ISSN: 2658-8455
Volume 4, Issue 3-2 (2023), pp. 451-469

IJAFAME
International Journal of Accounting, Finance, Auditing, Management & Economics

Cybercriminalité et cyber-résilience : Les enjeux de la sécurité numérique dans un monde connecté

Cybercrime and Cyber Resilience: The Challenges of Digital Security in a Connected World

Bouchra BOUNAAMANE, *(Doctorante)*
Laboratoire Etudes et Recherches en Management des Organisations et des Territoires (ERMOT)
Faculté des Sciences Juridiques, Économiques et Sociales de Fès
Université Sidi Mohamed Ben Abdellah de Fès, Maroc

Zineb DRISSI, *(Professeur d'Enseignement Supérieur)*
Laboratoire Etudes et Recherches en Management des Organisations et des Territoires (ERMOT)
Faculté des Sciences Juridiques, Économiques et Sociales de Fès
Université Sidi Mohamed Ben Abdellah de Fès, Maroc

Adresse de correspondance :	Faculté des Sciences Juridiques, Économiques et Sociales BP 42, Fès USMBA de Fès Maroc (Fès) 30000 0663-215258
Déclaration de divulgation :	Les auteurs n'ont pas connaissance de quelconque financement qui pourrait affecter l'objectivité de cette étude.
Conflit d'intérêts :	Les auteurs ne signalent aucun conflit d'intérêts.
Citer cet article	BOUNAAMANE, B., & DRISSI, Z. (2023). Cybercriminalité et cyber-résilience : Les enjeux de la sécurité numérique dans un monde connecté. International Journal of Accounting, Finance, Auditing, Management and Economics, 4(3-2), 451-469. https://doi.org/10.5281/zenodo.8063576
Licence	**Cet article est publié en open Access sous licence CC BY-NC-ND**

Received: May 19, 2023 *Accepted: June 19, 2023*

Cybercriminalité et cyber-résilience : Les enjeux de la sécurité numérique dans un monde connecté

Résumé :

Au cours des deux dernières décennies, le Maroc a connu une transformation notable pour devenir le principal centre technologique en Afrique. Le pays a enregistré le taux de croissance le plus élevé dans la région Afrique-Moyen-Orient en ce qui concerne les technologies de l'information et de la communication (TIC). Cette évolution rapide et réussie témoigne des progrès significatifs réalisés par le Maroc dans le domaine de la technologie.

Dans le contexte numérique actuel, les entreprises sont confrontées au défi de gérer de vastes ensembles de données et d'informations. Cette situation les rend de plus en plus incapables de les gérer et de les exploiter de manière efficace. Par conséquent, elles se retrouvent souvent à adopter des solutions qui sont inefficaces, coûteuses et risquées. Cela peut entraîner des problèmes tels que des pertes financières, une mauvaise prise de décision et une vulnérabilité accrue face aux menaces numériques.

En outre, la cybercriminalité constitue une menace croissante pour les entreprises, y compris celles du Maroc. Les cybercriminels exploitent l'essor rapide des technologies de l'information et de la communication, en particulier Internet, qui est devenu un outil essentiel pour le développement économique et la transformation sociale. La cybercriminalité ne connaît pas de frontières géographiques, ce qui signifie que les entreprises marocaines doivent prendre des mesures pour se protéger contre ces menaces et assurer leur stabilité.

Beaucoup d'internautes sont maintenant conscients des risques des cyberattaques et de leur impact potentiellement dévastateur sur la continuité des activités. Cependant, il est clair que la sécurité axée sur la protection présente des limites. Face à la menace croissante, il est essentiel de connaitre que le risque est devenu inévitable. Pour assurer la cyber-résilience d'une entreprise, il est impératif de mettre en place et de déployer une stratégie de cyber sécurité bien préparée qui assurera la cyber-résilience d'une entreprise donnée.

C'est en raison de cette particularité du sujet que nous avons réalisé une enquête et rédigé cet article. Ce dernier vise à explorer les concepts de base de la cybercriminalité et sa relation avec la cyber-résilience.

L'enquête sur le terrain a porté sur un échantillon de 19 entreprises provenant de divers secteurs d'activité et situées dans différentes régions du Maroc, dans le but d'obtenir une vision globale du sujet traité dans notre article. La collecte de données a été effectuée à l'aide d'un questionnaire, et les données ont été analysées à l'aide du logiciel SPSS.

Mots clés : Cybercriminalité, technologies de l'information et de la communication, entreprises marocaines, transformation technologique, cyber-résilience.
Classification JEL : M4, M49
Type de l'article : Recherche appliquée

Abstract:

Over the past two decades, Morocco has undergone a significant transformation to become the leading technology centre in Africa. The country has recorded the highest growth rate in the Africa-Middle East region in information and communication technologies (ICT). This rapid and successful development reflects the significant progress Morocco has made in the field of technology.

In today's digital environment, companies are faced with the challenge of managing vast amounts of data and information. This situation makes them increasingly unable to manage and exploit it effectively. As a result, they often find themselves adopting solutions that are inefficient, costly and risky. This can lead to problems such as financial losses, poor decision making and increased vulnerability to digital threats.

In addition, cybercrime is a growing threat to businesses, including those in Morocco. Cybercriminals are exploiting the rapid growth of information and communication technologies, in particular the Internet, which has become an essential tool for economic development and social transformation. Cybercrime knows no geographical boundaries, which means that Moroccan businesses must take steps to protect themselves against these threats and ensure their stability.

Many internet users are now aware of the risks of cyber-attacks and their potentially devastating impact on business continuity. However, it is clear that protection-focused security has its limitations. Faced with the growing threat, it is essential to acknowledge that risk has become inevitable. To ensure the cyber resilience of a company, it is imperative to establish and deploy a well-prepared cybersecurity strategy that will ensure the cyber resilience of a specific company.

It is because of this particularity of the subject that we conducted a survey and wrote this article. The aim of this article is to explore the basic concepts of cybercrime and its relationship with cyber-resilience.

The field survey was carried out on a sample of 90 companies from various business sectors and located in different regions of Morocco, with the aim of obtaining a global view of the subject covered in our article. Data was collected using a questionnaire, and analyzed using SPSS software.

Keywords : Cybercrime, information and communication technologies, Moroccan companies, technological transformation, cyber resilience.
JEL Classification : M4, M49
Paper type : Empirical research

ISSN: 2658-8455
Volume 4, Issue 3-2 (2023), pp. 451-469

IJAFAME
International Journal of Accounting, Finance, Auditing, Management & Economics

1. Introduction

Ramon Abbas, également connu sous le nom de Hushpuppi, est un influenceur nigérien qui s'est fait connaitre pour sa vie luxueuse affichée sur les réseaux sociaux. Cependant, il est soupçonné d'avoir détourné des centaines de millions de dollars grâce à des escroqueries en ligne en 2020, selon des informations de la BBC. Ces escroqueries, bien que très médiatisées, ne représentent qu'une petite partie de l'énorme problème de la cybercriminalité.

La cybercriminalité constitue un problème croissant pour les entreprises marocaines, qui dépendent de plus en plus des technologies de l'information et de la communication. Cette dépendance expose les entreprises à des risques en matière de sécurité des données et de protection des informations sensibles.

En raison de l'adoption croissante des technologies numériques, les entreprises marocaines sont de plus en plus visées par des attaques cybercriminelles. La montée en puissance du Maroc en tant que hub technologique en Afrique a attiré l'attention des cybercriminels qui cherchent à exploiter ces opportunités à des fins malveillantes.

À l'avenir, la capacité d'une entreprise à résister aux cyberattaques deviendra un élément essentiel pour sa survie. Selon Boris Cyrulnik, la résilience consiste à naviguer habilement dans les situations difficiles. La cyber-résilience englobe à la fois la cybersécurité et la gestion de la continuité des activités. Son objectif est de se prémunir contre les cyberattaques potentielles et de garantir la survie de l'entreprise en cas d'attaque.

