Méthodologie

Cette étude repose sur des entrevues qualitatives semi-dirigées pour saisir l'expérience des professionnels de la cybersécurité qui font face régulièrement à des cyberattaques dans le secteur financier. Nous avons interrogé 58 répondants issus de 37 organisations. Une approche d'échantillonnage ciblé a été adoptée pour obtenir une diversité de points de vue et d'expériences à travers cinq dimensions spécifiques (géographie, type d'institution, taille de l'institution, rôle de l'interviewé et expérience de l'interviewé) et pour s'assurer que diverses perspectives du réseau de la cyber-résilience étaient adéquatement représenté. La diversité géographique de l'échantillon tient compte à la fois de la nature mondiale des défis de la cyber-résilience auxquels sont confrontées les institutions financières et des caractéristiques culturelles ou réglementaires locales qui peuvent favoriser des pratiques nationales différentes. Les répondants ont été interrogés au Canada, aux États-Unis, au Royaume-Uni, aux Pays-Bas et en France. Certaines organisations avaient une vaste présence internationale, opérant sur des dizaines de marchés, tandis que d'autres maintenaient une empreinte locale. La taille des institutions pour lesquelles les personnes interrogées travaillaient variait également de manière significative - certaines d'entre elles avaient un chiffre d'affaires annuel inférieur à un milliard de dollars US, tandis que les bénéfices d'autres pouvaient atteindre cinq à dix fois ce montant - ce qui entraîne des niveaux variables de ressources et d'expertise disponibles pour mettre en œuvre des pratiques de cyber-résilience. Le secteur financier fournit divers services à des clients particuliers et commerciaux. Pour en tenir compte, l'échantillon comprenait des professionnels de la cybersécurité qui travaillent pour des banques, des compagnies d'assurance, des fonds de pension et des places de marchés. Les sociétés de conseil et de réponse aux incidents qui fournissent des services de cybersécurité aux entreprises financières et les régulateurs qui supervisent leurs activités ont également été interrogés. Les postes occupés par les personnes interrogées incluaient des directeurs de la sécurité de l'information (CISO), des directeurs des risques (CRO), des directeurs de centres d'opérations de sécurité (SOC), des équipes d'intervention en cas d'incident (CSIRT) et des unités de continuité des activités, en passant par des responsables d'équipes de tests de pénétration et des *red teams*, ainsi que des conseillers en gouvernance et en sécurité informatiques. L'expérience professionnelle dans un rôle de gestion ou de réglementation des cyber-risques allait d'une demi-année à plus de trente ans. Le tableau 1 donne un aperçu des caractéristiques socio-démographiques et professionnelles des répondants.

Les entretiens ont été réalisés entre août 2018 et novembre 2020 en personne (36), par appel téléphonique ou vidéoconférence (21), ou par courriel (1). Treize répondants (22 %) étaient des femmes. Les entretiens ont duré 57 minutes en moyenne (fourchette : de 31 à 90 minutes). Ils ont été enregistrés et transcrits en vue d'une analyse qualitative, à l'exception de trois entretiens dans des lieux publics (café ou restaurant) où le niveau sonore était trop élevé pour permettre l'enregistrement, et où des notes manuscrites ont été prises à la place. Les entretiens transcrits ont ensuite été importés dans NVivo 12 de QSR International, un logiciel d'analyse qualitative qui facilite l'exploration, le codage et la visualisation de grandes quantités de données non structurées.

Tous les entretiens ont suivi un scénario similaire : les répondants devaient d'abord expliquer comment ils définissaient la cyber-résilience, puis se souvenir de la cyber-attaque la plus grave qu'ils avaient subie. Ces questions ont été posées au début de l'entretien afin de susciter des souvenirs spécifiques et concrets d'événements perturbateurs uniques à l'organisation du participant et de la manière dont ces événements ont été gérés. Un objectif indirect était de minimiser le recours des participants à des déclarations génériques ou à des cas très médiatisés, réponses qui sont souvent utilisées pour détourner les questions portant sur un sujet sensible ou pour lequel l'organisation n'a pas de réponse. Le script de l'entretien comprenait ensuite des questions sur les technologies et les procédures (y compris les normes) utilisées pour favoriser la cyber-résilience, le rôle joué par les partenariats public-privé et l'expertise externe, les obstacles organisationnels à la cyber-résilience, l'impact du facteur humain sur la cyber-résilience et les aspects réglementaires de la cyber-résilience. Une dernière question ouverte permettait aux répondants de signaler tout thème qui, selon eux, avait été négligé.

Tableau 1. Statistiques descriptives des répondants

Pays	**Nombre de répondants**	**Pourcentages**
Canada	32	55%
Royaume-Uni	2	3.5%
États-Unis	4	7%
France	14	24%
Pays-Bas	6	10.5 %
Total	58	100%
Organisation		
Institution financière	36	62%
Autorité régulatrice	8	14%
Entreprise de réponse aux incidents	9	16%
Gouvernement	5	8%
Total	58	100%
Genre		
Femme	13	22%
Homme	45	78%
Autre	0	0%
Total	58	100%
Années d'expérience (dans l'organisation actuelle)		
Moyenne	11,4 ans	
Médiane	11 ans	
Éventail	0.5 – 31 ans	