



CIO.FOCUS

Les tops des bonnes pratiques des DSI américains pour éviter les flops

EN BREF

CIO France traduit régulièrement des articles en provenance de son homologue américain mettant en avant des listes de bonnes pratiques.

Ce CIO.Focus réalise une compilation de quelques uns de ces articles tirant des leçons des réalisations des DSI/ CIO américains.

Pour toute demande concernant CIO.focus :
contact-cio@it-news-info.com

Une publication de IT NEWS INFO :
40 bd Henri Sellier 92150 Suresnes

Rédacteur en chef :
Bertrand Lemaire
blemaire@it-news-info.com
Tél. : 01 41 97 62 10

Principaux associés :
Adthink Media et International Data
Group Inc.

Président et Directeur de publication :
Bertrand Gros

Directeur général : Jean Royné

Président du groupe Adthink Media :
Sylvain Morel

CIO est édité par IT NEWS INFO,
SAS au capital de 3000000 €

Siret : 500034574 00029 RCS Nanterre

SOMMAIRE

/ STRATÉGIE

Douze mauvaises habitudes qui ralentissent la DSI **3**

/ PROJETS

Les dix étapes à franchir pour un DSI nouvellement nommé **10**

/ PROJETS

Les 8 plus grandes erreurs commises par les DSI... **14**

/ STRATÉGIE

Les 5 meilleurs cas d'utilisation de l'apprentissage automatique pour la sécurité **19**

/ TECHNOLOGIES

Ces 9 compétences Legacy qui sont toujours très demandées **22**

/ STRATÉGIE

Les 12 plus grands problèmes auxquels doit faire face une DSI **25**



/STRATÉGIE

Douze mauvaises habitudes qui ralentissent la DSI

Les goulots d'étranglement semblent toujours nés des meilleures intentions, mais ils doivent être supprimés. De la gouvernance à l'approvisionnement manuel, voici ce qui affecte la capacité de votre organisation informatique à produire des résultats efficaces selon CIO Etats-Unis.

All est temps de faire face à un fait incontestable : votre DSI est trop lente. C'est le résultat de bonnes intentions qui ont mal tourné. Mais, dans la vie des entreprises, les intentions n'ont pas d'importance.

Quand la DSI est-elle trop lente ? Chaque fois qu'une partie de l'entreprise doit attendre l'informatique pour réaliser ce qu'elle doit faire. De nos jours, un slogan récurrent est « le délai de valorisation », mais ce qui est vraiment important, c'est « être en avance sur vos concurrents ».

Si l'informatique vous en empêche, vous pouvez parier que les dirigeants de votre entreprise sont en train de perdre patience à l'égard de la DSI.

Vous voulez accélérer votre DSI ? Commencez par vous débarrasser de ce qui la ralentit, c'est à dire ses goulots d'étranglement. En voici une douzaine pour commencer. Ignorez les votre à vos risques et périls.



1 La gouvernance

Les comités directeurs constituent une forme ancienne de gouvernance. Au fur et à mesure que la gouvernance établit le rythme de tout ce que fait la DSI, et que les comités ralentissent tout ce qu'ils touchent, faire des réunions de comités la pièce maîtresse de la gouvernance IT est suicidaire, quoique vous fassiez par ailleurs.

Commencez par la taille des dits comités. Tout membre supplémentaire ralentit les décisions d'un comité. Plus de cinq membres et l'avancement des travaux ralentit démesurément et la possibilité d'un consensus disparaît entièrement.

C'est pire si les membres du comité se considèrent eux-mêmes non pas comme des responsables informatiques mais comme des délégués d'un service qui, sans eux, n'obtiendrait pas ce à quoi il a droit. Ce genre de comité se disputera éternellement au lieu de résoudre les problèmes communs.

Ensuite, il y a le calendrier des réunions. C'est le métronome qui marque le rythme de chaque projet que le comité gouverne. Si un comité se réunit tous les mois, tout ce qui attend une décision attend un mois. Combien de projets avez-vous en cours qui pourraient se poursuivre avec un goulot d'étranglement comme celui-là ?

Comment résoudre ce problème ? Adoptez la culture de la nouvelle gouvernance. Considérez la gouvernance comme des marqueurs et reléguez les comités à un rôle de garde-fous. Ces comités peuvent empêcher des catastrophes, mais seulement en dernier recours. Laissez la culture de la gouvernance assurer l'essentiel du pilotage. Si chacun est capable d'appréhender ce qui est important et sait se focaliser dessus, l'essentiel de la gouvernance formelle devient superflue.

2 La multiplication des tâches

Il existe une règle simple pour la multiplication des tâches confiées à vos collaborateurs : ne le faites pas !

Ceci est particulièrement vrai pour les projets de développement de logiciels, où les études suggèrent que chaque interruption coûte 15 minutes de productivité perdue. Mais ce qui est vrai pour le développement d'applications est également vrai pour toutes les autres situations où les informaticiens doivent se concentrer.

Le défi à relever n'est pas de savoir que vous devez éviter la multiplication des tâches. C'est savoir comment l'éviter. La réponse réside dans la planification. Il devrait y avoir une règle inviolable : tous les projets doivent disposer de leur équipe complète ou ils ne peuvent pas être lancés.

Qu'est-ce qu'un projet avec une équipe complète ? Celui où aucune tâche n'attend jamais qu'un membre de l'équipe soit disponible pour être réalisée. Limiter le nombre de projets simultanés au nombre qui peuvent disposer d'équipes complètes permettra qu'aucun membre de l'équipe ne soit chargé simultanément de plusieurs tâches.

Le résultat, c'est que non seulement chaque projet sera achevé plus rapidement, mais aussi que l'ensemble du portefeuille de projets se terminera plus rapidement.



