Barracuda
Your journey, secured.

AVRIL 2024

Rapport de la DSI : Comment diriger votre entreprise face aux risques cyber ?

Table des matières

Introduction

En raison de l'utilisation croissante de technologies émergentes telles que l'intelligence artificielle (IA) dans les entreprises, il est plus important que jamais que leurs dirigeants sachent comment mettre en œuvre ces outils de manière efficace et sécurisée.

Pour de nombreuses entreprises, cela peut être difficile. Le panorama des risques informatiques est complexe et en constante évolution. Le langage en rapport aux menaces informatiques peut être très technique, plein de jargon et incompréhensible. De plus, les organisations ne sont pas toutes disposées à s'exposer à un même niveau de risque : ce qui constitue un niveau acceptable pour une entreprise peut être impensable pour une autre. Pour finir, les organisations commerciales doivent souvent trouver des compromis face aux priorités concurrentes en matière d'allocation de leurs ressources.

En matière de sécurité, l'objectif ultime de toute organisation est la résilience de ses systèmes informatiques. La pierre angulaire des stratégies de sécurité demeure la prise de mesures efficaces pour la prévention et la détection des problèmes. Cependant, il est préférable d'aller plus loin. Les faits avérés semblent indiquer qu'il est presque inévitable d'être affecté par un incident de sécurité. De nombreuses entreprises sont fréquemment touchées et, dans beaucoup de cas, il s'agit d'organisations qui ont subi un premier incident et qui, par la suite, ne se sont pas attaquées à sa cause profonde ou aux facteurs qui ont permis son déclenchement.

Ce qui importe le plus est ce que vous faites pour vous préparer et, en cas d'incident, pour résister, réagir et restaurer. C'est cela qui constitue la résilience informatique.

Vous pourrez presque rendre vos systèmes résilients en recourant à un dispositif de sécurité évolué et axé sur la défense en profondeur. De tels outils existent mais, au bout du compte, votre résultat dépendra de vos ressources humaines : les dirigeants de votre entreprise, ses professionnels de la sécurité informatique et ses employés en général.

Selon l'étude Cybernomics 101, que nous avons menée conjointement avec l'institut Ponemon, les problèmes de sécurité liés aux personnes sont de nature à nuire à la résilience des systèmes informatiques. Ces problèmes peuvent inclure un manque de soutien de la part des dirigeants d'une entreprise ou de la part des responsables de son service de sécurité, une pénurie de compétences et de personnel, ainsi que des variations dans la mise en œuvre des politiques de sécurité entre différentes parties d'une organisation. Pour de nombreuses entreprises, la sécurité de leur chaîne d'approvisionnement constitue un sujet d'inquiétude. Une autre préoccupation courante concerne la possibilité que certaines personnes extérieures à une organisation pourraient avoir accès à des données sensibles ou confidentielles. Ces deux domaines présentent des risques importants et sont souvent exploités par les pirates.

La plupart des organisations comprennent le niveau de risque qu'elles prennent. Seules 43 % d'entre elles jugent leur dispositif de sécurité très efficace. Cependant, ce chiffre n'est peut-être pas aussi inquiétant qu'il ne le semble. Lorsque l'on croit que l'on pourrait en faire plus pour mieux se protéger, il est plus probable que l'on concentre son attention et ses ressources sur les domaines qui en ont besoin. Au bout du compte, la sécurité d'une organisation peut ainsi être renforcée.

Dans ce rapport, nous examinons plus en profondeur ce que la recherche sur la résilience informatique a révélé. Nous vous offrons également des conseils pour vous aider à cheminer vers un avenir consolidé et plus résilient adapté à vos besoins.

Siroui Mushegian, DSI, Barracuda Networks Inc.

Méthodologie

Au total, l'institut Ponemon a interrogé 1 917 professionnels de la sécurité informatique dans le courant de septembre 2023. Parmi ces personnes, 522 étaient situées aux États-Unis, 372 au Royaume-Uni, 329 en France, 425 en Allemagne et 269 en Australie. L'échantillon final de personnes interrogées couvrait des organisations comptant entre 100 et 5 000 employés. Toutes ces personnes participaient activement à la gestion de fonctionnalités ou d'activités en rapport à la sécurité informatique dans leur organisation.

