de la cybersécurité dans toute l'organisation.

5. **Liens transversaux**

5.1. Compte tenu du grand nombre de cyberrisques et de vulnérabilités dans chaque organisation, il conviendrait d'établir officiellement des liens transversaux.

5.2. Une équipe spéciale multidisciplinaire relevant de la haute direction pourrait être créée en vue d'appuyer la coordination de la culture de la cybersécurité à l'échelle de l'organisation.

5.3. Les objectifs de l'équipe spéciale seraient notamment les suivants :

a) évaluer périodiquement le niveau de maturité de la culture de la cybersécurité dans l'organisation ;

b) détecter les risques et les opportunités en ce qui concerne la mise en œuvre de la culture de la cybersécurité ;

c) rapprocher les points de vue des différentes parties prenantes internes relativement à la culture de la cybersécurité ;

d) appuyer l'élaboration et la mise en œuvre d'activités transversales liées à la promotion d'une culture de la cybersécurité dans l'organisation.

6. **Communication**

6.1. La communication contribue de manière essentielle, sur le plan tant interne qu'externe, à garantir la mise en œuvre d'une culture de cybersécurité réussie. Elle constitue le principal moyen par lequel le niveau de sensibilisation attendu peut être atteint.

6.2. Pour que la communication soit efficace, certaines compétences devraient être considérées comme faisant partie d'une solide culture de la cybersécurité :

a) *écoute active* — processus par lequel les signaux verbaux et non verbaux sont observés, afin de reconnaître les valeurs et les besoins de l'autre personne, et de contribuer à l'amélioration de la communication au sein de l'équipe ;

b) *adaptation du style de communication à différents publics et situations* — comprendre comment les autres communiquent et personnaliser le message en vue de mieux les atteindre ;

c) *clarté de la communication* — déterminer ce qu'il faut communiquer et comment le faire.

6.3. La haute direction devrait veiller à ce que les politiques et directives internes en matière de cybersécurité, ainsi que la raison de leur introduction, soient dûment communiquées à l'ensemble du personnel. Un programme de communication interne solide contribue à l'acceptation et à la compréhension des mesures de cybersécurité par l'ensemble du personnel, et aide à promouvoir une culture de la cybersécurité dans l'organisation.

6.4. De plus, les programmes de communication interne contribueraient grandement à :

a) faire en sorte que l'ensemble du personnel soit pleinement conscient de ses devoirs, de ses droits et des mécanismes de rapports en place dans l'organisation ;

b) promouvoir le code de conduite numérique de l'organisation, qui comprend les processus, mesures et contrôles que le personnel doit respecter à tout moment.

7. Sensibilisation, formation et éducation

7.1 La sensibilisation, la formation et l'éducation sont des domaines clés du processus d'apprentissage qu'il conviendrait de mettre à profit pour instaurer une solide culture de la cybersécurité. La sensibilisation apporte des connaissances, la formation enseigne des compétences, et l'éducation fait acquérir des connaissances et des compétences dans un cadre théorique et, partant, intègre la sensibilisation et la formation.

7.2 Il conviendrait de faire suivre à tous les membres du personnel de l'aviation civile qui interagissent avec les actifs numériques de l'organisation, peu importe leur rôle ou leurs fonctions, un programme de sensibilisation, de formation et d'éducation à la cybersécurité, afin de s'assurer qu'ils possèdent les connaissances et les compétences nécessaires sur les risques, les mesures et les objectifs en matière de cybersécurité de l'aviation. Ces programmes devraient être adaptés au public, si nécessaire et possible.

7.3 Il conviendrait de dispenser des programmes de sensibilisation à la cybersécurité à tous les membres du personnel lors de leur embauche, ainsi qu'une formation périodique. Les intervalles de temps pour la périodicité du programme de sensibilisation doivent être déterminés en fonction du niveau de maturité de la culture de la cybersécurité dans l'organisation, et peuvent être revus en fonction de l'évolution de ce niveau de maturité.

7.4 Il est recommandé que les programmes de sensibilisation à la cybersécurité soient dispensés au moins une fois en présentiel (dans une salle de classe physique ou virtuelle). La cybersécurité n'est pas un sujet familier à l'ensemble du personnel et s'avère parfois difficile à comprendre sans les orientations d'un professionnel. L'interaction avec un professionnel dans une salle de classe facilite donc la compréhension des sujets de cybersécurité. Elle permet au formateur d'expliquer les concepts, les processus, les procédures et les contrôles d'une manière simplifiée afin qu'ils soient compris par le personnel ne possédant pas de connaissances techniques, ainsi que d'expliquer les avantages de l'amélioration de l'état de la cybersécurité de l'organisation et son effet positif sur la productivité globale du personnel.

7.5 Après une première séance de sensibilisation/formation en personne, les organisations peuvent envisager de recourir à des méthodes d'apprentissage en ligne (apprentissage géré par ordinateur) pour les formations périodiques. Cette décision devrait tenir compte de la progression de la culture de la cybersécurité dans l'organisation, ainsi que des changements apportés aux processus, contrôles et procédures de cybersécurité introduits dans l'organisation en réponse à l'évolution du paysage des risques de cybersécurité.

