AVANT-PROPOS

« En ne vous préparant pas,
vous vous préparez à échouer. »

Benjamin Franklin

PAR SÉBASTIEN

Quand je suis arrivé dans la cybersécurité en 2017, je craignais de tomber dans un monde extrêmement technique. Et croyez-moi, je n'ai pas été déçu ! Des acronymes en tout genre, des personnes avec des styles capillaires et vestimentaires particuliers, des impératifs technologiques venant parfois ralentir les habitudes de l'informatique… Bref, tout un monde parallèle.

Et pourtant assez vite, au contact de mes confrères, partenaires et clients en Europe comme aux États-Unis, j'ai pu confirmer l'intuition que ce monde était bien le repaire d'experts pointus dans leur domaine et rares sur le marché, mais qu'une fine frange des activités à y mener relevait nettement plus du cadre de la communication et du leadership. C'est donc avec ce prisme, en particulier au niveau de la direction cybersécurité, que j'ai pu collaborer avec des personnes tout en simplicité, en professionnalisme, et en recherche d'appui auprès du reste de l'organisation que ces mêmes hommes et femmes appelés « CISO » (*Chief Information Security Officer*) ou « RSSI » (responsable de la sécurité des systèmes d'information) sont là pour protéger.

Tous ces responsables, ou presque, me font part d'une quasi-souffrance dans le manque de ressources financières et humaines pour faire correctement face à la vague de menaces pesant sur eux. Tous ces responsables me confient également leur vécu, voire leur frustration, dans leur tentative de mobiliser efficacement le reste de l'organisation et de jouer leur rôle de première ligne de défense. Tous ces responsables, enfin, me font remonter un criant besoin de rallier la direction à leur cause, pour que

la cybersécurité devienne un enjeu stratégique et qu'elle sorte de son monde d'experts à la barbe hirsute, aux cheveux rouges et aux sweat-shirts à capuche.

C'est ainsi qu'après un nouveau rôle dans les ventes en cyber, puis en tant que chef d'équipe, j'ai eu une nouvelle fois dans ma carrière l'envie et la possibilité de joindre le personnel au professionnel. Très rapidement, j'ai compris que quand on s'adressait à ceux que dans notre jargon nous appelons « le CISO et au-dessus », mon expérience professionnelle en sûreté et les deux décennies passées à penser, à pratiquer et à enseigner le krav-maga allaient devenir utiles à la mission que je m'étais donnée : aiguiser les réflexes de la direction pour l'aider à répondre efficacement à une situation de crise cyber, et permettre aux RSSI d'avoir son écoute ainsi que les budgets nécessaires à la bonne poursuite de leur activité.

L'objet de cet ouvrage n'est donc pas de proposer une méthode de gestion de crise cyber d'un point de vue informatique, mais de partager les éléments, les observations, les retours d'expérience terrain prouvant qu'aussi douées soient les équipes techniques, si la direction et les collaborateurs ne sont pas parfaitement rodés, alors la réponse opérationnelle sera au mieux improvisée et aléatoire, et au pire catastrophique.

Et sans tomber dans le registre de la peur, mais plutôt en étant conscient de ce qui se passe autour de nous et des motivations sous-jacentes, l'objectif de ce livre est d'éclairer ses lecteurs sur le fait que l'entraînement à la gestion de crise cyber se doit d'être régulier et réaliste pour devenir vraiment performant. Pourquoi préparer toutes les facettes de l'organisation (informatique, cybersécurité, collaborateurs, direction) ? Comment s'entraîner, à quelle fréquence, etc. ? Autant de questions auxquelles ce livre se propose de répondre.

Cet ouvrage est le résultat d'une complicité du premier instant avec mon binôme, mon *partner in crime from Ireland in London*, Stephen Delahunty, rencontré à Boston en 2021. Un humour acéré, des compétences affûtées et un sacré sens de la mise en scène, ce garçon ! C'est

également le résultat d'une idée un peu folle née entre nous à Paris, un soir de décembre 2022 : « Et si on se lançait dans l'écriture d'un ouvrage mêlant nos expériences en préparation à la crise cyber ? » Quelques mois plus tard, en voici le résultat. Bonne lecture !

