A Lynchpin Media BRAND

CXO priorities

Comprendre comment les entreprises industrielles naviguent dans le paysage de menaces

un rapport de CXO Priorities en partenariat avec Quest

Quest

priorities

A Lynchpin Media BRAND

CONTENU

Quest

priorities

A Lynchpin Media BRAND

INTRODUCTION

L'expansion rapide des champs d'attaque et l'évolution constante du paysage des menaces ont pratiquement triplé les chances que chaque entreprise industrielle soit confrontée à un événement de cybersécurité suffisamment important pour perturber son processus de production. La pandémie a joué un rôle essentiel dans la mise en évidence des champs d'action des cyberattaques et des outils de cybersécurité restreints, mettant ainsi l'accent sur les procédures de reprise en cas de sinistre dans le secteur industriel.

Les cyberattaques constituent une menace croissante pour le secteur industriel et continuent de progresser en termes de volume et de sophistication. Nous assistons à des attaques perturbatrices qui entraînent des répercussions sur les processus industriels et la chaîne d'approvisionnement, avec des rançongiciels, des intrusions permettant le vol d'informations et de nouvelles activités des systèmes de contrôle industriel ciblant les adversaires.

L'effet de ces avancées et des systèmes d'entreprise dépourvus des contrôles de sécurité inhérents nécessaires pour se protéger, entraîne des arrêts de production, des pertes financières qui se chiffrent en millions, des perturbations de la chaîne d'approvisionnement et des atteintes à la réputation des entreprises.

Le secteur industriel est l'un des cinq secteurs les plus touchés par les cyberattaques. Selon les experts, pour commencer, chaque entreprise industrielle doit investir dans des programmes globaux de cyber-gestion qui s'étendent à l'ensemble de l'entreprise afin d'identifier les cyber-attaques, de s'en protéger, d'y réagir et de s'en remettre.

Quest

CXO priorities

A Lynchpin Media BRAND

APERÇU DE L'ENQUÊTE:

Pour en savoir plus, nous avons interrogé des cadres supérieurs sur leurs préoccupations en matière de cybersécurité au Royaume-Uni, en Allemagne et en France, dans le secteur industriel. Ce rapport explore les problématiques auxquelles sont confrontées les entreprises industrielles pour renforcer leurs politiques de sécurité et de reprise après sinistre.

Cette enquête a pour but de découvrir:

- La manière dont les entreprises industrielles s'y prennent pour faire face aux menaces actuelles et futures
- Les principaux défis liés aux menaces et les lacunes en matière de sécurité dans le secteur industriel
- Les priorités et les plans pour adopter de nouvelles technologies, s'aligner sur les structures et combler les lacunes en matière de compétences

Principales conclusions

- Plus de 38 % des entreprises industrielles subiraient une perte de revenus de 20 à 50 millions de dollars si leur environnement Active Directory était piraté pendant 24 heures, et 32 % subiraient une perte comprise entre 50 et 100 millions de dollars.
- L'espionnage industriel (21 %) et les rançongiciels (22 %) sont les plus grandes menaces pour la sécurité dans l'industrie manufacturière.
- Trente-trois pour cent des entreprises manufacturières considèrent que la cybersécurité est importante, mais se contentent de la sécurité existante sans procéder à un examen supplémentaire lors de l'adoption d'une nouvelle technologie.
- Quatre-vingts pour cent des personnes interrogées déclarent que la cybersécurité de leur entreprise a été négativement affectée par la pénurie de compétences.
- Plus de la moitié des personnes interrogées (54 %) considèrent que la cybersécurité est importante lors de l'adoption d'une nouvelle technologie.
- Deux tiers des personnes interrogées (66 %) pensent que les risques en matière de cybersécurité auront une incidence négative sur la vitesse à laquelle les nouvelles technologies seront adoptées dans leur entreprise.
- L'écrasante majorité (87 %) déclare que ses mesures de cybersécurité sont conformes au cadre du NIST.
- Plus de deux tiers des personnes interrogées (67 %) considèrent que la mise en place d'un dispositif de cybersécurité pour leur entreprise est une priorité moyenne ou élevée.
- Lorsqu'il s'agit d'évaluer si la cybersécurité d'une entreprise a été affectée par une pénurie de compétences, quatre cinquièmes des personnes interrogées déclarent avoir été affectées (80 %).
- Le rythme rapide d'adoption des nouvelles technologies (33 %) a été cité comme le plus grand défi à relever par les entreprises en matière de manque de compétences en cybersécurité, suivi de près par la dépendance à l'égard des technologies existantes (27 %) et les restrictions budgétaires (27 %).

