# Chapitre 1 : La nécessité de la cybersécurité

Ce chapitre explique ce qu’est la cybersécurité et pourquoi les professionnels de la cybersécurité sont de plus en plus demandés. Il explique ce que sont votre identité et vos données en ligne, où elles se trouvent et pourquoi elles intéressent les cybercriminels.

Ce chapitre parle également des données d’entreprise et pourquoi il faut les protéger. Il traite des pirates informatiques et de ce qu’ils veulent. Les professionnels de la cybersécurité doivent avoir les mêmes compétences que les agresseurs informatiques. Cependant, ils doivent travailler dans le cadre de la législation locale, nationale et internationale. Les professionnels de la cybersécurité doivent également faire preuve d’éthique.

Ce chapitre propose également un contenu expliquant brièvement la guerre cybernétique et les raisons pour lesquelles les pays et gouvernements ont besoin des professionnels de la cybersécurité pour les aider à protéger leurs citoyens et leurs infrastructures.

# Qu’est-ce que la cybersécurité ?

Le réseau d’informations électronique connecté est devenu une partie intégrante de notre vie quotidienne. Les entreprises en tout genre, comme les instituts médicaux ou les établissements financiers et scolaires, utilisent ce réseau pour leur bon fonctionnement. Elles utilisent le réseau en recueillant, en traitant, en stockant et en partageant d’énormes quantités d’informations numériques. Comme de plus en plus d’informations numériques sont rassemblées et partagées, la protection de ces informations devient encore plus essentielle pour notre sécurité nationale et pour la stabilité économique.

La cybersécurité consiste en l’effort continu pour protéger les systèmes mis en réseau et les données contre l’utilisation ou le méfait non autorisés. À titre personnel, vous devez protéger votre identité, vos données et vos périphériques informatiques. Au niveau de l’entreprise, tout le monde est responsable de la protection de la réputation, des données et des clients de l’entreprise. Au niveau national, la sécurité nationale, ainsi que la sécurité et le bien-être des citoyens sont en jeu.

# Votre identité en ligne et offline

Comme vous passez plus de temps en ligne, votre identité, en ligne et offline, peut affecter votre vie. Votre identité offline est la personne avec qui vos amis et votre famille interagissent au quotidien à la maison, à l’école ou au travail. Ils connaissent vos informations personnelles comme votre nom, votre âge ou votre adresse. Votre identité en ligne représente qui vous êtes dans le cyberespace. Votre identité en ligne traduit votre manière de vous présenter aux autres en ligne. Cette identité en ligne doit uniquement révéler une quantité limitée d’informations vous concernant.

Vous devez faire attention lorsque vous choisissez un nom d’utilisateur ou un pseudonyme pour votre identité en ligne. Le nom d’utilisateur ne doit pas inclure d'informations personnelles. Il doit être adéquat et respectueux. Ce nom d’utilisateur ne doit pas pousser les inconnus à penser que vous êtes une cible facile pour la cybercriminalité ou pour une attention indésirable.

# Vos données

Toute information vous concernant peut être considérée comme faisant partie de vos données. Ces informations personnelles permettent de vous identifier de manière unique comme individu. Ces données comprennent les photos et messages que vous échangez en ligne avec votre famille et vos amis. D'autres informations, dont votre nom, votre numéro de sécurité sociale, votre date et votre lieu de naissance, ou le nom de jeune fille de votre mère sont des informations que vous connaissez et qui sont utilisées pour vous identifier. Les informations comme les données médicales, scolaires, financières et relatives à l’emploi peuvent également être utilisées pour vous identifier en ligne.