PAR STEPHEN

Courant 2021, j'ai pris l'avion pour Boston pour rencontrer l'équipe IBM. En tant qu'Irlandais, c'était particulièrement marquant. Boston est la capitale non officielle de la diaspora irlandaise dans le monde et c'était mon premier voyage dans cette ville. Je venais d'être embauché par IBM au sein de l'équipe Cyber Range de la division cybersécurité. Le Cyber Range étant le joyau de la couronne de formation IBM Security pour ses clients, j'étais sur le point de rencontrer des personnes très talentueuses.

La ville et l'équipe ont été à la hauteur du battage médiatique – je n'ai pas été déçu. J'ai reçu un accueil chaleureux des deux. J'ai rencontré mon (désormais) ami et collègue Sébastien Jardin pour la première fois lors de ce voyage et je l'ai vu donner une session de formation sur la crise cyber. Je l'ai tout de suite aimé et j'ai appris que nous étions tous deux en compétition pour le même travail – mais heureusement, IBM a décidé de nous embaucher tous les deux.

IBM essayait de faire quelque chose de nouveau au Cyber Range. L'expérience de formation au combat au corps à corps de Sébastien et mes années dans la création de contenu et la réalisation télévisuelle apporteraient de l'innovation au Cyber Range : nous pourrions approfondir l'immersion dans les scénarios et avoir un plus grand impact chez nos clients. L'offre existait depuis 2016 et dans cette nouvelle réalité post-pandémie, nous avons compris qu'une approche plus agile, dynamique et adaptative de la conception et des formats proposés était nécessaire. Un modèle qui refléterait les réalités opérationnelles auxquelles nos entreprises et organisations étaient confrontées au quotidien, et qui s'affranchirait de la contrainte d'un lieu physique dédié. Sébastien et moi allions travailler en étroite collaboration et j'ai pu constater à quel point nos parcours différents et notre philosophie commune se complétaient à merveille.

Ce serait notre travail, comme nous l'avons vu, de défendre les intérêts des RSSI et des DSI auprès des directions générales du monde entier, mais aussi leur bataille constante contre des pirates informatiques sophistiqués et leur lutte pour obtenir l'adhésion du reste de la direction. « Nous pourrions vous aider avec une simulation de crise efficace, en quelques heures seulement, pour faire de la cybersécurité un impératif métier et transformer vos dirigeants en "Cyber Sponsors" », telle était la promesse que nous leur ferions.

Je souhaite partager une histoire qui, je pense, résume tout cela. Sébastien et moi étions à Paris pour réaliser un exercice de simulation de crise. À la faveur d'un changement de plan de dernière minute, j'allais devoir animer l'exercice avec Sébastien qui, en soutien, dirigerait les opérations en coulisse. Comme à l'accoutumée, la salle bourdonnait d'excitation alors qu'elle se remplissait de cadres d'une chaîne d'hôtels de renommée internationale, confortablement installés dans leur siège. J'étais dans les starting-blocks, prêt à lancer la simulation de crise cyber. Je ne savais pas qu'une question stimulante allait advenir, challengeant non seulement mon expertise mais l'essence même de notre mission ce jour-là. Comme toute personne qui dispense une formation à des dirigeants peut en témoigner, nous avons affaire à des personnes très intelligentes et à de grandes personnalités. Cette session n'allait pas faire exception à la règle.

Mon discours d'ouverture à peine entamé, le PDG, une personne distinguée emplie de confiance, m'a interrompu par une question directe et incisive. « Quel est le but de cet exercice ? » a-t-il demandé, sa voix résonnant dans la pièce. « Ne devrions-nous pas simplement accepter le coût des *ransomwares* comme une dépense opérationnelle et passer à autre chose ? » Sa question était en suspens, nous demandant de justifier les heures et les ressources investies dans la formation. (Il n'est pas rare d'être mis au défi lors de telles simulations. En fait, nous l'encourageons. C'est ainsi que Sébastien et moi restons affûtés et continuons d'apprendre.) Les participants étaient intelligents et avant-gardistes, conscients et aux prises avec les enjeux de l'ère numérique. Le PDG avait

un argument valable : les cyberattaques étaient devenues une réalité inévitable de la vie des entreprises. « Excellente question », ai-je répondu en cherchant le regard du PDG. « Il s'agit de survivre à l'attaque, de ne pas être anéanti. » Mes paroles étaient maintenant suspendues dans les airs, emportant avec elles le poids de l'expérience et de la formation.