Quest

priorities

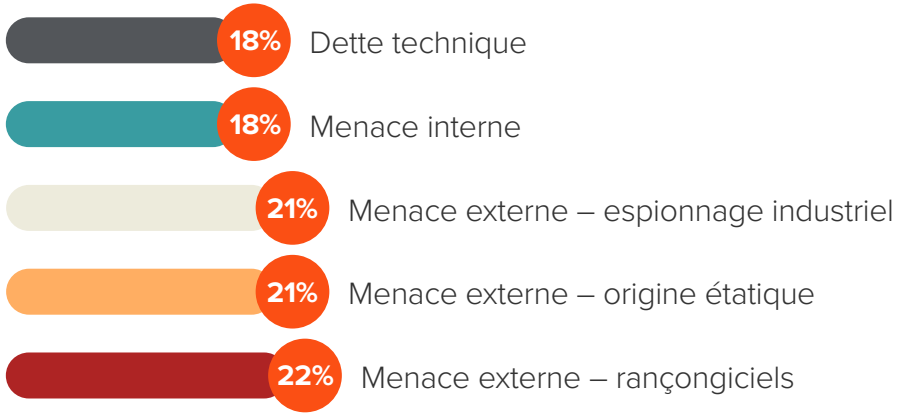
A Lynchpin Media BRAND

PARTIE 1:

Les défis de la cybersécurité dans le secteur industriel

La gestion de la montée des cyberattaques et la mise en adéquation des mesures de cybersécurité avec les cadres organisationnels constituent une préoccupation majeure pour de nombreuses entreprises industrielles. Dans cette section, nous examinons le panorama des menaces qui pèsent sur l'industrie et les principales difficultés rencontrées par les personnes interrogées pour protéger leur chemin d'attaque.

Quelles sont, selon vous, les plus grandes menaces pour la sécurité dans le secteur industriel? (Veuillez en choisir deux)



Principaux enseignements

Les rançongiciels (22 %), l'espionnage industriel (21 %) et les menaces d'origine étatique (21 %) sont considérés comme les plus grandes menaces pour la sécurité dans le secteur industriel. C'est une représentation précise de l'état actuel des champs d'attaque et de la nécessité pour les entreprises industrielles de prendre en compte la sécurité OT le plus tôt possible.

Quest

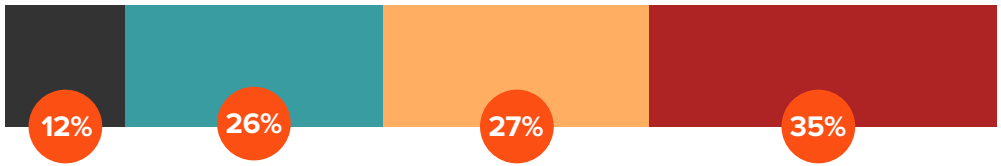
priorities

A Lynchpin Media BRAND

PARTIE 1:

Les défis de la cybersécurité dans le secteur industriel

Parmi les incidents suivants, quels sont ceux que vous avez connus dans votre entreprise? (Veuillez en choisir deux)



- Fuite de données involontaire (ordinateur portable envoyé à la mauvaise personne, etc.)
- Vol d'informations d'identification / compte compromis
- Phishing / ingénierie sociale
- Rançongiciels / logiciels malveillants

Principaux enseignements

Les personnes interrogées attestent que les attaques les plus fréquentes sont les rançongiciels et les logiciels malveillants (35 %), ainsi que l'hameçonnage et l'ingénierie sociale (27 %). Cela souligne la nécessité de mettre en place une sécurité multiniveaux contre les attaques ciblées et sans fichier, capable de stopper les virus, les logiciels espions, les logiciels malveillants et les rançongiciels. Il est inquiétant de constater que le secteur industriel est l'un des cinq secteurs les plus touchés par les cyberattaques, d'où la nécessité de mettre en place plusieurs niveaux de protection puissants.