3 Les projets

Traditionnellement, les organisations implante de nouvelles technologies dans le cadre de projets. Plus le design est complexe, plus le projet est grand. Mais au fur et à mesure que les projets croissent, le risque d'échec augmente géométriquement, alors que la probabilité d'un délai important se rapproche de la certitude.

Essayez plutôt, autant que possible, de mettre en oeuvre des versions successives au lieu de nouveaux projets indépendants. Chaque version permet des améliorations limitées aux impacts moins lourds en termes de risques de régression, de stress-tests de déploiement. Choisir des avancées par versions successives permet de vérifier l'un des truismes de la gestion informatique : les améliorations réussissent, les projets échouent.

Soit dit en passant, si vous optez pour cette manière de faire, vous ne devez pas décrire cela comme une révolution. Vous pouvez appeler cela Scrum et enthousiasmer toute l'entreprise.

Ne vous arrêtez pas là. L'organisation du travail de développement en versions crée encore des retards. Les sprints de Scrum typiques sont d'une durée d'un mois, ce qui établit un rythme mensuel pour les évolutions de l'entreprise, sans compter qu'il faut souvent aussi attendre une réunion d'un comité de gouvernance ou de gestion du changement.

Ensuite, allez jusqu'à l'intégration et au déploiement continus - en un mot, DevOps. Automatiser les tests, subordonner chaque changement de logiciel à une intégration continue et mettre chaque petit changement en production immédiatement. Avec des changements aussi petits, attendre un feu vert d'un comité quelconque est superflu.

Après tout, nous avons dépassé le temps où une virgule mal placée ferait exploser quelque chose.

4 Provisionnement manuel

Les équipes de développement peuvent disposer d'un environnement complet dans le cloud en quelques minutes - ou ils peuvent demander à la production informatique le même environnement et l'obtenir en quelques mois.

Ce n'est pas une limitation intrinsèque. C'est un choix. Comme les minutes sont plus courtes que des mois, et comme les fournisseurs de cloud public ont déjà perfectionné la technologie nécessaire, le meilleur choix est clair.

Commencez à automatiser et à habiller vos développeurs à gérer leurs provisionnements.



5 Favoriser les interfaces par rapport à l'intégration

Les nouvelles fonctionnalités créent de nouvelles valeurs. Mais dans la plupart des DSI, la nouvelle fonctionnalité est prise avec recul pour s'assurer qu'un changement de logiciel ne brise pas le plat de spaghettis des interfaces point à point réalisées sur mesure.

Nettoyez l'enchevêtrement d'interfaces et adoptez donc un système d'intégration bien conçu. De cette façon, les équipes projet pourront accélérer, les tests prendront moins de temps et les déploiements seront plus faciles.

Ensuite, essayez d'aller un peu plus loin : remplacez « Technologies de l'information » par « Systèmes d'intégration ». Celui-ci vise à offrir un accès fiable au portefeuille d'applications de l'entreprise via des API standards qui exposent les données et les fonctionnalités en tant que services sécurisés et bien définis.

6 Suppression de l'IT officieuse

Le Shadow IT -les systèmes déployés par les métiers sans avis de la DSI- provoque des problèmes. En particulier, avec cette IT officieuse, les îlots d'automatisme construits sur des bases médiocres sont la règle, et non l'exception.

Mais l'IT officieuse fait sans relâche ce que les métiers ont besoin. Et elle n'a pas à attendre un feu vert dans le cadre du processus de gouvernance IT, donc non seulement elle fournit ce dont les métiers ont besoin mais elle le fournit immédiatement. Regardez le shadow IT comme une source gratuite d'applications externalisées brillamment développées mais avec une architecture déplorable.

Eclairez sur l'IT de l'ombre. Donnez-lui un peu de soutien au lieu d'essayer de l'éliminer. En échange, vous multipliez votre capacité d'action, même après avoir pris en compte l'effort requis pour l'intégrer à votre SI.

Si vous avez transformé votre SI en système intégré, vous pouvez également mettre les API à la disposition du Shadow IT de l'entreprise, en résolvant du même coup les problèmes des îlots d'automatisation.



7 Exiger des solutions à 100 %

L'instinct de l'informatique est d'éprouver tout. Mais développer une sécurité pour un cas qui frappe le système une fois toutes les mille transactions prend autant que d'en développer une pour un cas qui se produit des centaines de fois par jour.

Tirez une leçon des premiers temps de l'informatique : programmez pour les cas généraux et laissez le reste comme des exceptions à traiter manuellement.

Les ordinateurs sont bons dans les cas généraux.
Les humains sont bons pour gérer des exceptions.

8 Création d'entrepôts de données

Choisissez un mot pour qualifier le projet d'entrepôt de données typique et il est probable que ce sera « en retard ».

D'accord, il y a deux mots. Mais les entrepôts de données sont encore chroniquement en retard en raison de la difficulté de concevoir des structures de données OLAP optimisées pour répondre à des questions que personne ne connaît à l'heure actuelle.

Entrez dans l'ère NoSQL. Ce qui rend le NoSQL intéressant, ce n'est pas seulement sa capacité à gérer de gros volumes de données. Encore plus important est sa capacité à accepter des données maintenant et laisser les analystes choisir leur structuration plus tard, quand viendra le temps de les interroger.

C'est cette qualité de « schéma à la demande » qui permet à Hadoop d'être mis en oeuvre bien plus rapidement que des entrepôts de données traditionnels.



9 Mettre l'accent sur le TCO

Vos décideurs oublient-ils que les coûts génèrent des avantages ? N'importe quel décideur lambda peut réduire les coûts. La difficulté consiste à réduire les coûts sans compromettre la mise en oeuvre. C'est là que le coût total de possession (TCO) entre en jeu et pas dans le bon sens.