Nous prenons également en compte l'impact économique d'une cyberattaque sur les entreprises et l'économie en général, y compris les pertes financières, les coûts de récupération, les atteintes à la réputation et la perte de confiance des consommateurs. Nous examinerons comment la cyber-résilience peut aider les entreprises à atténuer ces risques et à protéger leurs actifs financiers.

À partir de toutes ces considérations, la problématique que nous nous posons est la suivante :

Comment la cybercriminalité impacte-t-elle la nécessité et l'importance de développer des stratégies de cyber-résilience ?

Cette question de recherche globale peut être subdivisée en trois sous-questions : Qu'est-ce que la cybercriminalité ? Quelles sont les attaques les plus connues en matière de cybercriminalité ? Comment la cyber-résilience peut-elle atténuer les conséquences de la cybercriminalité et assurer la continuité des activités des entreprises ?

Pour cela, notre article suit une structure claire et organisée. Dans une première partie, nous examinons le cadre conceptuel en analysant la littérature existante sur trois aspects fondamentaux : La cybercriminalité, la cyber-résilience et la théorie de la gestion des risques. Nous explorons ces concepts en détail pour construire une base solide et une compréhension approfondie du sujet. La deuxième partie de notre article est consacrée à la méthodologie de recherche, nous adoptons une approche épistémologique positiviste. Notre raisonnement suit une approche déductive ou hypothético-déductive, commençant par une revue de la littérature et aboutissant à l'élaboration d'une proposition de recherche, cette dernière sera ensuite confrontée à des données empiriques recueillies sur le terrain. Pour notre étude empirique, nous avons choisi une approche de recherche quantitative pour tester notre modèle de recherche en validant ou en rejetant nos hypothèses. Enfin, notre conclusion souligne les limites de cette étude et discute des perspectives de recherches futures. Nous mettons en évidence les forces et les faiblesses de notre travail, en identifiant les domaines qui pourraient bénéficier d'une enquête plus approfondie.

2. Revue de littérature

2.1. La cybercriminalité : concepts généraux

Alors que la cybercriminalité se professionnalise et gagne en puissance chaque instant, mais jusqu'aujourd'hui il n'existe pas une définition universelle pour elle, ce qui rend ce terme difficile à conceptualiser due l'absence d'aucune définition légale ou réglementaire (Chawki, 2006).
Le terme « cybercriminalité » a été employé la première fois par le groupe de Lyon en 1996 (El Azzouzi, 2010), pour décrire, de façon relativement imprécise, tous les types de délits commis sur internet ou les nouveaux réseaux de communication.

2.1.1. La cybercriminalité, un phénomène transnational

Quoique non définie, et vue que c'est un phénomène transnational et qu'elle ne se réduit pas à sa dimension géographique, sur la base de toutes ces considérations nous allons voir dans un premier lieu la signification de mot « cybercriminalité », et en second lieu les différentes définitions adoptées en Europe et d'autres adoptées aux États-Unis, afin d'avoir une idée quasiment globale.
Le préfixe « cyber » a une histoire compliquée, il a été inventé à l'origine par Norbert Wiener et Arturo Rosenblueth dans les années 1940 alors qu'ils étaient les pionniers du domaine de la « cybernétique » (Wiener, 1948). Wiener et ses contemporains voyaient la cybernétique comme un domaine émergent axé sur les machines et les systèmes de rétroaction (Rid, 2016). Le cyber est devenu un moyen populaire de décrire apparemment tout ce qui concerne les ordinateurs et l'internet. Attaché à la « criminalité » connue depuis longtemps, forment une relation sophistiquée, donne naissance à de nombreuses victimes (Gueye, 2018).

2.1.2. La cybercriminalité, vers un encadrement à l'échelle internationale

Nous commencerons par situer la cybercriminalité dans le contexte européen, pour ensuite l'examiner dans le contexte des États-Unis.

- **Celui du ministère intérieur français :**

Afin de protéger les citoyens, la mission du ministère de l'intérieur est d'assurer l'Etat de droit, tant dans ses aspects littéraux que virtuels.
Conscient des dangers liés au développement du numérique, ce ministère a créé en 2014 la sous-direction de la lutte contre la cybercriminalité (SDLC) qui fait partie de la direction centrale de la police judiciaire du ministère de l'intérieur français.
La définition de la cybercriminalité de ce dernier est plus large : elle englobe « tous les actes délictueux susceptibles d'être commis sur les réseaux de télécommunications en général, et plus particulièrement sur Internet » selon le ministère de l'intérieur.

- **Celui de l'office Fédéral de la Police Suisse :**

Pour l'Office fédéral de la police suisse, la cybercriminalité s'entend « des nouvelles formes de criminalité spécifiquement liées aux technologies modernes de l'information, et de délits connus qui sont commis à l'aide de l'informatique plutôt qu'avec les moyens conventionnels » (Rapport d'analyse stratégique, 2001).

- **Celui de la convention de Budapest sur la cybercriminalité :**

Les Etats membres du Conseil de l'Europe et d'autres signataires de la Convention ont élaboré une classification claire de la cybercriminalité et des mesures pour la prévenir. Les principales classifications sont résumées dans (El Azzouzi, 2010) :

  - Les atteintes à la confidentialité, à l'intégrité et à la disponibilité des données et des systèmes informatiques,
  - Les atteintes purement informatiques (Falsification, et fraude informatique),

ISSN: 2658-8455
Volume 4, Issue 3-2 (2023), pp. 451-469

IJAFAME
International Journal of Accounting, Finance, Auditing, Management & Economics

- Les atteintes relatives à la contrefaçon de la propriété intellectuelle et des droits connexes.

Il convient de noter que cette Convention joue un rôle primordial au niveau mondial en favorisant le renforcement et l'harmonisation des législations nationales sur la cybercriminalité et en améliorant les partenariats entre les pays et les différents secteurs (Budapest, 23.XI,2001).

- **Celui de Département de la Justice des États-Unis :**

Selon le département américain de la Justice, la cybercriminalité est considérée comme une « violation du droit pénal impliquant la connaissance des technologies de l'information », qui distingue trois catégories de cybercriminalité (Pereira, 2016).
La première catégorie concerne les délits contre le matériel informatique, comme l'accès à un réseau.
Dans la deuxième catégorie, les ordinateurs sont utilisés comme armes. Par exemple, cela impliquerait de lancer une attaque par déni de service (DDoS) sur l'entreprise (Babinet, 2020).
La troisième catégorie est l'utilisation d'ordinateurs comme accessoire du crime. Par exemple, les criminels peuvent utiliser des machines pour stocker des données obtenues illégalement (El Azzouzi, 2010).

- **Celui de la Division Cybernétique du FBI et la CISA :**

Dans un premier temps, FBI la police fédérale américaine, a déclaré à plusieurs reprises, que les cybercrimes ont eu un impact dévastateur sur la sécurité économique et nationale des États-Unis. Les cybercrimes s'articulent autour de trois priorités principales : l'intrusion informatique, l'usurpation d'identité et la cyberfraude (Ghernaouti, 2017).
Dans un deuxième temps, la Cybersecurity and Infrastructure Security Agency (CISA) dirige le travail stratégique et unifié de la nation pour renforcer la sécurité, la résilience et la main-d'œuvre du cyberécosystème afin de protéger les services critiques et le monde de vie américain (CISA, 2021).

- **Celui du code pénal de Californie :**

Le code définit une liste d'actes illégaux entrant dans le champ de la cybercriminalité. Il accèdera ou permettra sciemment d'accéder à tout système ou réseau informatique afin de :

- Concevoir ou exécuter tout stratagème visant à frauder ou à faire extorquer,
- Obtenir de l'argent, des biens ou des services dans le bit de frauder,
- Altérer, détruire ou endommager tout système informatique, réseau, programme ou données (Boos, 2017).

Force est de constater que ce terme prend une ampleur immense, et elle-même définie de diverses façons complémentaires. La cybercriminalité est utilisée à toutes les sauces, même si elle demeure encore floue.