Quest

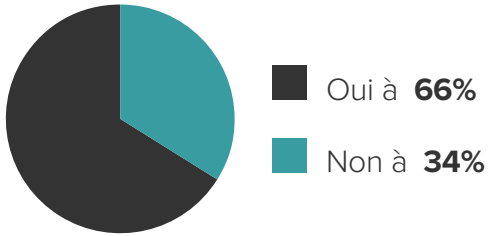
CXO priorities

A Lynchpin Media BRAND

PARTIE 1:

Les défis de la cybersécurité dans le secteur industriel

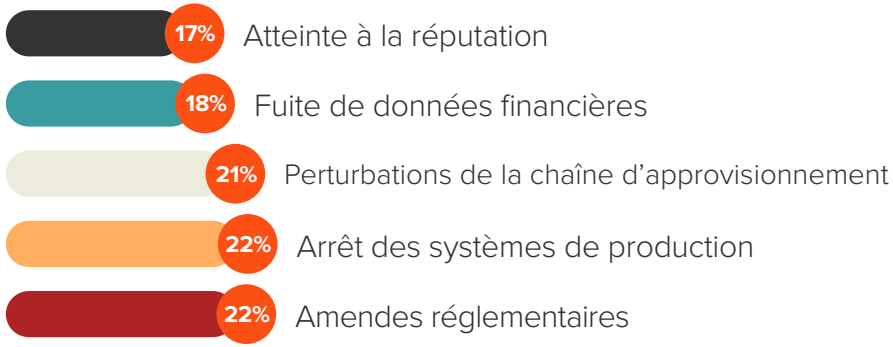
Pensez-vous que votre entreprise sera la cible d'une cyberattaque au cours des 12 prochains mois?



Principaux enseignements

Plus de la moitié des personnes interrogées (66 %) pensent que leur entreprise industrielle sera la cible d'une cyberattaque dans les 12 prochains mois. Cela montre bien que tant que la digitalisation se poursuivra, les pirates trouveront toujours de nouveaux moyens de cibler les systèmes de contrôle industriel, si bien que la sécurité devrait être une priorité élevée ou moyenne pour les entreprises à l'avenir.

Parmi les problématiques suivantes, quelles sont celles que vous souhaitez le plus atténuer grâce à des mesures de cybersécurité? (Veuillez en choisir deux)



Principaux enseignements

Les temps d'arrêt des systèmes de production (22 %) et les amendes réglementaires (22 %) sont les domaines les plus préoccupants pour les entreprises industrielles lorsqu'il s'agit de limiter les risques liés à la cybersécurité. Comme ces entreprises surveillent les projets et les risques associés, des outils de sécurité résistants seront essentiels pour renforcer les moyens de défense. Cela implique également que les budgets alloués à la sécurité seront probablement ajustés pour tenir compte de ces zones d'inquiétude.

Quest

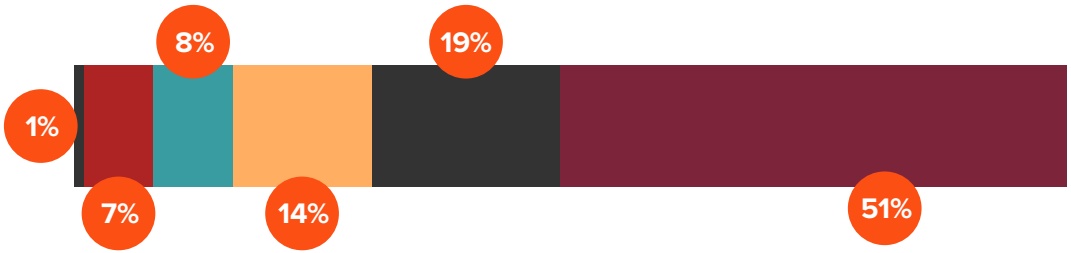
priorities

A Lynchpin Media BRAND

PARTIE 1:

Les défis de la cybersécurité dans le secteur industriel

A quelle fréquence examinez-vous les vulnérabilités et les possibilités d'attaque qui existent actuellement dans votre environnement Active Directory?



- Nous ne le faisons pas
- Je ne sais pas
- Chaque semaine
- Tous les ans
- Tous les mois 19
- Tous les 6 mois

Principaux enseignements

Plus de la moitié des personnes interrogées (51 %) déclarent que l'examen des vulnérabilités et des moyens d'attaque potentiels dans leur environnement Active Directory n'a lieu que deux fois par an. Seuls 19 % d'entre eux procèdent à des examens mensuels et 7 % à des examens hebdomadaires. Compte tenu de l'expansion rapide du paysage des menaces et de la façon dont les contrôles révèlent les pistes exploitables, il est fortement conseillé aux entreprises de recruter davantage de personnel de sécurité capable d'examiner et de protéger en permanence les actifs à fort enjeu.

Quest

priorities

A Lynchpin Media BRAND

PARTIE 1:

Les défis de la cybersécurité dans le secteur industriel

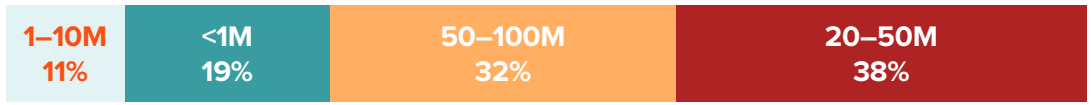
Si vous avez répondu “Nous ne le faisons pas” – Pourquoi ne procédez-vous pas actuellement à un contrôle?

- Manque d’expertise **50%**
- Manque de solutions et d’outils adéquats **50%**

Principaux enseignements

Le manque d’expertise (50 %) et l’absence d’outils et de solutions adéquats (50 %) sont les principales raisons pour lesquelles certaines entreprises industrielles n’examinent pas les vulnérabilités et les moyens d’attaque potentiels qui existent actuellement dans leur environnement Active Directory. Si la pénurie mondiale de professionnels cyber compétents et d’outils adéquats se poursuit, les entreprises auront de plus en plus de mal à gagner la bataille de la sécurité. Cela freinera clairement les progrès vers une protection adéquate et efficace dans le processus de production.

Quelle serait la perte de revenus estimée de votre entreprise si votre environnement Active Directory était compromis pendant 24 heures en dollars américains?



Principaux enseignements

Si l’environnement Active Directory d’une entreprise industrielle était compromis pendant 24 heures, 38 % de ces entreprises perdraient un chiffre d’affaires estimé entre 20 et 50 millions de dollars, tandis que 32 % subiraient une perte comprise entre 50 et 100 millions de dollars. À l’inverse, les entreprises qui seraient prêtes à adopter une approche plus proactive en matière d’investissement dans leur dispositif de sécurité pourraient économiser des millions. Il est également peu probable qu’un environnement Active Directory compromis ne dure que 24 heures. Cela signifie que l’investissement dans la sécurité n’est qu’une courbe ascendante et un mouvement stratégique dans la bonne direction pour permettre aux entreprises d’économiser davantage.