Une anecdote personnelle m'est alors revenue à l'esprit et je me suis surpris à raconter la fois où j'avais visité Rio de Janeiro. Mes hôtes, au fait des dangers de la ville, m'avaient prodigué des conseils pour surmonter d'éventuels ennuis : « Voyagez la nuit en voiture, ne portez pas votre belle montre et, surtout, ayez toujours sur vous deux portefeuilles, un pour vous et un pour le voleur. »

« Vous voyez », ai-je poursuivi, « emporter deux portefeuilles vous permet de survivre à une rencontre avec un voleur sans tout perdre, de même que la formation en simulation de crise donne à votre organisation les outils et les stratégies pour survivre à une cyberattaque. » La salle a retrouvé son excitation initiale, alors que le défi du PDG se transformait en acceptation. Il m'a fait un signe de tête et j'ai démarré la simulation. La pièce était animée d'une énergie renouvelée, les esprits se concentrant désormais sur les réalités des cybermenaces et sur la nécessaire résilience qu'elles appellent. L'importance de la survie et de la sauvegarde des personnes et des actifs de l'organisation était maintenant bien identifiée et comprise. Ce nouveau contexte « accidentel » a conduit à une participation pleinement engagée et, à travers les subtilités du scénario, nous avons exploré des stratégies, affiné nos compétences en matière de prise de décision et favorisé une compréhension plus fine de la préparation.

Au fur et à mesure que l'exercice de simulation se déroulait, le PDG et son équipe ont fait face à un déluge de cybermenaces repoussant toujours plus loin les limites de leur courage et de leur résilience. Le PDG a fait montre de son leadership et de son désir de relever ces défis, alors que tous les participants étaient aux prises avec des décisions

complexes, pesant les conséquences potentielles et exécutant des stratégies pour protéger leur organisation.

L'audace du PDG, qui a remis en question l'objectif de la formation de simulation de crise cyber, s'est avérée être un moment charnière qui a donné le ton à l'exercice. Il faisait son travail. Et rétrospectivement, il a rendu à tous les participants un grand service en déclenchant un sentiment d'urgence et de sérieux qui imprégnerait la formation.

En fin de compte, la question provocatrice du PDG est devenue un cadeau, un signal d'alarme pour tout le monde dans la salle, améliorant la compréhension par l'organisation des enjeux impliqués. Il a ainsi donné la mesure, le *la*, faisant de l'exercice de formation un effort essentiel pour protéger à la fois les personnes et les actifs incorporels. Ce moment charnière a propulsé le collectif sur la voie d'une participation active à l'entraînement, garantissant sa capacité à résister aux défis inévitables auxquels il serait confronté à l'avenir.

Cette équipe dirigeante a maintenant compris que résilience cyber et résilience de l'entreprise sont synonymes.

Notre mission a été un succès. Nous avons été réinvités six mois plus tard ; ce fut le début d'une belle histoire avec cette équipe et avec bien d'autres rencontrées au fil des semaines et des déplacements à travers le monde.

INTRODUCTION

« La vérité porte l'évidence en soi.
Dès qu'on la débarrasse des toiles d'araignée
de l'ignorance, elle brille avec éclat. »

GANDHI

Faisons une pause quelques instants dans nos vies organisées, rythmées, pressées pour regarder autour de nous. Là, tout de suite, à l'instant même où vous lisez ces quelques lignes, combien d'objets numériques, voire connectés, vous entourent ? Votre téléphone mobile, votre montre, le thermostat accroché au mur, la box Wi-Fi dont on vous a donné le code à l'hôtel pour vous assurer un débit optimal, peut-être même la cafetière qui émet ce doux sifflement annonciateur d'une boisson chaude et énergisante. Maintenant, projetez-vous à la maison, au bureau, sur vos lignes de production, dans vos laboratoires de recherche, dans votre bloc opératoire, dans l'avion, dans le train… et faites le même exercice. Le digital nous entoure, il est partout et c'est une très bonne chose, car il permet d'améliorer les performances, de réduire l'émission de polluants, d'optimiser l'usage des ressources, de faciliter le quotidien de milliards de personnes dans le monde. Et si l'on en croit les spécialistes du secteur, cette vague numérique est exponentielle.