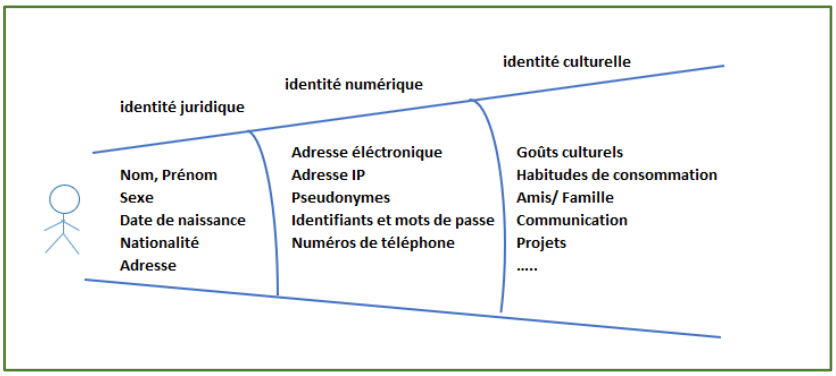
2.1.3. Techniques de cyberattaque : des maux qui ne cessent de faire des dégâts

Les cyberattaques représentent une menace potentielle pour toutes les entreprises, indépendamment de leur taille ou de leur secteur d'activité. La différence peut se réside dans la technique adoptée par les cyber-attaquants. Retour sur les techniques les plus dangereuses, les plus courantes ces dernières années.

2.1.3.1 L'usurpation d'identité : le cauchemar des victimes

L'identité numérique au sens strict est celle qui rend une personne unique sur le Web, tout comme la carte d'identité ou ADN, il le rend unique administrativement ou génétiquement (Tannier, 2010).
L'usurpation d'identité est une technique prépondérante aux différents pays du monde, la France par exemple enregistre 2000 à 2500 cas chaque année (Banque de France, 2013).

Figure 1 : Les différentes identités possibles



Source : Auteurs

L'usurpation d'identité est l'acte délibéré d'usurper l'identité d'une autre personne vivante pour commettre une fraude commerciale, civile ou pénale afin d'obtenir les finances d'une personne usurpée, ou de commettre un crime en son nom, ou d'accéder indument à (prestations sociales) (loi de juillet 2013) afin de bénéficier du marché ou des services sociaux à la place ou à leurs frais (Mattatia, 2014).

Les cybercriminels innovent constamment et inventent de nouvelles technologies pour chaque catégorie, voici quelques-unes des techniques utilisées pour le vol d'identité :

- Le SIM-Swapping : utilisée depuis 2016, cette technique visait initialement les détenteurs de cryptomonnaies. Cependant, en 2019, la même technique a été utilisée contre des personnes ou des comptes très en vue dans l'intention d'usurper l'identité de la victime (Enisa, 2021).

Si on parle de la manière de swapper une carte SIM, on peut dire que:

- Le fraudeur vole les informations d'indentification et le numéro de téléphone portable du client de la banque,
- Il manipule l'opérateur de téléphone mobile pour effectuer un échange de carte SIM sur le numéro de téléphone mobile du client,
- Il utilise les informations d'indentification du client pour initier une connexion à son compte bancaire en ligne,
- La banque envoie un SMS OTP au numéro de mobile du client, cependant l'OTP arrive sur l'appareil mobile du fraudeur et il est utilisé pour accéder au compte du client (Gupta & Awale, 2019).

- Les cartes cadeaux utilisées comme cheval de Troie pour compromettre la messagerie d'entreprise (BEC - Business Email Compromise). Dans de tels incidents, les attaquants se font passer pour une personne de confiance, appartenant généralement à l'entreprise (Litzistorf & Solleder, 2005), pour inciter la victime par la ruse à effectuer une transaction financière ou à divulguer des informations sensibles, personnelles ou professionnelles. Dans plus de la moitié des attaques BEC, la victime a été incitée à acheter une carte cadeau (Filiol, 2009). Au cours de la procédure d'achat, des informations sensibles, telles que des références de compte bancaire, ont été interceptées.

2.1.3.2. L'ingénierie sociale : causée par la fragilité humaine surtout

L'ingénierie sociale, comme d'autres techniques, est aujourd'hui un véritable fléau. Il n'existe pas un bien-fondé derrière cette technique, au contraire, l'ingénierie sociale ne cache que la volonté des pirates d'arnaquer, de voler, de tromper, de nuire et de tirer profit de leurs crimes informatiques.

Pour définir, l'ingénierie sociale est l'art de manipuler psychologiquement des personnes afin d'obtenir des informations confidentielles, et de les escroquer (Penven, 2013). Ces attaques ciblent en premier lieu les individus, vus que ces derniers restent la source la plus simple pour

ISSN: 2658-8455
Volume 4, Issue 3-2 (2023), pp. 451-469

IJAFAME
International Journal of Accounting, Finance, Auditing, Management & Economics

y arriver à leurs besoins à travers la force de persuasion et l'exploitation de la naïveté des utilisateurs, qui ont une tendance naturelle à faire confiance à l'autre (Ngo,2019).
L'explosion de la présence en ligne, l'utilisation des réseaux sociaux de manière massive, et la généralisation de la VoIP ont des conséquences (Coelho,2022) peuvent parfois être particulièrement douloureuses pour les victimes.

Figure 2 : Des éléments créant l'ingénierie sociale

Source : Auteurs

2.1.3.3. L'hameçonnage, ou Phishing : la portée d'entrée privilégiée des cybercriminels

De nombreux risques existent, comme nous l'avons déjà mentionné au début, mais celui de Phishing reste le risque le plus propagé dans le monde numérique.
Partant de ce fait, le Phishing est un ensemble de techniques basées sur l'envoi des e-mails à des destinataires choisies de façon aléatoire ou à travers des données obtenues illégalement, pour des objectifs purement financiers (Enisa, 2020).
La technique se fait par exemple comme suit : la victime reçoit un e-mail envoyé par un attaquant indiquant qu'il y a eu une violation de son compte bancaire et que le mot de passe doit être changé de toute urgence, accompagné d'un lien pour changer le mot de passe (Rapport Human Factor, 2015). Une fois le lien cliqué, la victime arrive sur un site qu'il pense être celui de la banque, alors qu'il s'agit en réalité d'une copie hébergée ailleurs et contrôlée par les cybercriminels, entrant ses informations d'ordre personnel, ajoutant aussi ses informations bancaires par la suite, de sorte que les attaquants arrivant à récupérer ces éléments et de les utiliser en effectuant des virements vers d'autres comptes dans la majorité des cas (Pernet, 2015).

2.1.3.4. Le Rançongiciel, ou Ransomware : une menace grandissante pour les entreprises

Un seul clic et l'informatique est paralysée, ces logiciels malveillants (malware, en anglais) bloquent les ordinateurs des victimes et réclament ensuite le paiement d'une « rançon » pour leur déverrouillage (Misini,2017). Pour parvenir à leurs fins, les cybercriminels utilisent des logiciels malveillants appelés rançongiciels, qui chiffrent les données personnelles d'une personne ou d'une organisation et exigent ensuite une rançon en échange de la clé de déchiffrement (Benabou,2021).
Parmi les différents types de rançongiciels en circulation, le plus répandu est le rançongiciel chiffrant, également connu sous le nom de crypto ransomware (Savage, Coogan & Lau, 2015). Son objectif principal est de crypter les données et les fichiers, les rendant ainsi inaccessibles à leur propriétaire légitime (Fortin, 2020).

Tout comme COVID-19, les attaques de rançongiciels opérés par l'homme sont devenues la deuxième pandémie en 2020 (Skulkin, 2022). Le principe est connu et pourtant il continue d'être sur le podium des compromissions les plus couteuses.