Le TCO ne se soucie pas de la fonctionnalité, sauf pour la limiter. Après tout, la façon la plus simple de réduire les coûts est de fournir et de maintenir des fonctionnalités moins développées. Moins d'utilisation, c'est un coût inférieur.

C'est ce qui se produira inévitablement avec un accent sur le TCO en raison de l'une des règles inviolables de la mesure : tout ce que vous ne mesurez pas, vous ne l'obtenez pas. Cela inclut la valeur de ce que la DSI réalise.

En outre, si l'accent est mis sur la réduction des coûts, personne ne se concentre sur l'accélération des choses. Si la vitesse n'est pas une priorité, la vitesse n'existera pas.

10 Obliger les innovateurs à adopter une architecture informatique « haute fidélité »

Les entreprises avaient l'habitude de tout faire pour être les mêmes demain qu'elles l'étaient hier. Elles ont exigé des systèmes parfaitement fiables, de « haute fidélité » qui n'ont jamais perdu de données et ont toujours donné la bonne réponse.

Mais, désormais, l'innovation importe autant que la fiabilité. C'est l'avenir car c'est là que l'avantage concurrentiel se produit.

Ne forcez pas les innovateurs - par exemple, les responsables de Shadow IT - à entrer dans l'architecture informatique « haute fidélité ». Offrez aux innovateurs un espace fermé qu'ils peuvent gérer par eux-mêmes afin qu'ils comprennent ce qui fait avancer vers le futur. Beaucoup de temps doit passer pour que leurs innovations soient de haute-fidélité alors qu'elles réussissent déjà dès leur démarrage.



11 Permettre une culture de complaisance

Même les DSI bien gérées peuvent être obsolètes, en particulier dans les entreprises qui responsabilisent les collaborateurs lorsqu'on essaie quelque chose d'innovant et que cela n'est pas valoriser, au lieu de les féliciter pour prendre le risque.

Une culture de complaisance ralentit les mises en production parce que personne ne voit le besoin de les accélérer. Après tout, c'est ainsi que nous avons toujours fait des choses ici.

Si c'est la culture que vous avez, secouez votre entreprise. L'alternative est la mort par l'ennui.

12 Établissement d'une relation métiers / informatique sans lien de dépendance

Selon vous, qu'est-ce qui donnera des résultats plus rapidement ? Une longue démarche, où l'IT « négocie » les accords de niveau de service tout en exigeant que ses « clients » internes « s'inscrivent dans ses exigences et spécifications » ou des conversations informelles qui commencent par « Qu'est-ce que vous essayez d'accomplir et comment pouvons-nous vous aider ? »

De nombreux experts appellent l'approche formelle « meilleures pratiques ». Ignorons-les. Adoptez une vraie meilleure pratique : favoriser de solides relations informelles et ne jamais négocier. Pourquoi ? Parce que la négociation est pour les gens qui sont assis sur des côtés opposés de la table de négociation. Or, en théorie, l'informatique et le reste de l'entreprise sont du même côté, n'est-ce pas ?



UN ARTICLE RÉDIGÉ PAR

La rédaction de CIO Etats-Unis



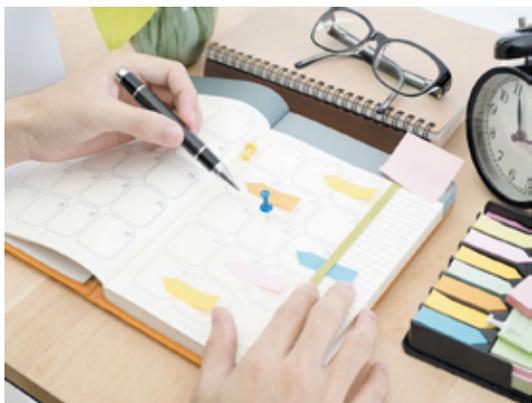
/ STRATÉGIE

Les dix étapes à franchir pour un DSI nouvellement nommé

Ce qu'accomplit un DSI lors de ses six premiers mois d'activité est essentiel et tient en dix étapes selon Deloitte.

La durée de vie moyenne d'un DSI à son poste est d'environ quatre ans. L'évolution des besoins de l'entreprise et l'insatisfaction à son égard suggèrent que le calendrier ne changera pas dans l'immédiat. Les DSI qui rejoignent une nouvelle entreprise font face à un certain nombre d'obstacles. « Le rôle décisif de la technologie dans la conduite des entreprises signifie que de nombreux DSI doivent l'utiliser pour accélérer la croissance de l'entreprise », déclare Khalid Kark, directeur de recherche du programme CIO de Deloitte. « *Les entreprises ne cherchent pas seulement des experts de la technologie, mais des experts des marchés de l'entreprise, aptes à inspirer l'organisation informatique et à développer une culture de la performance* ».

Les transitions sont particulièrement difficiles parce que les entreprises intéressées s'attendent à voir les nouveaux DSI se plonger directement dans la stratégie commerciale. Dans la réalité, ils doivent souvent passer des mois à mettre de l'ordre dans l'informatique. En outre, certains dirigeants commerciaux prennent du temps pour occuper les postes vacants de DSI parce qu'ils veulent s'assurer que les candidats s'intègrent parfaitement dans la culture de l'entreprise. Adobe Systems, par exemple, a mis sept mois pour trouver un DSI, ce qui oblige celle-ci, Cynthia Stoddard, à refaire toute l'identité de l'informatique. Deloitte préconise, après avoir aidé deux cents CIO à entrer dans leur nouveau rôle, une liste de dix étapes à franchir dans cette transition cruciale.