7.6 Les programmes de sensibilisation à la cybersécurité devraient être dispensés par des professionnels possédant les connaissances techniques requises. Toutefois, le manque de compétences non techniques des présentateurs constitue l'un des défis auxquels sont confrontés les programmes de sensibilisation technique, dans la mesure où des compétences adéquates en matière de communication et de « vente » contribuent grandement à susciter l'intérêt du personnel et à garantir son adhésion et son appui à la culture de la cybersécurité. En conséquence, les organisations devraient veiller à ce que les responsables des programmes de sensibilisation disposent à la fois des connaissances techniques et des compétences générales nécessaires pour susciter chez le personnel des changements de comportement en faveur de l'adoption d'une culture de la cybersécurité.

7.7 Un programme type de sensibilisation à la cybersécurité devrait comprendre notamment les sujets ci-après :

a) l'objectif du programme de sensibilisation ;

b) les mécanismes de communication en place dans l'organisation ;

c) les contrôles, processus et procédures de l'organisation en matière de cybersécurité ;

d) le rôle de l'élément humain dans la protection de l'organisation contre les cyberrisques ;

e) l'importance pour les membres du personnel de se rappeler mutuellement les principes de cybersécurité de l'organisation lorsque l'un d'eux observe des actions non conformes de la part de ses collègues ;

f) une vue d'ensemble des différentes méthodes d'exploitation pouvant cibler les personnes et leurs conséquences (y compris des exemples) ;

g) la façon de détecter les cyberactivités suspectes ;

h) l'impact de la complaisance sur l'organisation (y compris des exemples) ;

i) les principes de la cyberhygiène ;

j) le traitement approprié des données et informations sensibles ;

k) les mécanismes de rapports, la manière de les utiliser et les mécanismes de suivi.

7.8 Les campagnes de sensibilisation à la cybersécurité devraient aussi être utilisées périodiquement, à titre de rappel, pour renforcer les connaissances et les compétences du personnel. Divers outils sont disponibles à cette fin, notamment :

a) des *outils sur papier* — affiches, brochures, livrets, etc. Ce type de support peut être facilement distribué et assimilé. Cependant, il s'agit d'outils passifs qui nécessitent une mise à jour fréquente (et une nouvelle impression à chaque mise à jour) ;

b) des *outils en ligne* — courriels, bulletins d'information, messages sur les économiseurs d'écran, intranet, courtes vidéos, pages FAQ, apprentissage en ligne (apprentissage géré par ordinateur), etc. Le principal avantage de ces outils par rapport aux outils sur papier est leur capacité à atteindre l'ensemble de l'organisation. Ils sont relativement faciles à mettre à jour en termes de ressources et ont un faible coût de production.

8. Systèmes de rapport

8.1 L'une des pierres angulaires de la culture de la cybersécurité est l'élaboration et la mise en œuvre d'un système interne de rapports de cybersécurité. Ce système permet à l'organisation de gérer de manière proactive ses cyberrisques, de mesurer l'évolution de l'état de sa cybersécurité, de déterminer et

de planifier les besoins de sensibilisation et de formation du personnel, et d'adapter ses processus, contrôles et mesures internes en fonction de l'évolution des tendances en matière de cybersécurité et du niveau de maturité de la culture de la cybersécurité.

8.2 Les systèmes de rapports de cybersécurité rassemblent des éléments provenant tant du système de comptes rendus de sécurité de l'aviation que de celui de sûreté de l'aviation. À ce titre, ils couvrent deux domaines, dont le premier est le signalement des actions/erreurs personnelles qui ne sont pas conformes aux politiques et processus de sécurité de l'information de l'organisation, et le deuxième est le signalement des comportements suspects/erronés d'autres employés.

8.3 Lors de l'élaboration de leur mécanisme de rapports de cybersécurité, les organisations sont encouragées à tirer parti de l'expérience acquise dans le cadre de l'élaboration et de la mise en œuvre de systèmes de comptes rendus de sécurité et de sûreté de l'aviation.

8.4 Les éléments ci-après devraient être pris en compte lors de la mise en œuvre d'un système de rapports de cybersécurité :

a) la confidentialité des informations personnelles, en vertu de laquelle les données personnelles ne sont ni collectées ni stockées ; lorsque des données personnelles sont collectées, elles ne doivent servir qu'à obtenir des éclaircissements ou de plus amples informations sur l'incident signalé ou à fournir un retour d'information à l'auteur du signalement ;

b) afin de garantir la confidentialité des informations personnelles, il convient d'élaborer une politique qui définit clairement et rend comptables de leurs actes les personnes chargées de gérer, de maintenir et de garantir la confidentialité, ainsi que d'analyser et de suivre les informations recueillies ;

c) la fourniture d'une formation adéquate à l'ensemble du personnel sur la façon d'utiliser le système de rapports ;

d) la mise en œuvre d'une culture juste dans le système de rapports de cybersécurité, et la sensibilisation adéquate de tous les membres du personnel à la façon dont fonctionne une culture juste, afin qu'ils soient plus à l'aise pour fournir des informations ;

e) la mise en œuvre, le cas échéant, d'un programme d'incitation visant à encourager le membre du personnel à signaler ses propres erreurs et les cybercomportements suspects qu'il observe.