**Dossiers médicaux**

À chaque fois que vous vous rendez dans un cabinet médical, d'autres informations sont ajoutées à vos dossiers médicaux électroniques (DME). La prescription par votre médecin traitant devient une partie de votre DME. Votre DME inclut des informations sur votre santé physique, sur votre santé mentale et d'autres informations personnelles qui pourraient ne pas concerner la santé. Par exemple, si vous avez eu une consultation pendant votre enfance lorsque de grands changements se faisaient dans votre famille, cela sera inclus quelque part dans vos dossiers médicaux. Parallèlement à vos antécédents médicaux et à vos informations personnelles, le dossier DME peut également contenir des informations concernant votre famille.

Les dispositifs médicaux, comme les bracelets de remise en forme, utilisent la plate-forme cloud pour activer le transfert, le stockage et l’affichage sans fil de données cliniques telles que la fréquence cardiaque, la pression artérielle et la glycémie. Ces dispositifs peuvent générer une grande quantité de données cliniques qui peuvent s’intégrer à vos dossiers médicaux.

**Dossiers scolaires**

Au fur et à mesure que vous avancez dans vos études, des informations concernant vos diplômes et vos résultats d’examen, votre assiduité, les cours que vous avez suivis, vos récompenses et vos niveaux récompensés, ainsi que tout rapport disciplinaire peuvent être inclus dans votre dossier scolaire. Ce dossier peut également contenir des coordonnées, des dossiers de santé et de vaccination, ainsi que des dossiers scolaires particuliers, dont les programmes d'éducation personnalisés.

**Dossier d’emploi et dossier financier**

Votre dossier financier peut contenir des informations sur votre revenu et sur vos dépenses. Les dossiers fiscaux peuvent comprendre des fiches de paie, des relevés bancaires, votre antécédent de crédit et d’autres informations bancaires. Dans vos informations d’emploi, il y a vos emplois passés et votre performance y afférente.

# Où sont vos données ?

Toutes ces informations vous concernent. Il existe différentes législations qui protègent votre confidentialité et vos données dans votre pays. Mais est-ce que vous savez où sont vos données ?

Lorsque vous êtes dans le cabinet médical, la conversation que vous avez avec le médecin est enregistrée dans votre fiche médicale. À des fins de facturation, ces informations peuvent être partagées avec la compagnie d’assurance qui assure la facturation et la qualité appropriées. Maintenant, une partie de votre dossier médical pour la visite est également chez la compagnie d’assurance.

Les cartes de fidélité d’un magasin peuvent être une bonne manière d’économiser lors de vos achats. Cependant, le magasin établit un profil selon vos achats et utilise ces informations pour sa propre utilisation. Le profil montre une personne qui achète régulièrement un dentifrice d’une certaine marque et d’un certain arôme. Le magasin utilise cette information pour cibler l’acheteur avec des offres spéciales provenant d’un partenaire marketing. En utilisant la carte de fidélité, le magasin et son partenaire marketing ont un profil pour le comportement d’achat d’un client.

Lorsque vous partagez vos photos en ligne avec vos amis, est-ce que vous savez qui peut avoir une copie de vos photos ? Des copies de vos photos sont sur vos propres périphériques. Vos amis peuvent avoir des copies de ces photos téléchargées sur leurs périphériques. Si les photos sont partagées publiquement, des inconnus peuvent avoir leurs copies, également. Ils peuvent les télécharger ou prendre des captures d’écran de ces photos. Puisque les photos ont été publiées en ligne, elles sont également enregistrées sur les serveurs placés dans différentes régions du monde. Désormais, les photos ne sont plus présentes uniquement sur vos périphériques informatiques.

# Vos périphériques informatiques

Vos périphériques informatiques ne servent pas qu’à stocker vos données. Actuellement, ces périphériques sont devenus le portail vers vos données et ils permettent de générer des données vous concernant.

À moins que vous ayez choisi de recevoir des relevés sur papier pour tous vos comptes, vous utilisez vos périphériques informatiques pour accéder à ce genre de données. Si vous voulez recevoir une copie numérique du dernier relevé bancaire, vous utilisez les périphériques informatiques pour accéder au site Web du fournisseur de carte de crédit. Si vous souhaitez payer votre facture de carte de crédit en ligne, vous accédez au site Web de votre banque pour transférer des fonds en utilisant vos périphériques informatiques. En plus de vous permettre d’accéder à vos informations, les périphériques informatiques permettent également de générer des informations vous concernant.