1. Soyez vigilant sur votre agenda

A ce niveau de responsabilité, il faut décider des priorités initiales et les recalibrer constamment en fonction des attentes de l'entreprise. Il suffit de savoir que vous avez très peu de temps pour vous imposer. Donc, ce que vous faites au cours des six à neuf premiers mois est absolument critique. « *Au bout de six mois, vous devriez fournir un programme de changement, et si vous ne l'avez pas construit, cela vous mettra en situation d'échec car les attentes sont très élevées* », souligne Khalid Kark.



2. Faites adhérer votre équipe

Les transitions sont pleines d'incertitudes, de sorte que vous êtes obligé de rencontrer une certaine paralysie opérationnelle. Pour l'éviter, il faut expliquer votre vision stratégique à des membres clés et performants de votre équipe. Essayez de savoir s'ils adhèrent à votre plan. Des décisions difficiles devront être prises ultérieurement.



3. Évaluer les talents

Faites le point sur vos compétences, celles des membres clés de votre équipe, et voyez si elles correspondent à la culture que vous souhaitez créer. Si vous passez trop de temps à l'exécution, vous devrez peut-être reconfigurer votre équipe, réaligner les effectifs, ajouter de nouveaux talents et éliminer les pôles de décision disséminés.



4. Identifiez les lieutenants de confiance

La réorganisation de vos équipes de direction IT peut inspirer une nouvelle réflexion et réinitialiser les attentes en matière de performance. De plus, si vos adjoints ont joué un rôle avant votre arrivée, vous devrez peut-être les remplacer ou courir le risque qu'ils ne vous suivent pas. Mais, dans tous les cas de figure, vous ne pouvez pas ne pas tenir compte de l'état d'esprit de votre équipe de direction.



5. Etre aligné sur le business

Quand il restait un îlot, ce que votre patron pensait de votre département n'avait pas une grande incidence. Ce n'est plus le cas, vous devez rencontrer les acteurs clés du développement commercial, pour connaître leurs préoccupations et les aborder avec eux. La manière de s'engager et l'empathie entre les parties prenantes pourrait permettre d'engager des partenariats clés sur le terrain. « Être capable de comprendre comment vous vous engagez avec les différents acteurs du développement commercial devient beaucoup plus important que d'avoir une compétence technique », note Khalid Kark.



6. Connectez-vous avec les clients, les partenaires et les fournisseurs

Votre temps passe beaucoup dans les fonctions de back-office. À l'ère du numérique, vous devez vous concentrer davantage sur la relation client. La connexion avec le reste des parties prenantes dans la chaîne de valeur indique que vous êtes plus qu'un facilitateur. Elle vous aidera également à évaluer correctement le rôle de la technologie dans la valorisation. « On s'attendait à ce que vous restiez à l'extérieur il y a cinq ou huit ans, mais maintenant, il existe une pression pour que vous soyez investi dans la dynamique du marché ».



7. Faites vos preuves rapidement

Démontrer votre compétence en tant que leader informatique peut vous aider à gagner rapidement la confiance. Par exemple, un DSI, client de Deloitte, a mis en place un nouveau réseau sans fil à l'échelle de l'entreprise en quelques mois, résolvant les problèmes de connectivité qui rendaient depuis longtemps les employés très frustrés.



8. Obtenez des gains rapidement

Un nouveau réseau sans fil c'est sympa, mais il ne vous apportera que de la bonne volonté. Si vous abordez la question des systèmes informatiques défectueux et des projets bloqués avec une répercussion élevée parmi les acteurs de l'entreprise, c'est d'une autre dimension. Le report des décisions architecturales ou des dépenses importantes pèse sur l'entreprise. « *Vous devez baisser la tête et vous assurer que les choses de base fonctionnent efficacement et que les bonnes personnes sont aux bons endroits* ».



9. Prioriser la demande et l'offre IT

Utilisez ces premiers efforts pour évaluer votre arriéré de projet informatique et pour prioriser les prochaines étapes. Découvrez vos besoins en ressources. La solution sera-t-elle mieux livrée dans vos locaux ou via les services en cloud ? Vous devez travailler avec des partenaires commerciaux pour créer un processus de gouvernance, aligner la livraison des projets avec les besoins de l'entreprise. Deux semaines après son arrivée, un DSI interrogé par Deloitte avait découvert 1300 projets en cours, dont la plupart en retard ou en dépassement budgétaire. C'est un bon point de départ pour un échec catastrophique en informatique, souligne avec ironie Khalid Klark.



10. Savoir déléguer pour devenir un bon stratège

Les chefs d'entreprise veulent que leurs nouveaux DSI réorganisent la culture de l'informatique et revitalisent les talents pour se concentrer sur la stratégie. Mais le DSI peut très vite se retrouver à passer l'essentiel de son temps à débloquer et à résoudre les problèmes informatiques de base. Un distributeur mondial a embauché son nouveau DSI pour revitaliser les équipes IT et créer une nouvelle vision stratégique pour l'informatique. Quelques jours seulement après son arrivée, les pannes massives dans le système de points de vente de l'entreprise ont causé des ravages sur l'entreprise. S'il arrive à réduire la quantité de temps passé à résoudre les problèmes, en identifiant les compétences clés pour assumer cette responsabilité à sa place, cela lui permettra de faire évoluer la stratégie plus rapidement.



UN ARTICLE RÉDIGÉ PAR
IDG News Service



/ PROJETS

Les 8 plus grandes erreurs commises par les DSI

Pour les DSI, les retombées d'une gaffe stratégique peuvent être désastreuses pour eux-mêmes ou pour leur entreprise.