Ce rapport présente les résultats de notre enquête, ainsi que les divergences selon les effectifs des entreprises et leur appartenance à certains segments de marché verticaux. Les résultats ont été consolidés pour tenir compte de tous les pays étudiés.

Comment les organisations évaluent-elles leur posture de sécurité ?

Nous avons demandé aux personnes interrogées quel était leur degré de confiance dans leur capacité à gérer efficacement les risques, vulnérabilités et attaques en rapport à leurs systèmes informatiques. Nous avons catégorisé les réponses sur une échelle allant de 1 à 10, l'indice 1 correspondant à un très faible degré d'efficacité et l'indice 10 à une efficacité absolue.

Les entreprises du secteur financier sont, de loin, celles qui sont les plus confiantes dans leur capacité à faire face aux problèmes de sécurité. En effet, plus de la moitié d'entre elles (55 %) jugent leur posture très efficace. Les plus petites entreprises interrogées étaient les moins optimistes, avec environ la moitié (48 %) évaluant leur niveau de sécurité au bas de l'échelle.

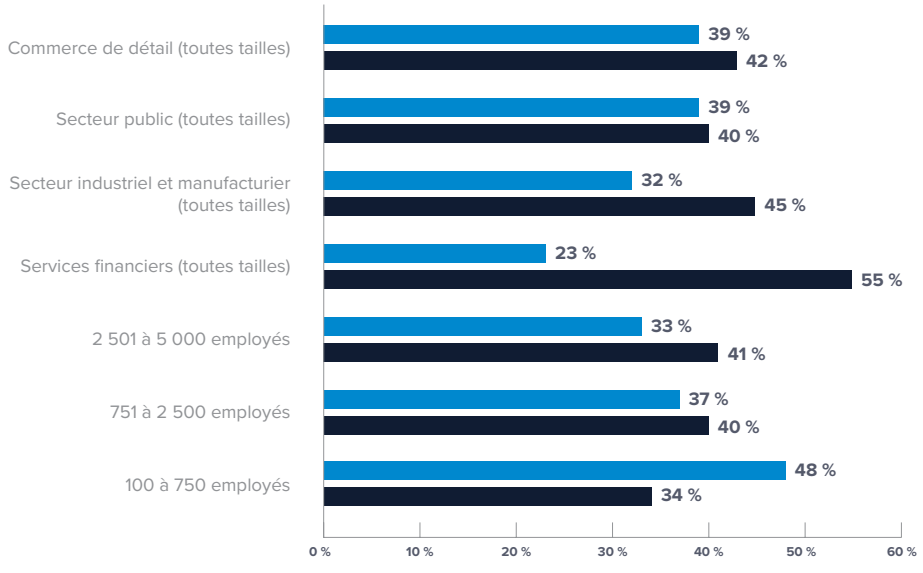


FIGURE 1

Quelle note attribueriez-vous à la posture de sécurité de votre organisation sur la base de l'efficacité de la protection qu'elle apporte contre les risques, les vulnérabilités et les attaques ? Veuillez utiliser notre échelle allant de 1 à 10.

Pas très efficace (1 à 4)

Très efficace (7 à 10)

n = 1 917

La catégorie « modérément efficace » (notes 5 et 6) n'est pas incluse dans ce tableau.

Les défis de la gouvernance

La variabilité des mesures de sécurité à l'échelle d'une entreprise

Pour les petites et moyennes entreprises, le principal problème de gestion est constitué par le manque d'uniformité des politiques et des programmes de sécurité dans l'entreprise. La moitié de ces organisations (48 % et 50 % respectivement) considèrent que ce problème est l'un des principaux auxquels elles doivent faire face, contre seulement un quart (27 %) des entreprises qui comptent entre 2 501 et 5 000 employés. Ce problème vient également en tête pour les services financiers (49 %), les commerces de détail (49 %) et le secteur public (40 %).

La mise en œuvre de politiques systématiques peut être très difficile à organiser pour les équipes de sécurité. Les chefs d'entreprise sont parfois réticents à faire appliquer des pratiques de sécurité qui semblent peu pratiques ou restrictives. Des employés résistent quelquefois à certains modes de contrôle, comme les accès « juste-à-temps » ou au « moindre privilège » aux applications ou données, surtout lorsqu'ils ont bénéficié d'un accès sans restrictions dans le passé.