2.1.3.5. Le courrier indésirable, ou Spam : un vecteur d'attaque toujours présent

Le SPAM n'est pas seulement un e-mail, le SPAM est un envoi massif des mails non sollicités par un expéditeur vers un grand nombre de destinataires, il a des fins commerciales, publicitaires ne respectant pas les obligations légales en matière de consentement des destinataires (Guillon, 2008). Et dans la majorité, il représente des fins à caractère malveillant, comme les tentatives de Phishing ou Ransomware via les comptes de messagerie. Quoi qu'il en soit, le SPAM est une véritable pollution numérique.

Le SPAM prend aussi une forme téléphonique, soit par SMS, MMS, ou un appel téléphonique, incitant le récepteur à rappeler un numéro surtaxé, envoyer un message à un numéro payant, et même de récupérer ses données confidentielles via les tentatives de Phishing (Barracuda, 2020).

Les SPAM ont toujours le vent en poupe, ils ne coutent presque absolument rien aux spammeurs et ils ne nécessitent pas un matériel à mettre en œuvre (Gastellier Prevost, 2009).

De faire simple, les spammeurs utilisent les e-mails pour envoyer des documents ou fichiers contenant des logiciels malveillants (malware, en anglais). Les malwares les plus répondus sont les virus, les chevaux de Troie, les logiciels espions (Barracuda, 2020). Toutes ces attaques sophistiquées partagent le même objectif, c'est de détruire le système de la victime et de tirer le maximum de profit financier.

De manière succincte :

- Le virus est un parasite qui, en s'attachant à un programme, peut contaminer l'ensemble de l'ordinateur (Charpentier, Montigny & Rousseau, 2004), et il est susceptible d'entrainer d'énormes perturbations dans son fonctionnement (Poirot, 2018). L'un des plus célèbres est le virus 'I love you' qui a sévi en 2000. Un message intitulé 'I love you' contenait une pièce jointe qui, lorsqu'elle était ouverte, se servait du carnet d'adresses de la victime pour se propager.
- Le cheval de Troie (Trojan Horse en anglais), est un logiciel en apparence légitime, mais lorsqu'il est ouvert, il permet au programme d'infecter ou de prendre le contrôle de l'ordinateur, et il peut causer plusieurs dégâts. Le cheval de Troie Emotet est une sorte de malware conçu principalement pour siphonner les informations financières et bancaires des utilisateurs par des e-mails de spam (malspams) (Abdelli & Ahmed Nacer, 2015).

Le logiciel espion ou mouchard (Spyware en anglais), il est un logiciel qui s'infiltre discrètement dans l'ordinateur pour surveiller et enregistrer l'activité et les informations confidentielles d'utilisateur (Kaldani & Prokopets, 2022). Ce logiciel peut être installé sur un Pc comme sur une tablette, un smartphone etc.

Lorsqu'une attaque a réussi, des secrets ont été volés, de l'argent dérobé, laissant derrière elle le débris d'une entreprise fragilisée et des salariés traumatisés et perturbés, et cela se généralise aussi sur les particuliers.

Cela nous amène à considérer la cyber-résilience comme une solution pour atténuer le risque de devenir victime de la cybercriminalité.

2.2. La cyber-résilience : un pilier crucial face à la menace croissante de la cybercriminalité

Il est désormais inévitable pour les entreprises d'être confrontées à une attaque, la question n'est plus de savoir si cela se produira, mais quand. Face à ce nouveau contexte, les entreprises doivent adopter une approche de la sécurité informatique basée sur la gestion des risques plutôt que sur leur élimination. C'est ainsi qu'est né le concept de cyber résilience.

ISSN: 2658-8455
Volume 4, Issue 3-2 (2023), pp. 451-469

IJAFAME
International Journal of Accounting, Finance, Auditing, Management & Economics

2.2.1. La cyber-résilience : comprendre les notions clés

La Banque Centrale Européenne a défini la cyber-résilience comme la capacité à se protéger et à reprendre rapidement ses activités en cas de cyber-attaque réussie. Cette définition a incité de nombreuses entreprises à adopter une approche globale du sujet, englobant la prévention, la gestion de crise, la reconstruction et la continuité des activités.

Le Dr Boris Cyrulnik, neurologue et psychiatre bordelais, utilise la métaphore de "naviguer dans les torrents" pour décrire la résilience. En psychologie, la résilience se réfère à la capacité d'un individu à se reconstruire et à mener une vie normale même après avoir vécu des traumatismes. En informatique, le principe est similaire. La cyber-résilience désigne la capacité d'une entreprise à maintenir ses opérations malgré une attaque ou une panne.

Le choix du terme "résilience" est délibéré : être résilient signifie pouvoir se rétablir rapidement d'une difficulté, être conscient de son environnement et renforcer ses positions et son expertise pour assurer la continuité des affaires (Hayes & Kotwica, 2019).

L'objectif de la résilience est d'évaluer les risques informatiques afin de limiter l'impact d'un incident, de maintenir le fonctionnement des applications essentielles, de préserver les données et de permettre une reprise rapide des activités. Ainsi, la résilience ne concerne pas seulement le département informatique, mais l'ensemble de l'entreprise.

La cyber-résilience repose sur deux axes principaux : faire face aux menaces en adoptant une approche préventive plutôt que curative, et être capable de rétablir rapidement la productivité en cas d'attaque informatique réussie. En somme, l'entreprise doit se préparer à toute éventualité, sachant qu'elle est constamment exposée aux attaquants cybernétiques qui peuvent frapper à tout moment (Cohen, 2016).

Prenons l'exemple des ransomwares, apparus pour la première fois en 1989. Les études montrent que la protection contre les ransomwares est une priorité absolue pour la plupart des entreprises, car elles cherchent à éviter la perte de productivité, la détérioration de leur réputation et de la confiance, ainsi que la diminution des revenus. Surtout avec la pandémie récente (Sakurai M, Chughtai H, 2020), qui a conduit à une période de télétravail sans préparation préalable.

La protection contre les ransomwares doit reposer sur une approche à deux volets mettant l'accent sur la sécurité et la résilience :

La cybersécurité vise principalement à prévenir les intrusions : "Verrouillez les portes pour empêcher les acteurs malveillants d'entrer en premier lieu."

La cyber-résilience vise à faire face à une violation cybernétique : "Il est probable que nous soyons dépassés. Nous devons planifier et nous préparer à poursuivre nos opérations malgré une brèche."

Il est essentiel de souligner que les entreprises doivent s'efforcer d'être à la fois sécurisées sur le plan cybernétique et résilientes face aux incidents.

2.2.2. Cyber-résilience et cybersécurité : les distinctions essentielles

La cybersécurité repose sur un principe binaire : soit l'environnement est sûr, soit il ne l'est pas. Elle englobe les mesures mises en place pour protéger un système d'information contre les menaces numériques, en empêchant les hackers d'accéder aux serveurs et aux données. En revanche, la cyber-résilience implique d'accepter sa vulnérabilité et d'être capable de riposter (Robertson & Rice, 2020). Elle reconnaît que protéger entièrement son infrastructure numérique contre les attaques ou les pannes est difficile, mais il est crucial de prendre conscience de cette vulnérabilité et des dangers présents.

La cyber-résilience va au-delà des concepts de défense et de prévention. Elle met l'accent sur la politique de sécurité, la prévention des risques, les tests, la réponse aux incidents et la capacité de l'entreprise à se rétablir en période de crise. Contrairement à la cybersécurité qui vise à

prévenir et à gérer les incidents de sécurité, la cyber-résilience prépare l'entreprise à faire face aux conséquences d'une cyber-attaque et à retrouver sa capacité à créer de la valeur après avoir été victime d'une attaque (Cohen, 2016).

2.2.3. La cyber-résilience : un enjeu pour faire face aux cyber-menaces

La cyber-résilience d'une entreprise se manifeste par sa capacité à se défendre contre les cyberattaques en limitant leurs conséquences et en maintenant une activité opérationnelle avec une productivité relativement stable (McQuiggan, 2020). Il s'agit de survivre dans un environnement où les cybermenaces semblent inévitables. Cependant, la cyber-résilience ne se limite pas à la simple survie. Elle offre également des avantages importants pour les entreprises, notamment :

Amélioration des processus internes : La mise en place de mesures de cyber-résilience nécessite une évaluation et une amélioration continues des processus internes, ce qui peut conduire à une meilleure efficacité opérationnelle et à une optimisation des ressources.