Tout le monde fait des erreurs. La plupart sont inoffensives, certaines sont embarrassants mais pardonnables, d'autres peuvent nuire à votre carrière, voire à votre entreprise. Certaines des gaffes informatiques les plus courantes comprennent le fait d'être coincé avec un fournisseur, de ne pouvoir se débarrasser de quelqu'un, embaucher ou promouvoir les bonnes personnes, et enfin cacher les problèmes à la direction, jusqu'à ce qu'il soit trop tard pour se rattraper. Voici les plus grandes erreurs que vous êtes susceptible de faire, et comment les éviter ou vous récupérer rapidement.

Erreur n°1 : le fournisseur mal verrouillé

C'est une forme de séduction. Les fournisseurs vous attirent avec des prix bas et des promesses sans fin. Mais une fois qu'ils vous ont fait signer, ils ne vous lâchent plus. « Une fois implantés, ils essaient de s'étendre dans votre environnement », explique Andrew Howard, directeur de la technologie chez Kudelski Security.

« Tout commence par de bonnes intentions, mais le fournisseur finit par disposer d'un contrôle significatif sur les actifs informatiques et d'un effet de levier considérable sur les prix. J'ai vu plusieurs responsables informatiques perdre leur emploi sur ce type de mauvaise gestion ».

Andrew Howard reconnaît qu'il y a aussi des avantages. Mis à part les remises sur volume, obtenir plusieurs produits du même fournisseur devrait assurer une meilleure intégration entre eux ainsi qu'une sécurité plus stricte. Et moins de fournisseurs à traiter. Cela peut être idéal pour les petites organisations. Mais quand vous décidez de changer, ne vous attendez pas à ce que le fournisseur vous aide. Andrew Howard se souvient quand il travaillait dans une société de conseil, d'un fournisseur de gestion de workflow qui a essayé d'empêcher sa société de passer à un autre fournisseur en refusant de remettre son code source. Cette exigence, qui figurait dans l'accord de licence de logiciel (SLA) original, a réussi à s'évaporer dans les négociations ultérieures.

« Beaucoup de nos partenaires rencontrent le même genre de problèmes avec les fournisseurs de plateformes cloud. Une fois que vous en avez une, il est difficile de faire passer l'infrastructure chez un concurrent ». Pour cette raison, de nombreux DSI passent par plusieurs fournisseurs de cloud. Les responsables informatiques doivent également travailler plus étroitement avec les achats pour éviter de devenir trop dépendants d'un seul fournisseur.

Erreur n° 2 : traiter le cloud comme une extension du centre de données

En février 2016, Best Egg Personal Loans (prêt et réduction de dettes) a migré d'un cloud privé basé sur VMware vers un cloud public fonctionnant sur Amazon Web Services. La société avait passé des mois à planifier, configurer et migrer des services de faible niveau. Tout était prêt à basculer. Mais, deux heures après son lancement, un serveur AWS critique est mort.

« *Le réveil fut brutal* », explique Brian Conneen, DSI de Best Egg, « *la stabilité d'un serveur cloud unique est inférieure à celle d'un serveur ou d'une machine virtuelle gérés en interne* ».

La disponibilité de 99,999% du cloud provient de la possibilité de provisionner de nouveaux serveurs pour remplacer ceux qui ont échoué. Le crash s'est produit pendant un week-end, et Best Egg a pu effectuer une récupération sans interruption de service, mais Brian Conneen avait subi une leçon précieuse : vous ne pouvez pas traiter un serveur cloud comme s'il s'agissait d'une autre machine de votre centre de données.

Après cela, la priorité de Best Egg était de s'assurer qu'il était vraiment optimisé pour un environnement cloud, il devait aussi surveiller de près les coûts du cloud. Brian Conneen a également appris que les serveurs sont jetables. Quand ils tombent, vous les jetez. Best Egg a dû construire beaucoup plus de redondance, assigner un pool de serveurs à des systèmes qui ne pouvaient pas se permettre un temps d'arrêt et créer des scripts qui génèrent automatiquement de nouveaux serveurs. Maintenant, lorsque Best Egg publie une nouvelle version du logiciel, il construit simplement de nouveaux serveurs, leur envoie le code et fait défiler les anciens.

« *Les avantages du cloud public ne peuvent être atteints que lorsque vous concevez votre infrastructure en fonction des atouts du cloud public* », explique-t-il. « *La simple migration de vos serveurs vers le cloud ne suffit pas, vous devez également migrer votre réflexion et votre approche* ».



Erreur n° 3 : sur estimer l'analyse de rentabilité

Cela a longtemps fait partie des cerveaux des DSI et même de leur cortex cérébral : pour obtenir une approbation pour une grosse dépense informatique, il faut avoir une solide analyse de rentabilité. Les DSI peuvent donc passer des semaines à rechercher des options, à calculer des hypothèses et à assembler des powerpoints.

« *C'est souvent pour rien* », dit Mark Settle, DSI d'Okta, un ISP. « *Il y a plusieurs années, j'étais interviewé par CIO et donnait une mini-conférence aux directeurs financiers sur l'importance des analyses de rentabilité. Le directeur financier m'a dit qu'il ne croyait pas aux chiffres issus de mes analyses de rentabilité, et n'approuve les principales initiatives informatiques que lorsque le Pdg lui-même donne son feu vert* ».

Les dépenses nécessaires en matière d'infrastructure ou de conformité sont des exceptions, ajoute Mark Settle. Mais gagner la confiance signifie non seulement faire votre travail informatique en toute transparence, mais également travailler en partenariat avec d'autres équipes au sein de l'organisation, en tenant compte de leurs processus existants et en les améliorant. Faites-le, et les Pdg seront beaucoup plus enclins à écouter vos idées lorsqu'une opportunité stratégique se présente.

« *Si vous présentez trop d'analyses où la rentabilité est surestimée, sans que les autres membres du Comex soient prêts à se battre pour vous, vous rendez les choses beaucoup plus difficiles pour vous* ».