Quest

priorities

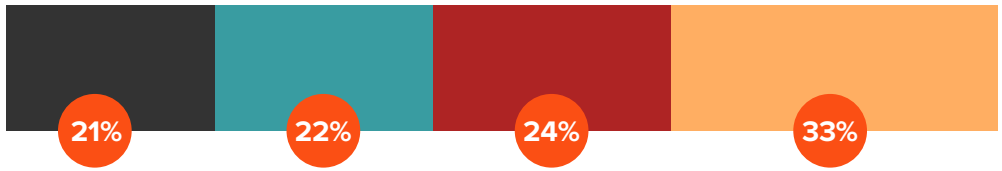
A Lynchpin Media BRAND

PARTIE 2:

Priorités et plans pour intégrer les nouvelles technologies, s'aligner sur les cadres de référence et combler les lacunes en matière de compétences

L'investissement et l'adaptation aux nouvelles technologies sont essentiels pour faire face à l'augmentation actuelle des attaques. Dans cette section, nous examinons les principales considérations des entreprises pour l'année à venir et leurs principales priorités.

Quelle est l'importance de la cybersécurité lors de la mise en place d'une nouvelle technologie?



- Nous pourrions envisager la cybersécurité, mais nous la considérons comme facultative dans la plupart des cas
- Nous ne la considérons pas comme importante
- Nous procédons toujours à un examen approfondi de la cybersécurité à chaque fois qu'une nouvelle technologie est adoptée
- Nous considérons que c'est important, mais dans la plupart des cas, nous faisons confiance à notre cybersécurité sans procéder à un examen plus approfondi

Principaux enseignements

Plus de la moitié des personnes interrogées (57 %) considèrent que la cybersécurité est importante lors de l'adoption d'une nouvelle technologie. Près d'un quart des personnes interrogées (24 %) déclarent qu'elles procèdent toujours à un contrôle de la cybersécurité à chaque fois qu'une nouvelle technologie est adoptée. Cela montre clairement que l'adoption de technologies innovantes est et sera toujours un élément critique pour permettre aux organisations de renforcer leur position en matière de sécurité. Nous constatons encore qu'une grande partie des entreprises font confiance à leur cybersécurité existante sans procéder à des vérifications supplémentaires, ce qui offre des opportunités aux vendeurs spécialisés dans la sécurisation de larges zones d'attaque liées à l'adoption de la technologie numérique.

Quest

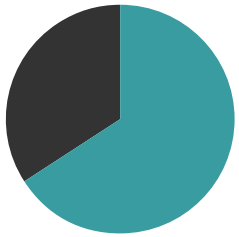
CXO priorities

A Lynchpin Media BRAND

PARTIE 2:

Priorités et plans pour intégrer les nouvelles technologies, s'aligner sur les cadres de référence et combler les lacunes en matière de compétences

Pensez-vous que les risques liés à la cybersécurité auront une incidence négative sur la vitesse d'adoption des nouvelles technologies dans votre entreprise?

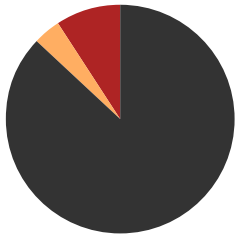


Oui à **66%** Non à **34%**

Principaux enseignements

Deux tiers des personnes interrogées (66 %) pensent que les risques potentiels liés à la cybersécurité auront un impact négatif sur la vitesse d'adoption des nouvelles technologies au sein de leur entreprise. Les entreprises doivent investir dans ces domaines pour protéger leurs réseaux et se préparer de manière adéquate à des situations de reprise après sinistre. Cela souligne la nécessité pour les fournisseurs de sécurité de mettre en œuvre ces plans de sécurité et d'aider ces entreprises à adopter les nouvelles technologies plus rapidement.

Vos mesures de cybersécurité sont-elles conformes au cadre du NIST?



Oui à **87%** Nous n'avons pas entendu parler du NIST **9%**

Non à **4%**

Principaux enseignements

L'écrasante majorité (87 %) déclare que leurs mesures de cybersécurité sont conformes au cadre du NIST. Sur le plan de l'informatique et de la cybersécurité, l'adhésion au cadre du NIST devrait être une priorité absolue pour les entreprises qui comprennent l'importance de la mise en conformité avec les réglementations. Les entreprises auront donc besoin de fournisseurs de sécurité capables de mener à bien la mise en œuvre de l'approche du cadre du NIST.