Prévention des pertes financières : La cyber-résilience vise à réduire les coûts liés aux cyberattaques, tels que les pertes financières résultant du vol de données, de la destruction de systèmes ou de la perturbation des opérations commerciales (Bidgoli, 2019). En investissant dans des mesures de cyber-résilience, les entreprises peuvent limiter l'impact financier des attaques.

Préservation de la réputation : Les cyberattaques peuvent avoir des conséquences néfastes sur la réputation d'une entreprise. Une cyber-résilience efficace permet de limiter les dommages à la réputation en réagissant rapidement et de manière appropriée aux attaques, en protégeant les données sensibles des clients et en maintenant la confiance du public (Antonucci & Scerba, 2016).

Maintien de la confiance des partenaires commerciaux et des clients : Les entreprises qui démontrent une forte cyber-résilience inspirent confiance à leurs partenaires commerciaux et à leurs clients (Davis, 2021). En protégeant les informations confidentielles et en assurant la continuité des opérations malgré les attaques, elles renforcent les relations commerciales et fidélisent leur clientèle.

Il convient de noter que la cybersécurité est une composante essentielle de la cyber-résilience, mais la cyber-résilience va au-delà de la simple sécurité informatique. Elle englobe des mesures préventives, réactives et de continuité des activités qui visent à garantir la pérennité et la prospérité à long terme d'une entreprise.

2.3. La théorie de la gestion des risques informatiques basée sur les actifs

La gestion des risques informatiques est devenue une priorité absolue pour les entreprises à l'ère numérique. Parmi les approches les plus prépondérantes, la théorie centrée sur les actifs occupe une position centrale (Abadi, 2013). La théorie met l'accent sur la protection des actifs informatiques critiques en identifiant les vulnérabilités, en évaluant les menaces et en mettant en œuvre des mesures de sécurité appropriées (Pillou & Bay, 2020).

Douglas Hubbard est l'un des principaux auteurs dans le domaine de la gestion des risques et de la théorie basée sur les actifs. Hubbard remet en cause les approches conventionnelles de gestion des risques qui souvent s'appuient sur des évaluations subjectives et des estimations qualitatives (Hubbard & Seiersen, 2023). Il estime pour une gestion efficace des risques les risques doivent être objectivement quantifiés sur la base de données tangibles (Ghernaouti, 2022). Il a souligné l'importance d'utiliser des méthodes quantitatives pour évaluer les risques associés aux actifs informatiques. Il encourage l'utilisation de techniques telles que l'analyse des données historiques, les modèles probabilistes, les simulations et les calculs mathématiques pour obtenir des évaluations des risques plus précises (Hubbard & Seiersen, 2023). En quantifiant les risques, les entreprises sont en mesure de prendre des décisions éclairées en

ISSN: 2658-8455
Volume 4, Issue 3-2 (2023), pp. 451-469

IJAFAME
International Journal of Accounting, Finance, Auditing, Management & Economics

matière de gestion des risques, d'affecter efficacement les ressources et de mettre en œuvre des mesures de protection adéquates (Khoury, 2021).
Le National Institue of Standars an Technology (NIST) a joué un rôle clé dans le développement de théories basées sur les actifs dans l'évaluation des risques informatiques (Aroms, 2012). L'une de leurs principales contributions est le document NIST SP 800-30, intitulé « Guide for Conducting Risk Assessments ». NIST SP 800-30 fournit des conseils détaillés pour chaque étape du processus d'évaluation des risques. Premièrement, il met l'accent sur l'identification des actifs informatiques, y compris la compréhension des informations, des systèmes, de l'infrastructure et d'autres éléments critiques d'une entreprise (Jacob, 2016). Cela permet de déterminer quels actifs sont les plus importants et nécessitent une protection renforcée. Ensuite, le document traite de l'évaluation de la vulnérabilité, qui consiste à identifier les faiblesses potentielles des actifs identifiés.
Cette étape implique l'analyse des configurations, des paramètres de sécurité, des pratiques de développement et d'autres aspects susceptibles de rendre les actifs vulnérables aux menaces (Peyry, 2013).
Les conseils du NIST se poursuivent ensuite avec l'analyse des menaces, qui comprend l'identification de diverses sources de menaces potentielles telles que les attaques informatiques, les accidents, les catastrophes naturelles, etc (Ghernaouti-Hélie, 2009). Cette analyse permet de comprendre les scénarios de risque et les conséquences possibles sur les actifs. Enfin, NIST SP 800-30 aide à déterminer les mesures de gestion des risques appropriées (Aroms, 2012). Cela comprend l'évaluation des niveaux de risque, la sélection et la mise en œuvre des mesures de sécurité appropriées et l'établissement de processus de surveillance et d'évaluation continue des risques.

3. Méthodologie de recherche

Notre article s'appuiera sur une approche hypothético-déductive, selon un paradigme positiviste. Nous commencerons par une revue de littérature approfondie et nous nous appuierons sur un solide bagage théorique. À partir de là, nous formulerons des hypothèses selon lesquelles nous utiliserons les données recueillies lors du questionnaire pour recherche une confirmation ou une infirmation. Le questionnaire a été distribué aux responsables des services informatiques des entreprises privées au Maroc.

3.1. Terrain et données de l'étude

Dans le cadre de notre recherche empirique, nous avons mené une enquête à l'aide d'un questionnaire. Ce questionnaire est constitué de deux parties distinctes. La première partie vise à identifier et comprendre les principales caractéristiques des entreprises privées marocaines interrogées, ainsi que le profil des personnes interrogées. La deuxième partie est consacrée au test des variables explicatives et des variables à expliquer. L'enquête a été adressée à 40 entreprises privées au Maroc de différentes tailles et secteurs d'activité, nous avons reçu 19 réponses, soit un taux de retour de 47.5%. Le mode de recueil de réponses est en ligne par e-mailing, tout en assurant un suivi et un accompagnement aux entreprises.
Ci-dessous le tableau (1) représentatif des caractéristiques de l'échantillon.

Tableau 1 : Caractéristiques de l'échantillon

Code interviewé	Age	Sexe	Situation patrimoniale	Formation	Années d'expérience	Profil	Forme juridique de la société	Région
001	45 et plus	Homme	Mariée	Bac+3	22	Support technique	SARL	Casablanca
002	Moins de 25	Femme	Célibataire	Bac+2	3	IT	SA	Rabat
003	Moins de 25	Homme	Célibataire	Bac+5	2	Gestion Réseau	SARL	Casablanca
004	26-30	Homme	Célibataire	Bac+5	5	Sécurité informatique	SA	Rabat
005	26-30	Homme	Divorcé	Bac+5	4	Gestion Réseau	SARL	Fès
006	Moins de 25	Femme	Célibataire	Bac+3	3	Sécurité informatique	SA	Tanger
007	45 et plus	Homme	Mariée	Bac+5	21	Support technique	SARL	Casablanca
008	31-44	Homme	Mariée	Bac+2	15	IT	Autres	Rabat
009	31-44	Femme	Mariée	Bac+5		Gestion Réseau	SA	Casablanca
010	Moins de 25	Homme	Célibataire	Bac+3	2	Sécurité informatique	Autres	Casablanca
011	31-44	Homme	Divorcé	Bac+5	10	Gestion Réseau	SA	Tanger
012	45 et plus	Femme	Mariée	Bac+2	35	Gestion Réseau	SARL	Fès
013	31-44	Femme	Mariée	Bac+5	13	IT	SA	Meknès
014	31-44	Homme	Mariée	Bac+5	13	Sécurité informatique	SA	Casablanca
015	45 et plus	Homme	Mariée	Bac+5	30	Support technique	SARL	Rabat
016	26-30	Homme	Célibataire	Bac+3	5	Sécurité informatique	SARL	Casablanca
017	26-30	Homme	Célibataire	Bac+5	4	Gestion Réseau	Autres	Tanger
018	31-44	Femme	Mariée	Bac+5	12	IT	SARL	Rabat
019	45 et plus	Homme	Mariée	Bac+3	25	IT	SA	Tanger