Erreur n° 4 : embaucher à un niveau trop bas de compétence

Il faut une équipe pour bâtir une entreprise prospère, mais il suffit d'un employé incompetent pour faire chuter tout le monde. « *La plus grande erreur des responsables informatiques est d'embaucher des gens qui ne sont pas plus intelligents et meilleurs qu'eux* », explique Derek Johnson, vice-président du développement commercial de la firme de recrutement Stride Search.

Malheureusement, les egos des DSI les empêchent souvent de choisir la bonne personne. Par exemple, il y a trois ans, Stride Search avait identifié l'ingénieur réseau et logiciel idéal pour l'un de ses clients, une startup dans le SaaS. Il était éloquent, charismatique, avait un doctorat en informatique et possédait plusieurs brevets. Tout le monde l'aimait, sauf le CTO de la startup. « *L'entrevue téléphonique s'est bien passée, mais l'entrevue en face-à-face a été un désastre absolu* », a déclaré M. Johnson. « *Le CTO, qui était à la fois cofondateur et responsable de l'embauche, a passé toute l'entrevue à insulter le candidat, mais le reste de l'équipe de direction a voulu faire une offre, mais le CTO a refusé. Finalement, le candidat est parti travailler pour un concurrent, qui a plus tard écrasé cette start-up, ce qui arrive si souvent que cela pourrait être une parabole* ».

Les entreprises peuvent lutter contre ce problème en exigeant qu'aucune personne n'ait le pouvoir d'opposer son veto à une embauche. Pour les postes supérieurs, le conseil d'administration d'une société et les subordonnés du candidat doivent également être impliqués.

« *Le fameux dicton : un joueur A recrute des joueurs A, alors que les joueurs B embauchent des joueurs C, fonctionne à plein. Il n'y a rien de plus catastrophique pour une organisation que d'engager la mauvaise personne à un poste clé, ou de passer à côté du bon profil* ».

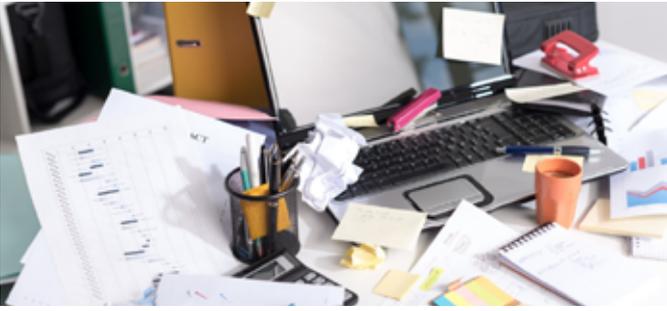
Erreur n° 5 : promouvoir le mauvais candidat interne

Si le fait de ne pas embaucher la bonne personne à l'extérieur est une erreur, la promotion du mauvais candidat interne l'est tout autant. De manière générale, la promotion interne est une excellente politique, note Giancarlo Di Vece, président d'Unosquare, un éditeur de logiciels informatiques. Mais vous devez le faire pour les bonnes raisons.

Les mauvaises ? Promouvoir quelqu'un pour le récompenser d'être un employé loyal. Cela peut mal tourner, surtout si l'employé n'est pas vraiment adapté pour le nouvel emploi. « *J'ai vu des directeurs informatiques faire d'un bon développeur un leader technologique, mais ensuite ce promu est devenu frustré et a fini par abandonner. Vous pensez que vous êtes un bon patron en donnant aux gens l'opportunité de grimper, et vous finissez par les perdre parce que vous les avez éloignés de ce qu'ils aimaient vraiment faire !* »

Giancarlo Di Vece dit que cela lui est arrivé il y a environ un an. Il avait embauché un développeur et l'avait mis sur la voie d'une promotion rapide. Bientôt, le développeur a dirigé une équipe de cinq personnes. Tout s'est bien passé pendant trois mois, jusqu'au jour où il est entré dans le bureau de Di Vece et a démissionné. Même si le travail de l'équipe était excellent, le développeur a estimé qu'il avait échoué dans son travail et ne pouvait revenir à l'ancien.

« *J'ai perdu une fantastique ressource de programmation en lui fournissant une promotion rapide* », depuis lors, Di Vece dit qu'il a mis en place un cadre où les candidats nouvellement promus peuvent fournir et recevoir des commentaires réguliers, et les superviseurs peuvent garder un œil sur ce qu'ils font pour les aider à réussir. La promotion interne est une bonne philosophie, mais ce n'est pas le bon choix dans tous les cas.



Erreur n° 6 : appliquer la méthodologie agile aux systèmes de base

Avec l'explosion des services de cloud computing et les demandes croissantes en termes de rapidité, les DSI comprennent qu'une grande partie de l'informatique est hors de leur contrôle. Mais les mêmes mécanismes de prestation souples qui permettent aux entreprises de placer des conteneurs Docker et des micro-services dans le cloud peuvent avoir un impact désastreux sur la base des systèmes informatiques qui sont de la responsabilité du DSI, par exemple : messagerie, téléphonie, ERP et back-office des applications, explique Andrew Howard de Kudelski.

« J'ai vu plus de DSI perdre leur emploi parce qu'ils ne pouvaient pas assurer le fonctionnement de la messagerie, que pour tout autre motif. Les méthodologies agiles vont souvent à l'encontre d'un contrôle des changements rigoureux qui sont nécessaires pour les systèmes de base. S'ils tombent en panne, les entreprises peuvent perdre de l'argent rapidement ».

Pour atténuer ce problème, les DSI doivent établir de solides limites, permettre des changements agiles sur les systèmes métier et imposant un contrôle des changements plus rigoureux sur les systèmes principaux.