Avec toutes ces informations sur vous disponibles en ligne, vos données personnelles sont devenues lucratives pour les pirates.

# Ils veulent votre argent

Peu importe ce que vous avez de valeur, les criminels le veulent.

Vos informations d’identification en ligne sont précieuses. Ces informations d’identification permettent aux voleurs d’accéder à vos comptes. Vous pouvez penser que les cartes de fidélité que vous avez obtenues ne sont pas utiles aux yeux des cybercriminels. Méfiez-vous. Après qu’environ 10 000 comptes American Airlines et United Airlines ont été piratés, les cybercriminels ont réservé des vols et des surclassements gratuits en utilisant ces informations d’identification volées. Même si les points fidélité ont été rendus aux clients par les compagnies aériennes, cet incident démontre la valeur des informations d'identification. Un criminel peut également profiter de vos relations. Ils peuvent accéder à vos comptes en ligne et à votre réputation pour vous tromper et vous faire transférer de l’argent à vos amis et à votre famille. Le criminel peut envoyer des messages indiquant que votre famille ou vos amis ont besoin que vous leur envoyiez de l’argent pour qu’ils puissent revenir chez eux de l’étranger après avoir perdu leurs portefeuilles.

Les criminels sont très imaginatifs lorsqu’ils essaient de vous tromper pour que vous leur donniez de l’argent. Non seulement ils volent votre argent, mais ils peuvent également voler votre identité et ruiner votre vie.

# Ils veulent votre identité

Pour les criminels, il ne s’agit pas de voler votre argent pour un gain monétaire à court terme, ils veulent des bénéfices sur le long terme en usurpant votre identité.

Comme les frais médicaux augmentent, l’usurpation d’identité médicale est également en hausse. Les usurpateurs peuvent voler votre assurance médicale et utiliser vos avantages médicaux pour eux-mêmes, et ces procédures médicales sont actuellement dans vos dossiers médicaux.

Les procédures de déclaration fiscale annuelle peuvent varier d'un pays à l'autre. Cependant, pour les cybercriminels, cette période est une merveilleuse opportunité. Par exemple, les personnes vivant aux États-Unis ont besoin de déclarer leurs impôts au plus tard le 15 avril de chaque année. L’IRS (Internal Revenue Service) ne vérifie pas la déclaration de revenus par rapport aux informations provenant de l’employeur avant le mois de juillet. Un usurpateur d’identité peut émettre une fausse déclaration d’impôt et percevoir le remboursement. Les déclarants légitimes ne le remarqueront que lorsque leur déclaration sera rejetée par l’IRS. En usurpant une identité, les usurpateurs peuvent ouvrir des comptes de carte de crédit et contracter des dettes en votre nom. Cela aura des impacts sur vos relevés bancaires et compliquera votre obtention de prêts.

Les informations d’identification personnelles peuvent également entraîner l’accès aux informations de l’entreprise et aux données du gouvernement.

# Les différents types de données d’entreprise

**Données traditionnelles**

Les informations de l’entreprise incluent les informations personnelles, les propriétés intellectuelles et les données financières. Les informations personnelles incluent des dossiers de candidature, des fiches de paie, des lettres d’offre, des contrats de travail et toute information utilisée dans les prises de décisions sur l’embauche. La propriété intellectuelle, comme les brevets, les marques déposées et les plans produit, permet à une entreprise d’avoir un avantage économique sur ses concurrents. Elle peut être considérée comme un secret commercial et la perdre serait désastreux pour l’avenir de l’entreprise. Les données financières, dont les comptes de résultat, les bilans comptables et les tableaux de trésorerie d’une entreprise, donnent un aperçu de la santé de l’entreprise.