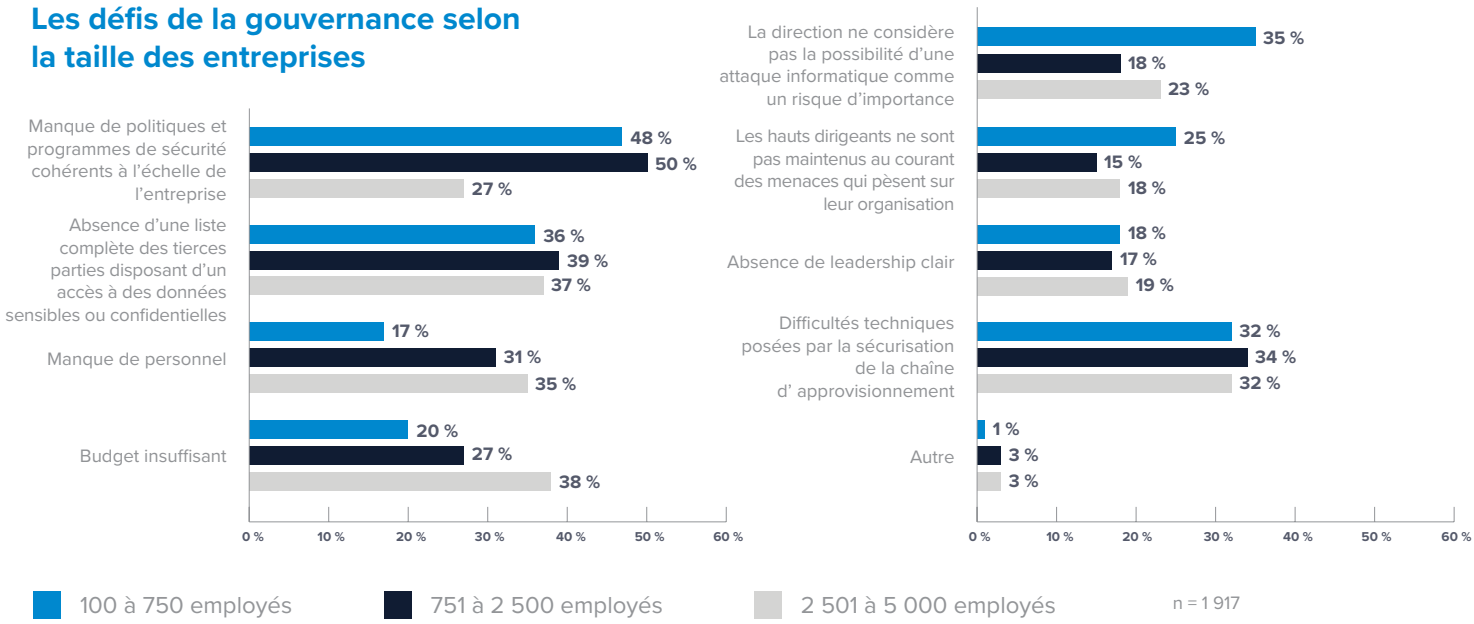
Certains employés peuvent ne pas être au courant des politiques de sécurité, ne pas savoir si elles s'appliquent à leurs systèmes ou à leur poste ou, parfois, pensent pouvoir s'y soustraire du fait de leur activité.

De tels malentendus peuvent occasionner une confusion et une résistance. En conséquence, les politiques peuvent ne pas être appliquées efficacement, ce qui aboutit à un accroissement des risques pris par une entreprise.

Plus vous communiquerez ouvertement et sans rien cacher à vos employés au sujet de vos politiques, plus vous vous faciliterez la tâche. Vos interlocuteurs doivent connaître le contenu de vos politiques, savoir à qui elles s'appliquent et comprendre l'importance de leur mise en œuvre. Ce type de conversations favorise la bonne compréhension et la coopération, particulièrement si vous étayez vos discussions par des séances de formation régulières. Il est également important que vous vous adaptiez aux changements. Vous devez donc réexaminer et réviser régulièrement vos politiques de sécurité, afin qu'elles prennent en compte l'évolution des risques et des besoins de votre entreprise.