Quest

priorities

A Lynchpin Media BRAND

PARTIE 2:

Priorités et plans pour intégrer les nouvelles technologies, s'aligner sur les cadres de référence et combler les lacunes en matière de compétences

Au cours des 12 prochains mois, dans quelle mesure la mise en place d'un cadre de cybersécurité sera-t-elle une priorité pour votre entreprise?

- **Priorité moyenne.** Nous devons prendre des mesures pour améliorer notre niveau d'alignement, mais nous devons trouver un équilibre avec d'autres objectifs en matière de sécurité
- **Faible priorité.** Nous ne donnons pas la priorité à la mise en conformité de l'OT dans un cadre de cybersécurité
- **Priorité élevée.** Nous avons maintenant beaucoup plus d'appareils connectés et donc beaucoup plus de risques - atteindre un niveau élevé de conformité est devenu un objectif stratégique

Principaux enseignements

Plus de deux tiers des personnes interrogées (67 %) considèrent que la mise en place d'un cadre de cybersécurité pour leur organisation est une priorité moyenne à élevée. Cela suggère que les entreprises doivent investir dans des infrastructures stratégiques pour prendre en charge un écosystème d'appareils connectés en croissance constante et parvenir à un équilibre entre les objectifs stratégiques et les objectifs de sécurité. Cela montre que les entreprises recherchent des solutions de cybersécurité impartiales et supérieures et adoptent une stratégie de gestion des risques à long terme qui soutient leur positionnement en matière de sécurité.

Quest

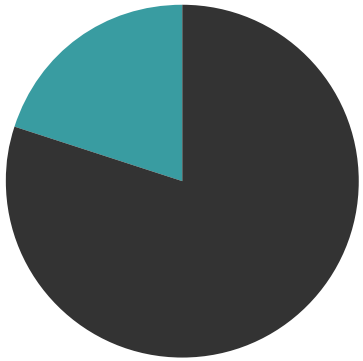
CXO priorities

A Lynchpin Media BRAND

PARTIE 2:

Priorités et plans pour intégrer les nouvelles technologies, s'aligner sur les cadres de référence et combler les lacunes en matière de compétences

La cybersécurité de votre entreprise a-t-elle été affectée par une pénurie de compétences?

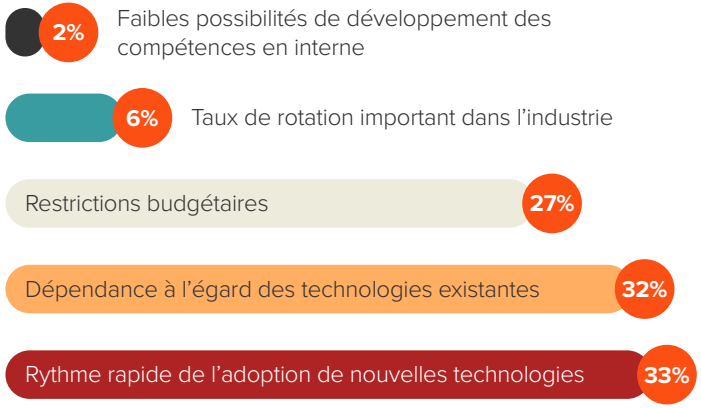


Oui à **80%** Non à **20%**

Principaux enseignements

Lorsqu'il s'agit de déterminer si la cybersécurité d'une organisation a été pénalisée par une pénurie de compétences, les quatre cinquièmes des personnes interrogées ont répondu par l'affirmative (80 %). Il est donc nécessaire de faire appel à un fournisseur de sécurité de confiance capable de mettre en œuvre une analyse des lacunes afin d'identifier les opportunités de croissance et d'établir des priorités en matière de ressources. Si l'on ne parvient pas à combler ce déficit de compétences, les dysfonctionnements sur le lieu de travail s'aggraveront, le personnel peinant à assumer leurs responsabilités et à accomplir les tâches qui leur sont confiées. La productivité étant au cœur des processus industriels, une analyse des lacunes en matière de compétences permettrait d'évaluer l'efficacité globale et d'être mieux placé pour faire face aux cyberattaques.