Une culture juste

8.5 Les organisations devraient encourager leur personnel à signaler les incidents de cybersécurité, grâce à l'adoption d'une culture juste. La culture juste est un concept mis en œuvre dans le cadre des comptes rendus de sécurité qui pourrait être d'une grande utilité pour promouvoir une culture de la cybersécurité.

8.6 Dans un contexte de rapports de cybersécurité, une culture juste encourage tout le personnel à notifier les incidents et les erreurs de cybersécurité. Il s'agit d'un environnement où chacun comprend qu'il sera traité équitablement en fonction de ses actions plutôt que du résultat de celles-ci. Dans un environnement de culture juste, tout le personnel est conscient qu'il n'est pas juste de sanctionner toutes les erreurs, peu importe les circonstances, mais il comprend aussi qu'il est inacceptable d'accorder une immunité générale de sanction, car certaines actions peuvent être motivées par une intention malveillante ou résulter d'une pure négligence et/ou nonchalance. D'où l'importance de distinguer clairement les actions acceptables de celles qui sont inacceptables lors de la conception d'une culture juste.

8.7 Une culture juste définit non seulement les responsabilités des membres du personnel envers leur organisation, mais aussi celles des cadres envers le personnel. Ces responsabilités devraient être incluses dans une politique dans laquelle la haute direction de l'organisation devrait :

a) encourager les membres du personnel à pratiquer la cyberhygiène et s'engager à reconnaître les efforts qu'ils déploient pour aider l'organisation à gérer les cyber-risques ;

b) s'engager à fournir à tous les membres du personnel les procédures, une sensibilisation, une formation et une éducation adéquates en matière de cybersécurité pour les aider à accomplir leurs tâches ;

c) assumer la responsabilité si un incident est causé par un défaut de sensibilisation ou un manque de rapidité dans la gestion d'un certain cyberrisque ;

d) encourager le personnel à signaler les cyberincidents, les dangers, les erreurs ou tout comportement suspect dont il est témoin, sans crainte de représailles.

Contrôle de la qualité

8.8 Les organisations devraient mettre en œuvre des programmes de contrôle de la qualité destinés à suivre la mise en œuvre concrète des mesures de cybersécurité. Les programmes de contrôle de la qualité peuvent être un outil efficace pour maintenir la vigilance du personnel et son attachement aux principes de la culture de cybersécurité. La fréquence et la rigueur de la réalisation des contrôles de qualité peuvent avoir une influence positive sur le personnel en démontrant la détermination de la direction à atteindre les objectifs de cybersécurité et à assurer la conformité.

8.9 Des contrôles réguliers de la qualité des mécanismes de signalement en place devraient être effectués dans le cadre des programmes de contrôle de la qualité.

9. Examen et amélioration continus

9.1 Les organisations devraient élaborer un cadre d'indicateurs de performance conçu pour évaluer l'impact des mesures en place sur la culture de la cybersécurité et pour déterminer l'écart existant entre les résultats souhaités et réels en matière de culture.

9.2 Certains éléments de la culture de cybersécurité étant susceptibles de ne pas être observés directement, une série d'indicateurs possibles peuvent être utilisés pour mesurer l'efficacité de la culture de cybersécurité. Parmi ces mesures peuvent figurer :

a) des statistiques sur les incidents signalés (comparées aux données extraites des journaux de l'organisation) qui permettent de mesurer, chez les membres du personnel, la performance en matière de cybersécurité, le niveau de sensibilisation et les progrès accomplis dans la promotion des rapports de cybersécurité ;

b) les résultats des séances de formation périodiques ;

c) les résultats des simulations d'attaques malveillantes servant à tester la réaction du personnel ;

d) des questionnaires et des entretiens.

10. **Environnement de travail positif**

10.1 Un environnement général de travail positif peut aussi influencer grandement l'engagement du personnel envers la culture de la cybersécurité et améliorer la performance en matière de cybersécurité.

10.2 Un environnement de travail positif devrait comprendre, au minimum, les éléments ci-après :

a) la participation du personnel aux processus décisionnels (suggestions d'amélioration des programmes de formation à la sensibilisation à la cybersécurité, p. ex.) ;

b) l'allocation au personnel d'un temps suffisant pour suivre une formation sur la cyber-hygiène appropriée ;

c) un mécanisme de reconnaissance des bonnes performances (c'est-à-dire des incitations et/ou des programmes de récompense) ;

d) la fourniture d'un retour d'information au personnel sur les suggestions et les rapports de cybersécurité ;

e) la fixation d'objectifs clairs, réalisables et mesurables en ce qui concerne les incidents de cybersécurité, et le retour d'information périodique au personnel sur les progrès de l'organisation à cet égard ;

f) la fourniture des procédures, de la sensibilisation, de la formation et des outils nécessaires pour permettre au personnel d'accomplir ses tâches ;

g) l'octroi au personnel du niveau approprié d'autonomie et de responsabilité.

— FIN —