FIGURE 2

Les défis de la gouvernance selon la taille des entreprises



Le manque de soutien et de compréhension de la part des équipes de direction

Pour les petites entreprises qui ont participé à notre enquête, les difficultés liées aux dirigeants constituent un sujet d'inquiétude majeur. Dans un peu plus d'un tiers des cas (35 %), il nous a été signalé que la direction ne considère pas la possibilité d'une attaque informatique comme un risque d'importance. Il ne serait pourtant pas judicieux d'incriminer les dirigeants d'entreprise à ce sujet. Lorsque l'on ne comprend pas un problème, il est difficile de s'y intéresser ou de s'en inquiéter. Un quart des entreprises les plus petites admettent que leurs dirigeants les plus haut placés ne sont pas maintenus au courant des menaces qui pèsent sur leur organisation. C'est aux professionnels de la sécurité qu'il incombe de parler dans un langage que les chefs d'entreprise comprennent. Ces professionnels doivent communiquer comme des conteurs. Ils doivent être capables d'expliquer comment protéger la réputation d'une entreprise par le biais de programmes de défense anticipateurs et polyvalents.

Liste de gestion des risques

Pour aider une équipe de direction à comprendre les risques auxquels elle est confrontée ainsi que ses choix en matière de sécurité, un moyen utile consiste à lui présenter une liste d'options. Cette démarche peut permettre de mieux comprendre quels sont les risques qui nécessitent une attention plus particulière et quel niveau général de risque peut être considéré comme tolérable.

En recourant à la méthodologie constituée des quatre étapes ci-dessous, vous serez en mesure de mieux comprendre les risques auxquels votre organisation est actuellement confrontée :

1. **Les menaces :** Les circonstances ou événements susceptibles de nuire aux activités de votre organisation, à ses actifs, à ses personnes ou à d'autres organisations.
2. **Les vulnérabilités :** Les faiblesses qui exposent votre organisation ou vos actifs à des risques d'exploitation.
3. **L'éventualité :** La probabilité qu'un risque se matérialise.
4. **Le niveau de risque :** La potentialité d'effets indésirables.

Une fois que vous avez compris quel est votre niveau de risque, vous pouvez décider du niveau de protection que vous souhaitez et dont vous avez besoin :

- Par exemple, un « haut niveau de protection » implique de presque tout verrouiller. Vous pouvez bénéficier d'une sécurité presque parfaite en suivant ce type de démarche. D'un autre côté, elle peut vous obliger à introduire certaines contraintes susceptibles d'aboutir à une complexité accrue, à de nouveaux retards et à des mésententes.
- À l'autre extrémité de l'échelle, une « faible protection » signifiera que vous n'apporterez que peu de restrictions d'accès à vos systèmes. Une telle stratégie ouverte est pratique, mais elle est aussi très risquée.

Toutes les entreprises ne disposent pas dès le premier jour de tous les moyens, outils et processus qu'il leur faut pour assurer leur sécurité. En considérant votre sécurité avec une liste d'options, vous pourrez élaborer un plan d'action pour prévoir le cheminement à suivre vers votre objectif et les risques à gérer en cours de route.

Cette liste d'options pourra vous aider à comprendre quels sont ceux de vos risques qui nécessitent une attention plus particulière. Avec un registre centralisé de vos risques, vous serez mieux en mesure de garder un œil sur les risques pris par votre organisation et de prendre des décisions éclairées pour les gérer ou les atténuer.

Le manque de compétences et l'impossibilité de surveiller et de contrôler les tierces parties

Pour les plus grandes entreprises qui ont participé à notre enquête, ce sont les budgets insuffisants et la manque de professionnels de sécurité compétents qui constituent les principaux sujets d'inquiétude, avec des proportions respectives de 38 % et de 35 %.

Les risques liés aux chaînes d'approvisionnement sont invariablement perçus comme constituant un problème d'importance, ceci dans les entreprises de toutes tailles. Deux sources majeures de ces risques nous sont apparues, chacune ayant été citée par environ le tiers des personnes interrogées. La première est due au fait de ne pas disposer d'une liste complète des tierces parties ayant accès à des données sensibles ou confidentielles. La seconde est constituée par le défi d'ordre technique posé par la sécurisation d'une chaîne d'approvisionnement.