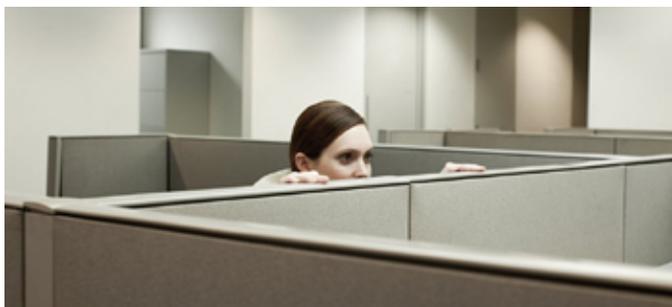
Erreur n° 7 : dire trop souvent « oui »

Les meilleurs responsables informatiques sont souvent accusés de dire « non » à l'innovation. Mais un problème plus grave survient quand ils ne savent pas comment affronter les gens, et risquent de perdre le contrôle sur la sécurité de leurs systèmes, explique Richard Henderson, stratège mondial en sécurité informatique chez Absolute.

« Combien de fois les informaticiens ou les responsables de la sécurité ont-ils reçu un appel de quelqu'un de haut placé exigeant l'accès à quelque chose de risqué ? À quelle fréquence les unités commerciales déploient-elles un nouvel outil ou un service cloud inédit sans vérification appropriée ni approbation des équipes informatiques ou de sécurité ? »

Selon Richard Henderson, des outils comme le stockage dans le cloud et les solutions en SaaS peuvent offrir d'énormes avantages aux équipes. Mais lorsque les responsables informatiques approuvent systématiquement les demandes exceptionnelles, ils créent de nouveaux angles morts dans leur organisation et, potentiellement, de nouvelles vulnérabilités.

Il est difficile de dire « non » à son PDG, mais vous devez avoir un plan en place pour faire face aux exceptions. Un solide système de gestion des actifs est essentiel, de même qu'un logiciel qui surveille les périphériques d'extrémité et vous alerte lorsque les utilisateurs se connectent à des services cloud communs. *« Dire oui trop souvent, rend impossible le maintien des actifs en conformité, surtout si vous n'êtes pas dans la boucle quand quelqu'un du marketing crée une nouvelle instance AWS. »*



Erreur n° 8 : cacher les problèmes (à son patron)

Quand un grand projet commence à battre de l'aile, beaucoup de responsables informatiques tentent de l'enterrer, espérant le réparer avant que les patrons ne s'en aperçoivent, explique Mark Settle d'Okta. Les choses vont en fait s'aggraver. Au moment où ils finissent par admettre que la nouvelle version du code a amené une interruption de 48 heures, ou qu'ils ont besoin de 4 millions de dollars supplémentaires pour terminer leur projet, ils ont perdu leur crédibilité.

« Plus tôt vous exposerez les mauvaises nouvelles et mieux ce sera. Les mauvaises nouvelles ne s'améliorent jamais d'elles-mêmes et plus tôt les gens commenceront à s'en occuper, et plus vous aurez de chances de récupérer le projet et de revenir sur la bonne voie. Fournir de mauvaises nouvelles n'est jamais facile, mais ce sera le cas si vous avez établi et maintenu une bonne relation de travail avec votre boss ».

Les DSI doivent créer des occasions de discuter avec le directeur financier et d'autres membres de la direction lorsqu'ils ne sont pas en mode crise. Ce n'est pas toujours facile pour les gens axés sur la technologie, mais ce sont des compétences dont ils ont besoin pour avancer.



UN ARTICLE RÉDIGÉ PAR

Dan Tynan / IDG News Service

(traduit et adapté par Didier Barathon)



/ TECHNOLOGIES

Les 5 meilleurs cas d'utilisation de l'apprentissage automatique pour la sécurité

L'apprentissage automatique pourrait aussi être la meilleure réponse à la prochaine attaque de type WannaCry.

À son niveau le plus simple, l'apprentissage automatique est défini comme « la capacité pour les ordinateurs d'apprendre sans être explicitement programmés pour cela ». En utilisant des techniques mathématiques appliquées à d'énormes ensembles de données, les algorithmes d'apprentissage automatique construisent des modèles de comportements. Netflix, par exemple, offre de nouvelles séries télévisées basées sur votre historique de visionnage précédent, la voiture autonome apprend sous quelles conditions un quasi-accident peut se produire avec un piéton.

Quelles sont les applications d'apprentissage automatique en matière de cybersécurité ? En principe, il peut aider les entreprises à mieux analyser les menaces et à répondre aux attaques et incidents de sécurité. Il va automatiser des tâches plus subtiles, auparavant effectuées par des équipes de sécurité étirées et parfois sous-qualifiées. C'est une tendance en croissance rapide. Les analystes d'ABI Research estiment que l'apprentissage automatique en cyber sécurité augmentera les dépenses en big data, en intelligence artificielle et en analytique de 96 milliards de dollars d'ici 2021.

Google et Amazon utilisent l'apprentissage automatique

Plusieurs géants mondiaux de l'IT travaillent sur ce sujet. Google utilise l'apprentissage automatique pour analyser les menaces contre les terminaux mobiles fonctionnant sur Android, ainsi que pour identifier et supprimer les logiciels malveillants des combinés infectés. Amazon a acquis la start-up harvest.AI et lancé Macie, un service utilisant l'apprentissage automatique.

Simultanément, les spécialistes de la sécurité ont travaillé à intégrer l'apprentissage automatique dans leurs produits, nouveaux et anciens, de manière à améliorer la détection des logiciels malveillants. « La plupart des grandes entreprises de sécurité sont passées d'un système basé sur la signature pour détecter les logiciels malveillants, à un système d'apprentissage automatique qui tente d'interpréter les actions et les événements », déclare Jack Gold, président de J. Gold Associates. « C'est clairement la voie à suivre dans le futur. L'intelligence artificielle et l'apprentissage automatique changeront radicalement la façon dont la sécurité est faite ».