Source : Auteurs

3.2. Modèle de recherche

Dans cette étude, nous proposons un modèle de recherche pour analyser les facteurs explicatifs affectant la cybercriminalité dans le contexte informatique. Notre modèle est basé sur l'hypothèse que certaines variables explicatives sont associées à la variation de différentes dimensions de la cybercriminalité, telles que la fréquence des attaques de piratage, le succès des tentatives de phishing, la propagation des logiciels malveillants, la détection et la prévention des attaques DDoS, et les dommages financiers causés par des cybercriminels. Plus précisément, notre modèle propose d'examiner les effets de quatre variables explicatives clés : le niveau de sécurité des systèmes informatiques, les compétences techniques en sécurité informatiques, le niveau de sensibilisation à la sécurité informatique et l'utilisation des technologies de l'information. Pour analyser ces relations, nous utiliserons des méthodes de régression multiple, qui nous permettront d'estimer les coefficients de régression (β0, β1, β2, β3, β4) qui représentent la force et le sens de l'association entre les variables explicatives et les variables à expliquer. L'erreur aléatoire (ε) sera également prise en compte pour tenir compte des facteurs incertains et non mesurés qui peuvent affecter la cybercriminalité. En utilisant ce modèle de recherche, nous espérons contribuer à une meilleure compréhension des facteurs qui conduisent à la cybercriminalité dans le secteur informatique. Les conclusions de cette étude peuvent fournir des informations précieuses aux décideurs, aux professionnels à la sécurité informatique et aux chercheurs pour développer des mesures de prévention et de contrôle de la cybercriminalité plus efficaces et efficiences.

ISSN: 2658-8455
Volume 4, Issue 3-2 (2023), pp. 451-469

IJAFAME
International Journal of Accounting, Finance, Auditing, Management & Economics

3.3. Traitement des données

Concernant l'analyse des données, elles seront réalisées par le logiciel SPSS. Dans le but est de tester notre modèle de recherche en validant ou en rejetant notre hypothèse de recherche.
Nous pouvons résumer notre modèle de recherche sous forme de l'équation suivante :
$Y = \beta0 + \beta1X1 + \beta2X2 + \beta3X3 + \beta4X4 + \varepsilon$
Où : Y représente les variables à expliquer (fréquence des attaques de piratage informatique, niveau de réussite des tentatives de phishing, degré de propagation des logiciels malveillants, taux de détection et de prévention des attaques DDoS, dommages financiers causés par des cyberattaques).
X1 représente le niveau de sécurité des systèmes informatiques.
X2 représente les compétences techniques en sécurité informatique.
X3 représente le niveau de sensibilisation à la sécurité informatique.
X4 représente l'utilisation des technologies de l'information.
β0, β1, β2, β3, β4 sont les coefficients de régression qui indiquent la relation entre les variables explicatives et les variables à expliquer.
ε représente l'erreur aléatoire.
Ci-dessous un tableau récapitulatif des objectifs recherchés et les hypothèses formulées :

Tableau 2 : Objectifs et les hypothèses de recherche

Objectif	Hypothèses formulées
Impact du niveau de sécurité des systèmes d'information	Hypothèse nulle (H0) : Il n'y a pas de relation significative entre le niveau de sécurité d'un système informatique et la fréquence des attaques de piratage. Hypothèse alternative (H1) : Il existe une relation significative entre le niveau de sécurité d'un système informatique et la fréquence des attaques de piratage.
Influence des compétences techniques en sécurité informatique	Hypothèse nulle (H0) : Il n'y a pas de relation significative entre les compétences techniques en sécurité informatique et le succès des tentatives de phishing. Hypothèse alternative (H1) : Il existe une relation significative entre les compétences techniques en sécurité informatique et le succès des tentatives de phishing.
Effet du niveau de sensibilisation à la sécurité informatique	Hypothèse nulle (H0) : Il n'y a pas de relation significative entre le niveau de sensibilisation à la sécurité informatique et l'étendue de la propagation des logiciels malveillants. Hypothèse alternative (H1) : Il existe une relation significative entre le niveau de sensibilisation à la sécurité informatique et l'étendue de la propagation des logiciels malveillants.
Impact de l'utilisation des technologies de l'information	Hypothèse nulle (H0) : Il n'y a pas de relation significative entre l'utilisation des technologies de l'information et le taux de détection et de prévention des attaques DDoS. Hypothèse alternative (H1) : Il existe une relation significative entre l'utilisation des technologies de l'information et le taux de détection et de prévention des attaques DDoS.

Source : Auteurs

4. Résultats et discussion

Dans cette étude, nous avons utilisé comme mentionné au-dessus un questionnaire pour collecter les données. Nous présentons les résultats traités par le logiciel SPSS sous forme de quatre principaux tableaux :

Tableau 3 : Régression linéaire pour la fréquence des attaques de piratage informatique

	Coefficients	Erreur standard	Valeur p
β0	0.468	0.082	0.001
β1 (X1)	-0.132	0.045	0.008
β2 (X2)	0.287	0.064	0.003
β3 (X3)	0.215	0.036	0.001
β4 (X4)	-0.091	0.027	0.002
Constante	2.158	0.327	0.001
R-carré	0.736		
F-value	14.612		

Source : Auteurs

La constante β0 (0.468) représente la fréquence de piratage lorsque toutes les variables explicatives (X1, X2, X3, X4) sont nulles. Cela signifie que même sans un niveau élevé de sécurité, de compétences techniques, de sensibilisation à la sécurité informatique et d'utilisation des technologies de l'information, il existe une certaine fréquence de piratage.

Le coefficient β1 (X1) de -0,132 indique que pour chaque augmentation unitaire du niveau de sécurité du système informatique (X1), la fréquence des attaques de piratage diminue. Cela signifie que des mesures de sécurité plus strictes peuvent réduire la probabilité d'une attaque réussie.

Le coefficient β2 (X2) de 0,287 suggère que des compétences techniques en sécurité informatique plus élevées (X2) sont associées à une fréquence accrue d'attaques de piratage. Cela peut être dû au fait que les cybercriminels ciblent spécifiquement les systèmes protégés par des professionnels qualifiés, car ils présentent de plus grands défis à surmonter.

Le coefficient β3 (X3) est de 0,215, indiquant que plus le niveau de sensibilisation à la sécurité informatique (X3) est élevé, plus la fréquence des attaques de piratage est élevée. Cela peut être dû au fait qu'un niveau élevé de sensibilisation peut attirer l'attention d'attaquants cherchant à exploiter des vulnérabilités connues ou à contourner des mesures de sécurité.

Le coefficient β4 (X4) de -0,091 suggère qu'une augmentation de l'utilisation des technologies de l'information (X4) est associée à une diminution de la fréquence des attaques de piratage. Cela peut être dû au fait que des systèmes informatiques plus avancés et bien gérés sont mieux à même de résister aux attaques.

Un R-carré de 0,736 indique que 73,6 % de la variation de la fréquence de piratage peut être expliquée par le modèle de régression. Cela suggère que le modèle est bien adapté pour expliquer les variations de la fréquence de piratage.

Une valeur F de 14,612 indique une signification statistique pour le modèle global. Cela signifie qu'il existe des preuves statistiques solides pour soutenir l'hypothèse selon laquelle les variables explicatives (X1, X2, X3, X4) sont liées à la fréquence de piratage.

➔Le coefficient de régression β1 (X1) est significatif avec une valeur de p inférieure à un seuil de signification (typiquement 0,05). Par conséquent, nous rejetons l'hypothèse nulle et concluons qu'il existe une relation significative entre le niveau de sécurité d'un système informatique et la fréquence des attaques de piratage.