Ce qui est à l'origine de ces inquiétudes est probablement le fait qu'une grande partie des chaînes d'approvisionnement se situent au-delà du périmètre de sécurité d'une entreprise. Plus quelque chose échappe à votre contrôle, plus vous prenez de risques, surtout si certains de vos fournisseurs opèrent sur des marchés où les réglementations de sécurité sont relativement laxistes.

L'informatique fantôme est aussi devenue une préoccupation majeure. L'usage sans supervision d'applications logicielles pose des risques pour la sécurité, car il est fréquent que ces outils informatiques ne soient pas couverts par les politiques des entreprises. Même les outils logiciels approuvés peuvent présenter des risques, car un grand nombre d'entre eux sont devenus des plates-formes avec des marketplaces pour des applications et des modules d'extension tiers. Ces ajouts peuvent permettre à des intrus d'agir au-delà du périmètre de sécurité d'une entreprise pour accéder à des données sensibles.

Notons également que, bien que les outils d'IA générative à usage libre puissent être bénéfiques pour l'innovation et la productivité, ils enregistrent les données qui leur parviennent et ces données servent de base à leur modèle pour apprendre. En conséquence, l'usage sans supervision de ces outils peut aboutir à la propagation des données d'une entreprise au-delà de son périmètre de sécurité.

Aperçu d'un secteur : les services financiers

Les entreprises du secteur financier ont la conviction que leur posture de sécurité est robuste. Seules 3 % d'entre elles n'ont pas de plan en place pour répondre aux incidents.

Ce n'est pas surprenant. Le secteur financier est très réglementé, avec des exigences strictes en matière de conformité et des sanctions en cas d'infraction. Ses employés comprennent qu'il doivent travailler dans le cadre de la réglementation en vigueur et qu'ils ont des processus et des procédures à respecter. Les conseils d'administration et les hauts dirigeants approuvent les mesures de sécurité, et les budgets sont suffisants. En conséquence, des stratégies sont en place pour la planification de la continuité des activités (PCA) et celle de la reprise après sinistre (PRA/PRS). Ces organisations sont donc bien placées pour se remettre rapidement d'un incident.

Le secteur doit cependant faire face à certains problèmes en matière de sécurité. Un grand nombre de sociétés financières sont d'une très grande taille. Elles se sont développés d'acquisition en acquisition et, en fin de compte, elles sont devenues d'énormes organisations d'envergure mondiale dont le fonctionnement reste fragmenté. À l'échelle mondiale, la mise en œuvre de procédures de sécurité robustes est extrêmement difficile.

Aperçu d'un secteur : le commerce de détail

Les détaillants ne sont pas aussi confiants que les services financiers en ce qui concerne leur posture de sécurité d'ensemble, 39 % d'entre eux la jugeant plutôt inefficace. 42 % estiment cependant que leur posture de sécurité est très efficace, ce qui met en évidence la complexité et la dichotomie présentes dans ce secteur en rapport à la sécurité.

D'une part, il y a les institutions corporatives comme les sièges sociaux. Elles disposent des équipements, des logiciels d'entreprise, des centres de données et des dispositifs de protection les plus modernes. D'autre part, il y a aussi les centres de distribution, les chaînes de production et d'approvisionnement, et les magasins dans lesquels les ventes au détail sont effectivement réalisées. Les outils technologiques utilisés dans cette infrastructure peuvent être tout autres. Il peut s'agir en grande partie d'équipements vétustes qui seraient difficiles ou coûteux à éliminer, et les équipes informatiques doivent essayer de faire de leur mieux avec ce qu'elles ont.

Les commerces de détail sont les entreprises les plus susceptibles de citer deux types de problèmes comme constituant un défi majeur pour leur gestion. L'un est l'absence d'une liste des tiers ayant accès à des données sensibles et confidentielles (46 %). L'autre est posé par les difficultés d'ordre technique éprouvées pour sécuriser les chaînes d'approvisionnement (35 %).