Mais comme toute innovation depuis que le monde est monde, elle a un côté positif et une face sombre. Rappelons par exemple que Robert Oppenheimer n'avait à l'origine pas imaginé, alors qu'il travaillait sur la fission de l'uranium et du plutonium dans le laboratoire de Los Alamos (Nouveau-Mexique, États-Unis) que sa création pourrait raser des villes entières et générer les pertes humaines que nous connaissons tous.

Voici également ce que nous dit Christophe Vannier, CISO chez Carrefour Banque & Assurance : « L'informatique, selon sa définition académique, est la science du traitement automatique et rationnel de

l'information, considérée comme le support des connaissances et des communications. À l'origine, elle était réservée aux experts en raison de sa complexité. Le monde digital a émergé de cette complexification, grâce à un usage répandu plutôt qu'à une technologie en particulier. Cependant, dès le début, la sécurité des systèmes et des informations qu'ils véhiculent a été prise en compte, en particulier dans des domaines tels que la défense, la finance et l'énergie, où le secret, la résilience et la précision sont cruciaux. La protection contre le vol, la corruption et l'indisponibilité des données faisait partie intégrante des systèmes de traitement depuis le début, ce qui a conduit à des protocoles sécurisés et des centres de calcul protégés.

Aujourd'hui, malgré la simplification apparente due à la digitalisation, les systèmes se sont complexifiés de manière exponentielle. En 1983, Internet comptait seulement 1 000 serveurs connectés, tandis qu'à l'heure actuelle ce chiffre s'élève à des dizaines de milliards, tous fonctionnant sur un protocole par défaut non sécurisé, le TCP/IP (le protocole SSL est né en 1994). En ligne, comme dans la vie réelle, il existe un nombre proportionnellement similaire de personnes malveillantes et de délinquants. L'avantage d'être derrière un clavier est d'être moins exposé, voire anonyme, ce qui peut transformer rapidement un ordinateur connecté en une arme. Par conséquent, l'usage d'un ordinateur nécessite des consignes de sécurité minimales qui devraient être respectées par l'utilisateur honnête.

Depuis plus de 30 ans, on a certes formé des utilisateurs à utiliser les applications (progiciels), mais leur a-t-on vraiment appris à devenir des utilisateurs informatiques (informaticiens) ? Non et c'est tant mieux, car ces derniers sont sans doute les moins réceptifs aux consignes de sécurité. Toute la problématique repose sur l'attitude que l'utilisateur doit ou devrait avoir face aux événements. C'est pour cela que les *wargames* existent : pour entraîner les individus et organes de commandement (de direction) à faire face à une situation imprévue. » Et pourtant… c'est bien ce qu'ont compris les cybercriminels, certains États et groupes d'hacktivistes qui, voyant cette surface d'attaque numérique augmenter d'année en année, avec toujours plus de pression pour livrer des

produits et services rapidement et au meilleur prix, ne cessent de perfectionner leurs actions malveillantes à des fins financières, politiques ou idéologiques.

Aujourd'hui, il ne se passe pas une semaine dans le monde, et notamment en France, sans que la presse ne se fasse l'écho d'une organisation, publique ou privée, ayant fait l'objet d'une cyberattaque. Mais entendons-nous bien, ces articles ne sont que la partie émergée de l'iceberg et ne traitent pas des incidents et autres tentatives d'attaque. Non, ils traitent de crises d'origine cyber venant impacter durement le fonctionnement de l'organisation. Et dans ce domaine, personne n'est à l'abri. Grandes comme petites entreprises, secteur public comme secteur privé. Tout le monde est touché ou, pour reprendre la citation de La Fontaine : « Ils ne mouraient pas tous, mais tous étaient frappés. »

Parfois, les pertes financières sont gigantesques (par exemple, en France, la cyberattaque de 2017 ayant touché Saint-Gobain leur aurait coûté 250 millions d'euros de chiffre d'affaires et 80 millions de résultats). Parfois, la direction générale doit démissionner, tant le montant de perte est abyssal et la gestion de la crise catastrophique (par exemple, aux États-Unis, Equifax en 2017, avec ses pertes de 1,4 milliard de dollars, une des plus grosses fuites de données personnelles de l'histoire touchant près de 150 millions d'Américains, et certains membres de la direction générale vendant leurs parts quelques jours avant que le scandale éclate). Parfois, ce sont des vies qui sont perdues (par exemple, en 2021, une patiente est décédée lors de la cyberattaque de l'hôpital universitaire de Düsseldorf en Allemagne).