**Internet des objets et Big Data**

Avec l’émergence de l’Internet des objets (IoT, Internet of Things), les données à gérer et à sécuriser sont de plus en plus nombreuses. L’IoT est un vaste réseau d’objets physiques, dont les capteurs et les équipements qui s’étendent au-delà du réseau informatique traditionnel. Toutes ces connexions, en plus du fait que nous avons des capacités et des services de stockage élargis grâce au cloud et à la virtualisation, entraînent la croissance exponentielle des données. Ces données ont créé un nouveau centre d’intérêt dans la technologie et l’entreprise. C’est ce qu’on appelle le « Big Data ». En raison de la vitesse, du volume et de la variété de données générés par l’IoT et les opérations quotidiennes de l’entreprise, la confidentialité, l’intégrité et la disponibilité de ces données sont vitales pour la survie de l’entreprise.

# Confidentialité, intégrité et disponibilité

Confidentialité, intégrité et disponibilité, appelées ensemble la triade CIA (Figure 1), sont une directive pour la sécurité de l’information pour une entreprise. La confidentialité garantit l’anonymat des données en limitant l’accès par le chiffrement de l’authentification. L’intégrité garantit que l’information est exacte et fiable. La disponibilité garantit que les personnes autorisées peuvent accéder à l’information.

**Confidentialité**

Un autre terme pour la confidentialité serait l’anonymat. Les politiques d’entreprise devront limiter l’accès à l’information au personnel autorisé et garantir que seules ces personnes autorisées consultent ces données. Les données peuvent être compartimentées selon le niveau de sécurité ou de sensibilité de l’information. Par exemple, un programme Java ne devrait pas avoir accès aux informations personnelles de tous les employés. Par ailleurs, les employés doivent suivre une formation pour comprendre les bonnes pratiques en matière de protection des informations sensibles pour se protéger et pour protéger l’entreprise contre les attaques. Parmi les méthodes permettant de garantir la confidentialité, il y a le cryptage des données, l’ID et le mot de passe liés au nom d’utilisateur, l'authentification à deux facteurs et la réduction au minimum de l’exposition des informations sensibles.

**Intégrité**

L’intégrité représente l’exactitude, la cohérence et la fiabilité des données pendant tout leur cycle de vie. Les données ne doivent pas être altérées durant le transfert ni être modifiées par des entités non autorisées. Les permissions de fichiers et le contrôle d’accès pour les utilisateurs peuvent empêcher l’accès non autorisé. Le contrôle des versions peut être utilisé pour empêcher des modifications accidentelles par des utilisateurs autorisés. Les sauvegardes doivent être disponibles pour restaurer les données corrompues et le hachage des sommes de contrôle peut permettre de vérifier l’intégrité des données pendant le transfert.

Une somme de contrôle est utilisée pour vérifier l’intégrité des fichiers ou des chaînes de caractères après leur transfert d’un périphérique à un autre dans votre réseau local ou sur Internet. Les sommes de contrôle sont calculées grâce à des fonctions de hachage. Parmi les sommes de contrôle les plus courantes, il y a MD5, SHA-1, SHA-256 et SHA-512. Une fonction de hash utilise un algorithme mathématique pour transformer les données en une valeur de longueur fixe qui représente les données, comme illustré à la Figure 2. La valeur hachée est simplement présente pour comparaison. Il est impossible d’extraire directement les données d’origine à partir de la valeur hachée. Par exemple, si vous avez oublié votre mot de passe, vous ne pourrez pas le récupérer à partir de la valeur hachée. Il vous faut réinitialiser le mot de passe.

Après le téléchargement d’un fichier, vous pouvez vérifier son intégrité en vérifiant les valeurs hachées à partir de la source en fonction de celles générées en utilisant un calculateur de hachage. En comparant les valeurs de hachage, vous pouvez être sûr que le fichier n’a pas été altéré avec le transfert ou corrompu pendant celui-ci.