Aperçu d'un secteur : les organismes publics

Les organisations du secteur public sont de celles qui sont plus susceptibles de ne pas avoir confiance dans leur posture de sécurité. 39 % d'entre elles jugent cette posture plutôt inefficace. Le problèmes les plus souvent cités comme constituant un obstacle à une bonne gestion sont l'insuffisance des budgets (39 %) et, en première position, l'absence de politiques et de programmes de sécurité uniformes à l'échelle d'une organisation (40 %). Un peu plus d'une de ces organisations sur 10 (12 %) n'a pas de plan de réponse aux incidents en place.

Le secteur public est difficile à protéger. Le nombre de bureaux et d'employés à couvrir est considérable, les budgets sont toujours serrés et l'attention des dirigeants est souvent concentrée ailleurs, en particulier lorsqu'il s'agit de dirigeants politiques. De nombreuses organisations du secteur public sont confrontées à des budgets et à un financement en constante évolution. Les décisions à ce sujet dépendent du parti au pouvoir, et les changements sont souvent soudains. Dans ces circonstances, il peut se révéler ardu de planifier une sécurité à long terme.

La planification de la réponse aux incidents

La bonne nouvelle est que, dans environ la moitié des organisations qui ont participé à notre enquête — quels que soient leur secteur d'activité ou leur nombre d'employés —, un plan de réponse aux incidents a été établi et est appliqué de manière systématique dans la totalité de l'organisation. De plus, ce plan fait l'objet de tests protocolaires au moins une fois par an dans plus de la moitié des cas, selon les entreprises interrogées.

Malheureusement, la bonne nouvelle s'arrête là. Environ un quart (23 %) des plus grandes entreprises n'ont jamais testé leur plan de réponse aux incidents. La raison en est probablement que, dans une entreprise de grande taille, ce processus peut être complexe, exiger beaucoup de temps et perturber les activités. À l'échelle d'une telle entreprise, la mise en œuvre d'un plan de type PCA ou PRA peut être coûteuse, car elle peut nécessiter la sauvegarde de volumes considérables de données ou celle de systèmes de grande envergure.

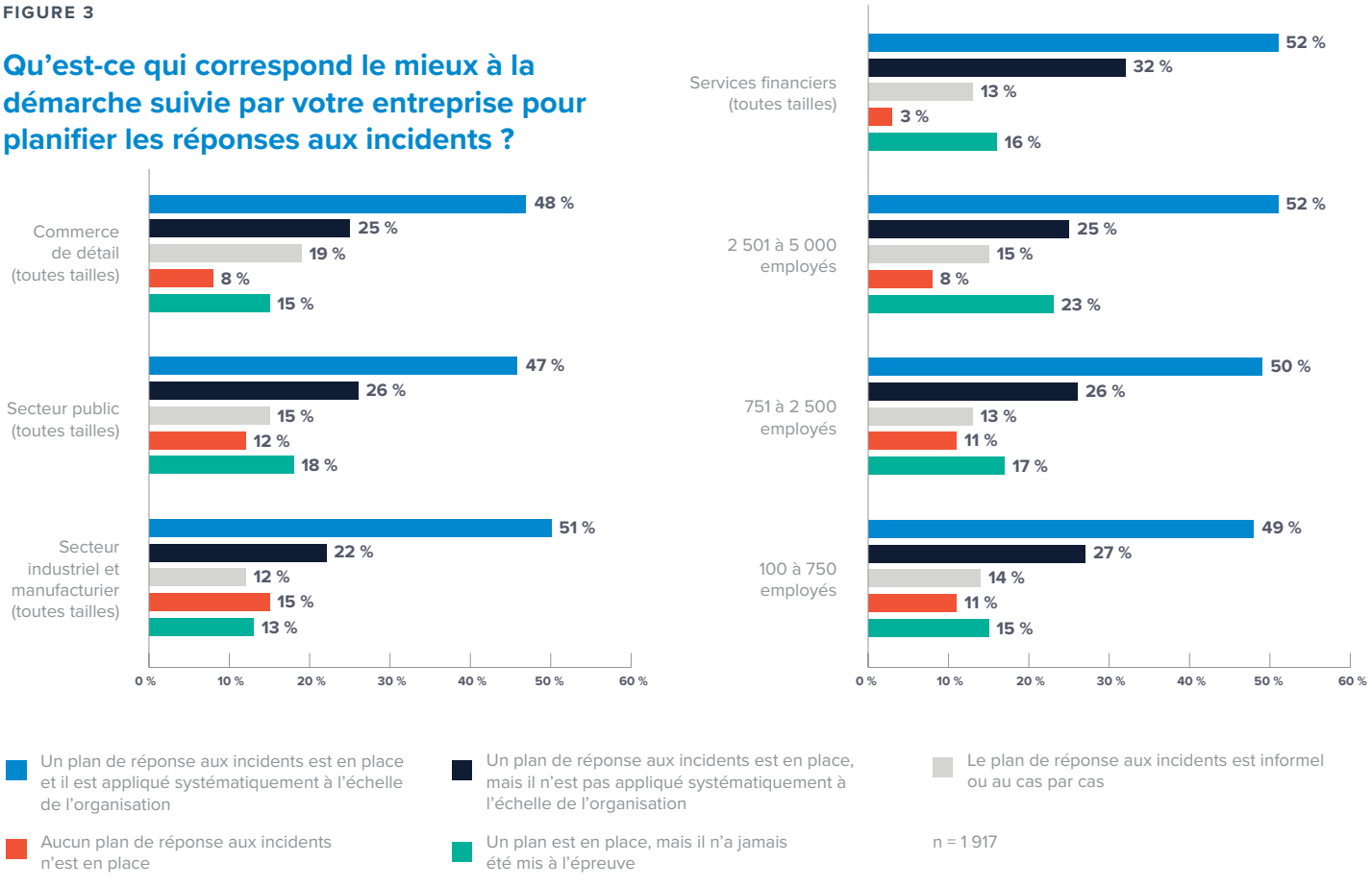
De plus, environ une organisation sur dix a admis qu'elle n'avait pas de plan de réponse aux incidents en place.