Quel est le plus grand défi auquel votre entreprise est confrontée en matière de déficit de compétences dans le domaine de la cybersécurité?



Principaux enseignements

Le rythme rapide d'adoption des nouvelles technologies (33 %) a été cité comme le plus grand problème de manque de compétences en cybersécurité pour les entreprises, suivi de près par la dépendance à l'égard des technologies existantes (27 %) et les restrictions budgétaires (27 %). Cela suggère que les entreprises devraient travailler avec des fournisseurs qui peuvent les aider à transmettre une culture de la sécurité qui optimise la mise en œuvre des nouvelles technologies et qui proposent des offres à des prix raisonnables. Les entreprises devraient envisager d'investir dans la formation à la cybersécurité et de mettre à jour les technologies existantes afin que chacun soit conscient des signaux d'alarme potentiels pour assurer la sécurité de ses données et de ses collègues.

CONCLUSION

La majorité des personnes interrogées ayant déclaré que la mise en conformité à un cadre de cybersécurité était une priorité moyenne à élevée pour leur entreprise au cours de l'année à venir, il n'y a pas de meilleur moment pour investir dans des fournisseurs de cybersécurité qui se concentrent sur la résilience à long terme et qui ont l'expertise nécessaire pour limiter les amendes réglementaires. Les conséquences d'une pénurie de compétences en cybersécurité peuvent être néfastes pour une entreprise, et étant donné que les menaces manquées sont la principale conséquence, il est impératif d'investir dans la formation. En outre, comme les entreprises souhaitent réduire leur champ d'attaque en raison de la mise en place de technologies numériques, c'est une excellente occasion pour les fournisseurs d'offrir une approche globale pour moderniser les environnements Active Directory et l'innovation. Cependant, étant donné qu'un pourcentage plus élevé de personnes interrogées pense que les risques de cybersécurité affecteront négativement la vitesse d'adoption des nouvelles technologies, les fournisseurs doivent proposer un prix confortable qui permette aux organisations d'en tirer le maximum d'avantages.

Un autre sujet de préoccupation est de s'assurer que les entreprises ont mis en place les mesures de protection appropriées pour lutter contre les pannes de système et les interruptions de la chaîne d'approvisionnement. Les résultats soulignent que les rançongiciels, les logiciels malveillants, l'hameçonnage et l'ingénierie sociale sont les principaux sujets de préoccupation des entreprises. En adoptant une approche à long terme et en recourant à un fournisseur de confiance pour les aider à mettre en place une stratégie proactive en matière de technologie et d'innovation, les entreprises peuvent s'engager sur la voie d'une meilleure cyber-résilience. Le secteur industriel est soumis à de nombreuses incertitudes et le fait d'avoir un fournisseur ayant une expertise en matière de reprise après sinistre constituerait un avantage significatif pour la mise en place d'une éthique de la sécurité à l'échelle de l'entreprise.

COMME LES ENTREPRISES SOUHAITENT RÉDUIRE LEUR CHAMP D'ATTAQUE EN RAISON DE L'ADOPTION DES TECHNOLOGIES NUMÉRIQUES, C'EST UNE EXCELLENTE OCCASION POUR LES FOURNISSEURS D'OFFRIR UNE APPROCHE GLOBALE DE LA MODERNISATION DES ENVIRONNEMENTS ACTIVE DIRECTORY ET DE L'INNOVATION.

Lynchpin Media est une société mondiale de services de médias technologiques, de données et de marketing. Nous aidons à sensibiliser, développer et cibler des comptes clés, et capter des informations clés sur les tendances régionales. Visite **lynchpinmedia.com** pour plus d'informations.

CxO Priorities, eine Lynchpin-Medienmarke

63/66 Hatton Garden
London, EC1N 8LE

En savoir plus: **www.cxopriorities.com**

Fondé par

Quest