**Disponibilité**

La maintenance des équipements, la réparation des matériels, la mise à jour des systèmes d’exploitation et des logiciels, et la création de sauvegardes permettent de garantir la disponibilité du réseau et des données pour les utilisateurs autorisés. Des plans doivent être mis en place pour reprendre rapidement les activités après des catastrophes naturelles ou d’origine humaine. Des équipements ou des logiciels de sécurité, notamment les pare-feu, évitent les interruptions dues aux attaques comme le déni de service (DoS). Le déni de service survient lorsqu'un hacker tente de saturer les ressources pour que les services ne soient pas disponibles pour les utilisateurs.

# Les conséquences d’une brèche dans la sécurité

Il n'est pas possible de protéger une entreprise contre toute cyberattaque potentielle, et ce, pour certaines raisons. L’expertise nécessaire pour configurer le réseau et assurer sa sécurité peut être très chère. Les agresseurs découvriront toujours de nouvelles méthodes pour cibler les réseaux. À terme, ils réussiront une cyberattaque avancée et ciblée. La priorité sera alors de déterminer à quelle vitesse votre équipe de sécurité peut répondre à l’attaque pour minimiser les pertes de données, le temps d’arrêt et la perte de chiffre d'affaires.

Dès maintenant, vous savez que tout ce que vous publiez en ligne peut y rester pour toujours, même si vous avez réussi à supprimer toutes les copies en votre possession. Si vos serveurs ont été piratés, les informations personnelles confidentielles peuvent devenir publiques. Un pirate informatique (ou un groupe de pirates) peut vandaliser le site Web d’une entreprise en publiant de fausses informations et ainsi, ruiner la réputation de cette entreprise qu'elle a mis des années à bâtir. Les pirates peuvent également arrêter le site Web de la société et lui causer des pertes du chiffre d'affaires. Si le site Web est en panne sur de plus longues périodes, l’entreprise peut paraître peu fiable et perdra éventuellement en crédibilité. Si le site Web ou le réseau de la société a été violé, cela pourrait entraîner la fuite de documents confidentiels, la révélation de secrets commerciaux et le vol de propriété intellectuelle. La perte de toutes ces informations peut entraver la croissance et l’expansion de l’entreprise.

Le coût d’une brèche est largement plus élevé que le remplacement des périphériques perdus ou volés, l’investissement dans la sécurité existante et le renforcement de la sécurité physique du bâtiment. L’entreprise peut être chargée d’informer tous les clients concernés de la brèche et pourrait avoir à faire face à des procédures judiciaires. Avec toute cette tourmente, les employés peuvent choisir de quitter l’entreprise. L’entreprise peut avoir besoin de se concentrer davantage sur la réparation de sa réputation que sur sa croissance.

# Les différents types d’agresseurs

Les agresseurs sont des individus ou des groupes qui tentent d’exploiter la vulnérabilité à des fins personnelles ou financières. Ils s’intéressent à tout, des cartes de crédit aux conceptions de produits et tout ce qui a de la valeur.

**Amateurs** – Ces personnes sont quelques fois appelées Script Kiddies. Ce sont généralement des agresseurs avec peu ou pas de compétence. Ils utilisent souvent des outils ou des instructions découvertes sur Internet pour lancer des attaques. Certains d’entre eux sont simplement curieux, tandis que d’autres essaient de démontrer leurs compétences et entraînent des méfaits. Ils peuvent utiliser des outils basiques, mais le résultat peut quand même être dévastateur.