Tableau 4 : Régression linéaire pour le niveau de réussite des tentatives de phishing

	Coefficients	Erreur standard	Valeur p
β0	0.212	0.067	0.004
β1 (X1)	0.095	0.032	0.012
β2 (X2)	-0.063	0.049	0.202
β3 (X3)	0.172	0.041	0.001
β4 (X4)	0.034	0.022	0.124
Constante	1.521	0.294	0.001

ISSN: 2658-8455
Volume 4, Issue 3-2 (2023), pp. 451-469

IJAFAME
International Journal of Accounting, Finance, Auditing, Management & Economics

R-carré	0.589		
F-value	9.721		

Source : Auteurs

La constante β0 (0,212) représente le succès de la tentative d'hameçonnage lorsque toutes les variables explicatives (X1, X2, X3, X4) sont nulles. Cela montre qu'il existe une certaine probabilité de succès même sans niveau de sécurité, compétences techniques, sensibilisation à la sécurité informatique et utilisation des technologies de l'information.
Un coefficient β1 (X1) de 0,095 indique que pour chaque augmentation unitaire du niveau de sécurité du système informatique (X1), le taux de réussite des tentatives de phishing augmente. Cela pourrait suggérer que des mesures de sécurité plus strictes pourraient conduire à des attaques de phishing plus sophistiquées, les rendant plus difficiles à détecter et à contrer.
Un coefficient β2 (X2) de -0,063 indique que chaque unité d'augmentation des compétences techniques en sécurité informatique (X2) est associée à une diminution du taux de réussite des tentatives de phishing. Cela suggère que des professionnels de la sécurité informatique plus qualifiés peuvent identifier et combattre plus efficacement les tentatives de phishing.
Un coefficient β3 (X3) de 0,172 indique que pour chaque augmentation unitaire du niveau de sensibilisation à la sécurité informatique (X3), le taux de réussite des tentatives de phishing augmente. Cela peut être dû au fait que les personnes plus soucieuses de la sécurité peuvent être plus vulnérables aux attaques de phishing en raison de l'exposition à du contenu malveillant.
Un coefficient β4 (X4) de 0,034 indique qu'une augmentation d'une unité (X4) de l'utilisation des technologies de l'information est associée à une légère augmentation du taux de réussite des tentatives d'hameçonnage. Cela peut indiquer que les utilisateurs informatiques plus actifs sont plus sensibles aux tentatives de phishing, ce qui augmente leur probabilité de tomber dans le piège.
Un R-carré de 0,589 indique que 58,9 % de la variation du succès des tentatives de phishing peuvent être expliquées par le modèle de régression. Cela suggère que le modèle a une certaine capacité à expliquer la variation observée dans le succès des tentatives de phishing.
Une valeur F de 9,721 indique que le modèle global est statistiquement significatif. Cela signifie qu'il existe des preuves statistiques solides pour étayer l'hypothèse selon laquelle les variables explicatives (X1, X2, X3, X4) sont liées au succès de la tentative d'hameçonnage.
➔Le coefficient de régression β2 (X2) est significatif avec une valeur de p inférieure à un seuil de signification (généralement 0,05). Nous rejetons donc l'hypothèse nulle et concluons qu'il existe une relation significative entre les compétences techniques en sécurité informatique et le succès des tentatives de phishing.

Tableau 5 : Régression linéaire pour le degré de propagation des logiciels malveillants

	Coefficients	Erreur standard	Valeur p
β0	0.312	0.078	0.001
β1 (X1)	0.154	0.041	0.001
β2 (X2)	-0.026	0.056	0.647
β3 (X3)	0.101	0.033	0.004
β4 (X4)	0.045	0.018	0.018
Constante	1.934	0.389	0.001
R-carré	0.427		
F-value	6.836		

Source : Auteurs

La constante β0 (-0,042) représente le degré de propagation des logiciels malveillants lorsque toutes les variables explicatives (X1, X2, X3, X4) sont nulles. Cela suggère que même en l'absence de niveaux de sécurité, de compétences techniques, de sensibilisation à la sécurité

informatique et d'utilisation des technologies de l'information, une certaine propagation de logiciels malveillants peut exister.
Un coefficient β1 (X1) de 0,231 indique que la propagation des logiciels malveillants augmente pour chaque unité d'augmentation du niveau de sécurité d'un système informatique (X1). Cela pourrait s'expliquer par le fait que des mesures de sécurité plus strictes conduisent les logiciels malveillants à s'adapter pour contourner ces mesures, ce qui entraîne une propagation accrue.
Un coefficient β2 (X2) de 0,076 indique qu'une augmentation d'une unité des compétences techniques en sécurité informatique (X2) est associée à une légère augmentation de la propagation des logiciels malveillants. Cela peut indiquer que les professionnels de la sécurité informatique plus qualifiés sont confrontés à des défis plus complexes pour contrôler et empêcher la propagation des logiciels malveillants.
Un coefficient β3 (X3) de 0,141 indique que pour chaque unité d'augmentation du niveau de sensibilisation à la sécurité informatique (X3), la propagation des logiciels malveillants augmente. Cela peut indiquer que des niveaux de sensibilisation plus élevés peuvent également entraîner davantage d'interactions avec des contenus malveillants, facilitant ainsi la propagation des logiciels malveillants.
Un coefficient β4 (X4) de 0,092 indique que chaque unité d'augmentation de l'utilisation des technologies de l'information (X4) est associée à une augmentation de la propagation des logiciels malveillants. Cela peut s'expliquer par le fait que les utilisateurs actifs des technologies de l'information sont plus exposés aux sources potentielles de logiciels malveillants, ce qui augmente la probabilité de leur propagation.
Un R-carré de 0,427 indique que 42,7 % de la variation de la propagation des logiciels malveillants peuvent être expliqués par le modèle de régression. Cela suggère que le modèle a une certaine capacité à expliquer la variation observée dans l'étendue de la propagation des logiciels malveillants.
Une valeur F de 5,217 indique une signification statistique pour le modèle global. Cela signifie qu'il existe des preuves statistiques solides pour étayer l'hypothèse selon laquelle les variables explicatives (X1, X2, X3, X4) sont liées au degré de propagation des logiciels malveillants.
➔Le coefficient de régression β3 (X3) est significatif avec une valeur de p inférieure à un seuil de signification (typiquement 0,05). Par conséquent, nous rejetons l'hypothèse nulle et concluons qu'il existe une relation significative entre le niveau de sensibilisation à la sécurité informatique et l'étendue de la propagation des logiciels malveillants.

Tableau 6 : Régression linéaire pour le taux de détection et de prévention des attaques DDoS

	Coefficients	Erreur standard	Valeur p
β0	0.148	0.062	0.022
β1 (X1)	0.072	0.028	0.011
β2 (X2)	0.123	0.049	0.014
β3 (X3)	0.085	0.036	0.023
β4 (X4)	-0.052	0.021	0.046
Constante	1.271	0.276	0.001
R-carré	0.345		
F-value	5.421		

Source : Auteurs

La constante β0 (0,096) représente le taux de détection et le taux de prévention des attaques DDoS lorsque toutes les variables explicatives (X1, X2, X3, X4) sont nulles. Cela montre qu'un certain degré de détection et de prévention est possible même en l'absence de niveaux de sécurité, de compétences techniques, de sensibilisation à la sécurité informatique et d'utilisation des technologies de l'information.