D'autres fois, c'est la survie de l'entreprise, voire d'une économie entière qui est en jeu (par exemple, en France, le risque de défaillance d'une TPE/PME augmenterait d'environ 50 % dans les six mois suivant l'attaque selon les assureurs[1], et le tissu économique français est composé à 99,9 % de TPE/PME). Bref, vous voyez bien au travers de ces quelques

1 « Les TPE et PME sont les cibles privilégiées des pirates informatiques en 2022 selon l'Anssi », www.francenum.gouv.fr, 8 février 2023.

exemples que la cybersécurité, c'est-à-dire la réduction du risque lié au numérique, est loin d'être un sujet uniquement technique.

Si l'on en croit l'excellent ouvrage de vulgarisation *Cyberattaques* de notre confrère Gérôme Billois[2], la cybermenace ne date pas d'hier, mais remonte aux origines mêmes de la création d'Internet. Depuis, cette menace s'est concrétisée ouvertement et la cybercriminalité coûte actuellement à l'économie mondiale la bagatelle de 6 000 milliards de dollars (comme on peut le lire publiquement de diverses sources de confiance). À titre de comparaison, c'est l'équivalent de six crises des *subprimes*. Vous vous souvenez du chaos mondial qui régnait en 2007 lors de cette crise ? Vous vous rappelez les messages alarmants des gouvernements et des grandes banques de toute la planète ? Eh bien, la cybercriminalité, c'est cela tous les ans, et avec un rythme de croissance effréné. Un vrai business, très lucratif et nettement moins dangereux que de tirer au lance-roquette sur un transporteur de fonds en pleine rue. Nous sommes prêts à parier que si Pablo Escobar était encore de ce monde, il aurait troqué la cocaïne contre un ordinateur.

Si tout cela est possible, c'est que le numérique fait partie de notre quotidien. Comment travailler sans informatique ? Et comment réagirions-nous si nous étions les otages d'acteurs malveillants ayant pris le contrôle de nos outils digitaux ? Essayez d'imaginer, ne serait-ce que deux secondes, que le pacemaker connecté de votre père soit piraté et que l'on vous demande de payer pour qu'il cesse de danser la zumba dans son sommeil. Ainsi, on nous demande souvent si le paiement d'une rançon est une « bonne pratique ». Bien sûr que non et pour de nombreuses raisons, mais quand on regarde froidement les chiffres, il est clair que la réalité dépasse souvent la théorie ou les versions officielles.

Alors que faire ? Baisser les bras, mettre de côté une forte somme d'argent en cryptomonnaie, prévenir son assureur et attendre que cela

2 *Cyberattaques. Les dessous d'une menace mondiale*, Gérôme Billois (avec Nicolas Cougot), illustrations de Pascal Garnier, Hachette, 2022.

nous arrive ? Ou relever la tête, redresser les épaules, être conscient qu'en matière de crise cyber, ce n'est pas une question de « si », mais de « quand », et se préparer sérieusement ? Préparer l'ensemble de l'organisation pour que les collaborateurs puissent jouer leur rôle de première ligne de défense, que les équipes informatiques et de cybersécurité restent à la page, et que la direction générale ait les meilleurs réflexes pour prendre les bonnes décisions sous la pression.

Cet ouvrage répond à toutes ces questions, et bien plus encore (fiches-outils, témoignages croisés…). Il vise à devenir votre guide de chevet, vous rappelant les bons réflexes au quotidien. Il vous permettra également d'ouvrir les yeux sur notre dépendance au numérique et sur les moyens de continuer de vivre, produire, travailler, tout en réduisant le risque que des personnes malveillantes viennent mettre à mal ce que vous aimez et ce en quoi vous croyez.