Lorsqu'une organisation ne planifie pas la marche à suivre en cas d'incident affectant sa sécurité, elle risque de se retrouver dans la situation précaire où elle ne sait pas comment réagir face à certains événements. Dans ces moments, elle risque donc de ne rien faire ou, si elle agit, de commettre des erreurs.

Une démarche basée sur une ou des « équipes violettes » peut contribuer à renforcer l'efficacité des réactions aux incidents dans une entreprise. Les équipes violettes ont pour mission d'organiser et de coordonner des simulations de réponse à des incidents. Elles créent des situations au cours desquelles une « équipe rouge » cause un incident simulé auquel une « équipe bleue » doit réagir. Ces simulations permettent aux entreprises d'apprendre à mieux détecter les incidents affectant leur sécurité. Elles aident également les entreprises à améliorer leurs mesures de réaction et d'atténuation ainsi qu'à tirer les leçons de leur expérience.

FIGURE 3

Qu'est-ce qui correspond le mieux à la démarche suivie par votre entreprise pour planifier les réponses aux incidents ?



Checklist de cyber-résilience

La checklist de cyber-résilience suivante s'appuie sur le cadre de cybersécurité de l'U.S. National Institute of Standards and Technologies (NIST).

OBJECTIF	AXE STRATÉGIQUE POUR LES CHEFS D'ENTREPRISE – CE QUE VOUS DEVEZ SAVOIR	PROGRESSION
PRÉPARATION	**Organiser** • Conformité réglementaire Quelles sont vos obligations en matière de législation et de conformité dans chacun des marchés où vous opérez ? • Implication et responsabilité de la direction Qui, au sein de l'équipe de direction, doit être impliqué dans les décisions relatives à la cyber-résilience et aux risques ? • La cyberassurance De quel type d'assurance avez-vous besoin/dans quel type d'assurance êtes-vous prêt ou capable d'investir ?	☐ ☐ ☐
	Identifier • Gestion des actifs De quels actifs disposez-vous, où se trouvent-ils et qui y a accès ? Quels sont les éléments clés dont vous disposez pour assurer la continuité de vos activités et de vos opérations ? • Gestion des risques et stratégie Quels sont vos actifs les plus exposés ? Quels sont les risques auxquels ils sont confrontés ? Quel est l'impact potentiel d'une attaque en termes de dommages, de perturbations ou de pertes ?	☐ ☐
RÉSISTER	**Protéger** • Processus, politiques et technologies de sécurité Comment protéger au mieux les biens, les infrastructures et les personnes dans la limite des ressources disponibles ? • Formation de sensibilisation à la cybersécurité Comment formez-vous et accompagnez-vous les employés ? • Maintenance et contrôle : correctifs, etc. Avez-vous mis en place les mesures de sécurité de base ? Application de correctifs, authentification robuste, contrôles d'accès (authentification multifactorielle/Zero Trust), etc.	☐ ☐ ☐
	Détection • Technologies et procédés de détection Vos systèmes de sécurité peuvent-ils détecter et bloquer les menaces nouvelles et émergentes ? • Centre des opérations de sécurité Votre surveillance de la sécurité est-elle fiable et continue ? Pouvez-vous superviser et gérer l'ensemble du parc informatique 24 heures sur 24, 7 jours sur 7 ? Disposez-vous des outils, des compétences et des effectifs nécessaires pour enquêter sur les signaux d'alerte et les anomalies ?	☐ ☐