**Pirates (hackers)** – Ce groupe d’agresseurs entre par effraction dans les ordinateurs ou dans les réseaux pour obtenir l’accès. Selon l’objectif de l’intrusion, ces agresseurs sont classés chapeaux blancs, chapeaux gris ou chapeaux noirs. Les agresseurs Chapeaux blancs entrent par effraction dans les réseaux ou dans les systèmes informatiques pour en découvrir les faiblesses afin que la sécurité de ces systèmes puisse être améliorée. Ils effectuent ces intrusions sur autorisation et tous les résultats sont signalés au propriétaire. D’un autre côté, les agresseurs Chapeaux noirs profitent de toute vulnérabilité à des fins personnelles, financières ou politiques illégales. Les agresseurs Chapeaux gris se trouvent entre les Chapeaux noirs et les Chapeaux blancs. Ils peuvent découvrir une vulnérabilité dans un système. Ils peuvent signaler la vulnérabilité aux propriétaires du système si cela correspond à leur plan. Mais certains pirates Chapeaux gris publient les faits sur la vulnérabilité sur Internet pour que d'autres agresseurs puissent l’exploiter.

La figure propose des détails sur les termes pirate informatique Chapeau blanc, pirate informatique Chapeau noir et pirate informatique Chapeau gris.

**Pirates organisés** – Ces pirates incluent des organisations de cybercriminels, des hacktivistes, des terroristes et des pirates financés par des gouvernements. Les cybercriminels sont généralement des groupes de criminels professionnels qui misent sur le contrôle, le pouvoir et la richesse. Ils sont très sophistiqués et organisés et ils peuvent même offrir des services de cybercrime à d’autres criminels. Les hacktivistes effectuent des déclarations politiques pour sensibiliser sur les questions qui leur sont importantes. Les agresseurs financés par des gouvernements rassemblent des renseignements ou commettent des sabotages au nom de leurs gouvernements. Ces agresseurs sont généralement très bien formés et bien financés et leurs attaques sont axées sur des objectifs spécifiques qui profitent à leur gouvernement.

Menaces internes et externes

**Menaces internes pour la sécurité**

Les attaques peuvent provenir de l’intérieur d’une entreprise ou de l’extérieur, comme illustré dans la figure. Un utilisateur interne, par exemple un employé ou un partenaire contractuel, peut accidentellement ou intentionnellement :

* Mal gérer les données confidentielles ;
* Menacer le fonctionnement des serveurs internes ou des périphériques de l’infrastructure réseau ;
* Faciliter les attaques venant de l’extérieur en connectant un support USB infecté dans le système informatique de l’entreprise ;
* Inviter accidentellement un malware dans le réseau par des e-mails ou des sites Web malveillants.

Les menaces internes sont également susceptibles d'entraîner des dégâts plus importants que ceux des menaces externes, car les utilisateurs internes disposent d’un accès direct au bâtiment et aux périphériques de l’infrastructure. Les employés connaissent également le réseau d’entreprise, ses ressources et ses données confidentielles, ainsi que les différents niveaux de privilèges des utilisateurs et des administrateurs.

**Menaces externes pour la sécurité**

Les menaces externes provenant des amateurs et des agresseurs expérimentés peuvent exploiter les vulnérabilités dans le réseau ou dans les périphériques informatiques, ou utiliser le piratage psychologique pour obtenir l’accès.

# Qu’est-ce que la guerre cybernétique ?

Le cyberespace est devenu une autre dimension importante de la guerre ; c’est là que les pays peuvent entrer en conflit sans avoir à affronter les troupes et machines de guerre traditionnelles. Cela permet aux pays avec une présence militaire réduite d’être aussi puissant que les autres dans le cyberespace. La guerre cybernétique est un conflit basé sur Internet qui implique la pénétration dans les réseaux et les systèmes informatiques des autres pays. Ces agresseurs disposent de ressources et d’expertise pour lancer des attaques massives basées sur Internet contre d’autres pays pour entraîner des dégâts ou interrompre les services, par exemple en arrêtant une infrastructure électrique.