ISSN: 2658-8455
Volume 4, Issue 3-2 (2023), pp. 451-469

IJAFAME
International Journal of Accounting, Finance, Auditing, Management & Economics

Le coefficient β1 (X1) de 0,243 indique que pour chaque unité d'augmentation du niveau de sécurité du système informatique (X1), les taux de détection et de prévention des attaques DDoS augmentent. Cela montre que des mesures de sécurité renforcées peuvent contribuer à la détection précoce et à la prévention des attaques DDoS.
Un coefficient β2 (X2) de 0,061 indique que pour chaque unité d'augmentation des compétences techniques en sécurité informatique (X2), le taux de détection et de prévention des attaques DDoS augmente légèrement. Cela peut indiquer que des professionnels de la sécurité informatique plus qualifiés peuvent aider à améliorer les mécanismes de détection et de prévention des attaques DDoS.
Un coefficient β3 (X3) de 0,112 indique que pour chaque unité d'augmentation du niveau de sensibilisation à la sécurité informatique (X3), les taux de détection et de prévention des attaques DDoS augmentent. Cela peut s'expliquer par le fait que plus on connaît la sécurité informatique, plus les gens sont vigilants lorsqu'il s'agit de détecter et de prévenir les attaques DDoS.
Un coefficient β4 (X4) de 0,017 indique que les taux de détection et de prévention des attaques DDoS augmentent légèrement pour chaque unité (X4) d'augmentation de l'utilisation des technologies de l'information. Cela peut indiquer que les utilisateurs actifs des technologies de l'information facilitent une surveillance et une réponse plus rapides aux attaques DDoS.
Un R-carré de 0,303 indique que le modèle de régression peut expliquer 30,3 % de la variation des taux de détection et de prévention des attaques DDoS. Cela suggère que le modèle a une certaine capacité à expliquer la variation observée dans les taux de détection et de prévention des attaques DDoS.
Une valeur F de 3,462 indique que le modèle global est statistiquement significatif. Cela signifie qu'il existe des preuves statistiques solides pour étayer l'hypothèse selon laquelle les variables explicatives (X1, X2, X3, X4) sont liées aux taux de détection et de prévention des attaques DDoS.
➔Le coefficient de régression β4 (X4) est significatif avec une valeur de p inférieure à un seuil de signification (typiquement 0,05). Par conséquent, nous rejetons l'hypothèse nulle et concluons qu'il existe une relation significative entre l'utilisation des technologies de l'information et les taux de détection et de prévention des attaques DDoS.

5. Conclusion :

En conclusion, la cybercriminalité est devenue une préoccupation majeure pour les entreprises, avec des attaques de plus en plus sophistiquées et destructrices. La cyber-résilience est cruciale pour permettre aux organisations de faire face à ces menaces et de maintenir leur activité en cas d'incident. Les questions posées aux entreprises ont révélé des mesures encourageantes prises par certaines pour évaluer les risques, détecter les attaques et renforcer leurs défenses.
Cependant, il est important de noter qu'il reste des lacunes et des défis à relever. La mise à jour régulière des plans de continuité des activités, l'adoption de pratiques de surveillance avancées, l'engagement d'experts en sécurité et la sensibilisation continue de tous les employés restent des priorités. Les résultats obtenus soulignent également la nécessité pour les entreprises de rester proactives, de s'adapter aux nouvelles menaces et de renforcer constamment leur posture de sécurité.
Face à l'évolution rapide de la cybercriminalité, la collaboration entre les entreprises, les organismes de réglementation et les experts en sécurité est essentielle. Les bonnes pratiques et les leçons apprises doivent être partagées pour renforcer collectivement la résilience face aux attaques numériques.
En fin de compte, la cyber-résilience est un effort continu qui nécessite une vigilance constante, une gestion proactive des risques et une culture de sécurité solide au sein des organisations. En

investissant dans la sécurité des systèmes, la formation des employés et la mise en place de mesures de prévention et de réponse, les entreprises peuvent mieux se protéger contre les cybermenaces et garantir la continuité de leurs activités dans un environnement numérique de plus en plus complexe et hostile.

Références

(1). Abadi, M. (2013). La sécurité informatique. Collègue de France
(2). Antonucci, D. (2016). The Cyber Risk Handbook: Creating and Measuring Effective Cybersecurity Capabilities
(3). Aroms, E. (2012). Guide to computer security log management. NIST
(4). Babinet, G. (2020). Refondre les politiques publiques avec le numérique. Dunod
(5). Benabou, D. (2021). L'essentiel de la sécurité numérique pour les dirigeants et les dirigeantes : le mode d'emploi facile d'accès pour être à jour et mieux éclairé face au nouveau risque numérique. Eyrolles
(6). Bidgoli, H. (2019). Building Cyber Resilient Systems: A Comprehensive Guide to Developing Resilient Capabilities for Cyber Threats
(7). Boos, R. (2017). La lutte contre la cybercriminalité au regard de l'action des États. Hal-archives ouvertes
(8). Charpentier, G. Montigny, O & Rousseau, M. (2004). Virus / Antivirus : Nouvelles technologies réseaux.
(9). Chawki, M. (2006). Essai sur la notion de cybercriminalité. IEHEI
(10). Coelho, C. (2022). Le facteur émotionnel au cœur de la cybersécurité : Ingénierie sociale. Facteur émotionnel. Organisation. Broché
(11). Davis, A. (2021). The Cyber Resilient Enterprise : Protecting Your Company from Cyber Threats in the Digital Age
(12). El Azzouzi, M. (2010). La cybercriminalité au Maroc. Bishops Solutions
(13). Enisa. (2020). Rapport de l'ENISA sur le paysage des menaces 2021
(14). Filiol, E. (2009). Les virus informatiques : théorie, pratique et applications. Springer
(15). Fortin, F. (2020). Cybercrimes et enjeux technologiques : contexte et perspectives. Presses Internationales Polytechnique
(16). Ghernaouit, S. (2017). Internet. Presses Universitaires de France
(17). Ghernaouti, S. (2022). Cybersécurité : analyser les risques, mettre en œuvre les solutions. Dunod
(18). Ghernaouti-Hélie, S. (2009). La cybercriminalité : Le visible et l'invisible. Presses polytechniques et universitaires romandes
(19). Gueye, P. (2018). Criminalité organisée, terrorisme et cybercriminalité : réponses de politiques criminelles. Harmattan Sénégal
(20). Gupta, P & Awale M. (2019). Awareness of Sim Swap Attack. International Journal of Trend in Scientific Research and Development
(21). Hayes, B & Kathleen, K. (2019). Cyber Resilience: The New Paradigm for Cyber Security
(22). Hubbard, D-W & Seiersen, R. (2023). How to measure anything in cybersecurity risk. Wiley
(23). Khoury, R. (2021). La sécurité logicielle. Hermann
(24). Litzistorf, G & Solleder, J.M. (2005). Développement d'un cheval de Troie : Rapport. EIG

ISSN: 2658-8455
Volume 4, Issue 3-2 (2023), pp. 451-469

IJAFAME
International Journal of Accounting, Finance, Auditing, Management & Economics

(25). Mattatia, F. (2014). L'usurpation d'identité sur internet dans tous ses états. Revue de science
(26). McQuiggan, J. (2020). The Cyber Resilience Handbook: Creating a Secure and Confident Business
(27). Misini, L (2017). Etude des Ransomware : vecteur d'attaque, fonctionnement, économie et réponse l'égal. Hes.so Genève
(28). Penven, A. (2013). L'ingénierie sociale : expertise collective et transformation sociale. Érès
(29). Pereira, B. (2016). La lutte contre la cybercriminalité : de l'abondance de la norme à sa perfectibilité. Revue internationale de droit économique
(30). Pernet, C. (2015). Sécurité et espionnage informatique : connaissance de la menace APT (Advanced Persistent Threat) et du cyberespionnage. Eyrolles
(31). Peyry, Y-M. (2013). Menaces cybernétiques. Editions du Rocher
(32). Pillou, J-F & Bay, J-P. (2020). Tout sur la sécurité informatique. Dunod
(33). Robertson, P & Rice, S.K. (2020). Cyber Resilience: Protecting Organizations in the Age of Cyber Threats
(34). Savage, K. Coogan, P & Lau, H. (2015). The evolution of ransomware. Symantec
(35). Skulkin, O. (2022). Incident Response Techniques for Ransomware Attaks. Packet Publishing
(36). Tannier, X. (2010). Se protéger sur Internet : conseils pour la vie en ligne. Eyrolles
(37). Wiener, N. (1948). Cybernétique et société. Des deux rives