AGIR	**Atténuer** • Planification et processus de réponse aux incidents Disposez-vous d'un plan de réponse aux incidents couvrant l'ensemble de l'entreprise ? Est-il régulièrement testé et mis à jour ? Comment procédez-vous pour circonscrire et neutraliser les incidents ? Pendant combien de temps vos systèmes critiques peuvent-ils tenir en cas d'interruption ? Pouvez-vous revenir à des processus manuels si nécessaire ? Dans le cas où une interruption affecte vos clients, quel est le niveau de service contractuel ? Votre système est-il sur site ou dans le cloud ? (S'agit-il d'un service de sécurité (SaaS) fourni par une entreprise, d'un système d'entreprise, etc.) En termes de conformité réglementaire, qui devez-vous informer et quand ? • Communications internes et externes • Analyse et atténuation des incidents	☐ ☐ ☐
RÉCUPÉRER	**Restaurer** • Planification de la reprise Disposez-vous d'un plan de continuité des activités/un plan de reprise après sinistre ? Avez-vous mis en place une solution de « haute disponibilité » avec votre fournisseur de cloud ? Avez-vous besoin de l'assistance d'un tiers pour identifier et combler toutes les lacunes ? • Communications internes et externes • Améliorations Quelles leçons avez-vous apprises ? Quelles mesures prenez-vous ou devez-vous prendre pour renforcer votre sécurité ?	☐ ☐ ☐

Conclusion

La résilience informatique relève de la responsabilité de tous, mais c'est surtout aux professionnels de la sécurité que cette charge incombe. Vous pouvez bénéficier de ressources utiles à ce sujet. Par exemple, certaines méthodes fondamentales et pratiques peuvent vous aider à vous assurer que, au minimum, vos éléments de base sont bien en place.

Avec le modèle de checklist ci-dessus, vous disposez d'un excellent moyen de maintenir votre équipe et votre entreprise sur la bonne voie et de responsabiliser votre personnel. Vous pouvez adapter ce document aux caractéristiques de votre environnement professionnel. Il peut vous servir de base pour établir une feuille de route ou un plan d'action comportant des jalons, des attentes et une liste des parties responsables.

Pour en savoir plus

Un grand nombre d'outils, de documents-cadres et de lignes directrices sont à votre disposition pour vous aider à vous frayer un chemin vers la résilience de vos systèmes informatiques. Voici quelques-unes de ces ressources, pour vous aider à vous lancer :

- La gestion des systèmes informatiques : code de pratique (Royaume-Uni)
- Association nationale des directeurs d'entreprise (États-Unis)
- Institut australien des directeurs d'entreprise (Australie)
- La cybersécurité : document-cadre, édition 2.0 (États-Unis)

Barracuda en quelques mots

Notre objectif : faire du monde un endroit plus sûr. Chez Barracuda, nous pensons que chaque entreprise doit pouvoir disposer de solutions de sécurité cloud-first adaptées, abordables, intuitives et facilement déployables. Nous protégeons vos emails, réseaux, données et applications à l'aide de solutions innovantes capables de s'adapter au parcours de nos clients, et de se développer en conséquence. Plus de 200 000 entreprises partout dans le monde ont choisi Barracuda pour veiller à leur sécurité pendant qu'elles prospèrent.

Pour en savoir plus, rendez-vous sur fr.barracuda.com.

Barracuda
Your journey, secured.