L’attaque ayant impliqué le programme malveillant Stuxnet qui a été conçu pour endommager l’usine d’enrichissement nucléaire de l’Iran constitue un exemple d’attaque financée par des gouvernements. Le programme malveillant Stuxnet n’a pas piraté des ordinateurs pour voler des informations. Il a été conçu pour endommager des équipements physiques contrôlés par des ordinateurs. Ce malware a utilisé un codage modulaire programmé pour effectuer une tâche spécifique dans le matériel. Stuxnet a utilisé des certificats numériques volés pour que l’attaque semble légitime sur le système. Cliquez sur Lire pour regarder la vidéo concernant Stuxnet.

Cliquez [ici](https://contenthub.netacad.com/legacy/I2CS/2.1/fr/course/files/1.4.1.1%20Video%20-%20Breaking%20Down%20Stuxnet.pdf) pour lire la transcription de cette vidéo.

Cliquez [ici](https://vimeo.com/25118844) pour voir une autre vidéo et en savoir plus sur Stuxnet.

# L’objectif de la guerre cybernétique

L’objectif principal de la guerre cybernétique est d’obtenir un avantage sur les hackers, qu’ils soient des nations ou des concurrents.

Un pays peut envahir en permanence l’infrastructure d’un autre pays, voler des secrets de défense et rassembler des informations sur la technologie pour combler les manques dans ses industries et dans son armée. En plus de l’espionnage industriel et militaire, la cyberguerre peut saboter l’infrastructure d'autres pays et coûter des vies dans les pays ciblés. Par exemple, une attaque peut interrompre l’infrastructure électrique d’une grande ville. Le trafic serait interrompu. L’échange de biens et services est entravé. Les patients ne pourront pas recevoir les soins nécessaires dans des situations urgentes. L’accès à Internet peut également être interrompu. En affectant l’infrastructure électrique, l’attaque peut affecter la vie quotidienne des citoyens ordinaires.

En outre, des données sensibles compromises peuvent permettre aux agresseurs de prendre en otage le personnel au sein du gouvernement. L’information peut permettre à un agresseur de prétendre être un utilisateur autorisé pour accéder à des équipements ou à des informations sensibles.

Si le gouvernement n’est pas capable de se défendre contre les cyberattaques, les citoyens peuvent perdre leur confiance dans les capacités du gouvernement à les protéger. La guerre cybernétique peut déstabiliser un pays, interrompre le commerce et affecter la confiance des citoyens en leur gouvernement, même sans invasion physique du pays ciblé.

# Conclusion

Ce chapitre a permis d’expliquer les caractéristiques et les propriétés de la cybersécurité. Il a permis d’expliquer pourquoi les professionnels de la cybersécurité seront de plus en plus demandés. Le contenu explique pourquoi votre identité et vos données personnelles en ligne sont vulnérables vis-à-vis des cybercriminels. Il présente également quelques conseils sur comment protéger votre identité et vos données personnelles en ligne.

Ce chapitre traite également des données de l’entreprise : qu’est-ce que c’est, où sont-elles et pourquoi faut-il les protéger. Il explique qui sont les agresseurs et ce qu’ils veulent. Les professionnels de la cybersécurité doivent avoir les mêmes compétences que les agresseurs informatiques. Ils doivent également travailler dans le cadre des législations locales, nationales et internationales. Les professionnels de la cybersécurité doivent également faire preuve d’éthique.

Enfin, ce chapitre a permis d’expliquer brièvement la guerre cybernétique et les raisons qui incitent les pays et gouvernements à recourir aux professionnels de la cybersécurité pour les aider à protéger leurs citoyens et leurs infrastructures.

Si vous souhaitez découvrir plus en détail les concepts de ce chapitre, référez-vous à la page des [ressources et activités supplémentaires](https://contenthub.netacad.com/legacy/I2CS/2.1/fr/course/files/IntroCybersecurity%20-%20Additional%20Resources%20and%20Activities.pdf) dans les Ressources des étudiants.