Cette transformation ne se produira pas du jour au lendemain. Il faut distinguer l'apprentissage automatique et l'apprentissage profond. Dans sa première phase d'autonomisation de la cyberdéfense, nous voyons principalement les cas d'utilisation évidents permettant d'identifier des modèles d'activités malveillantes sur le point terminal, réseau, fraude ou SIEM, explique Dudu Mimran, CTO de Deutsche Telekom Innovation Laboratories (et également du Cyber Security Research Center de l'université israélienne Ben Gourion). « Je crois que nous verrons de plus en plus de cas d'utilisation, dans les domaines de la défense contre les interruptions de service, l'attribution et la modification du comportement de l'utilisateur. »



L'apprentissage automatique en sécurité comprend 5 cas principaux d'utilisation :

1. L'apprentissage automatique pour détecter les activités malveillantes et arrêter les attaques

Les algorithmes d'apprentissage automatique aideront les entreprises à détecter plus rapidement les activités malveillantes et à arrêter les attaques avant qu'elles ne commencent. David Palmer directeur de la technologie de la start-up Darktrace au Royaume-Uni a récemment aidé un casino en Amérique du Nord lorsque ses algorithmes ont détecté une attaque d'exfiltration de données qui utilisait un « aquarium connecté comme entrée dans le réseau ». La firme assure avoir également empêché une attaque similaire pendant la l'attaque Wannacry.

« Nos algorithmes ont repéré l'attaque en quelques secondes dans le réseau d'une agence NHS (système de santé britannique) et la menace a été atténuée sans causer de dommages à cette organisation, en fait, aucun de nos clients n'a été infecté par WannaCry, y compris ceux qui n'avaient pas patché contre elle. »

2. L'apprentissage automatique pour analyser les points de terminaison mobiles

L'apprentissage automatique est déjà largement répandu sur les appareils mobiles, mais jusqu'à présent, la majeure partie de cette activité a été consacrée à l'amélioration des expériences vocales sur Now, de Google, Siri d'Apple et Alexa d'Amazon. Pourtant, il existe aussi une application pour la sécurité. Comme mentionné ci-dessus, Google utilise l'apprentissage automatique pour analyser les menaces contre les terminaux mobiles.

En octobre, MobileIron et Zimperium ont annoncé une collaboration pour aider les entreprises à adopter des solutions mobiles anti-malware intégrant l'apprentissage automatique. MobileIron a déclaré qu'il intégrerait la détection de menaces basées sur l'apprentissage machine au moteur de sécurité et de conformité de MobileIron et vendrait la solution combinée, qui permettrait de détecter les menaces de périphériques, de réseaux et d'applications et de prendre immédiatement des mesures automatisées.

3. L'apprentissage automatique pour améliorer l'analyse humaine

L'apprentissage automatique en cybersécurité est censé améliorer l'analyste humain dans tous les aspects de son travail : la détection des attaques malveillantes, l'analyse du réseau, la protection des terminaux et l'évaluation de la vulnérabilité. Son meilleur champ d'action porte sur l'intelligence des menaces.

Par exemple, en 2016, le Laboratoire d'informatique et d'intelligence artificielle (CSAIL) du MIT a mis au point un système appelé AI 2, une plate-forme de sécurité adaptative qui a aidé les analystes à trouver des « aiguilles dans la botte de foin ». En examinant des millions de connexions quotidiennes, le système a pu filtrer les données et les transmettre à l'analyste humain, réduisant les alertes à environ 100 par jour. L'expérience, réalisée par le CSAIL et la start-up PatternEx, a montré que le taux de détection des attaques atteignait 85% avec une diminution par cinq des faux positifs.

4. L'apprentissage automatique pour automatiser les tâches de sécurité répétitives

Le véritable avantage de l'apprentissage automatique est qu'il pourrait automatiser des tâches répétitives, permettant au personnel de se concentrer sur un travail plus valorisant. David Palmer explique que l'apprentissage automatique devrait en fin de compte viser à « supprimer le besoin pour les humains de prendre des décisions répétitives et de faible valeur. Laissez les machines gérer le travail répétitif, les humains peuvent libérer du temps pour faire face à des problèmes stratégiques, comme la modernisation de Windows XP. »

Booz Allen Hamilton a emprunté cette voie, utilisant des outils d'IA pour allouer plus efficacement les ressources de sécurité humaine, triant les menaces afin que les salariés puissent se concentrer sur les attaques les plus critiques.

5. L'apprentissage automatique pour fermer les vulnérabilités du jour zéro

Certains croient que l'apprentissage automatique pourrait aider à réduire les vulnérabilités, en particulier les menaces du jour zéro et d'autres qui ciblent des dispositifs IoT en grande partie non sécurisés. Une équipe de l'université d'État de l'Arizona a utilisé l'apprentissage automatique pour surveiller le trafic sur le darkweb afin d'identifier les données relatives aux exploits du jour zéro. Forts de ce type d'informations, les entreprises pourraient potentiellement fermer les vulnérabilités et arrêter les exploits de correctifs avant qu'ils n'entraînent une violation de données.

Il reste des pièges à éviter

Méfiance, l'apprentissage automatique n'est pas une solution miracle. Il y a de nombreux pièges. Les systèmes d'apprentissage automatique rapportent parfois des faux positifs provenant de systèmes d'apprentissage non supervisés où les algorithmes déduisent des catégories basées sur des données. Certains analystes expliquent que l'apprentissage automatique en sécurité peut représenter une solution « boîte noire ». Ils sont donc obligés de placer leur confiance et leur responsabilité sur les épaules du vendeur et des machines.

Autre obstacle, la plupart des inventions d'apprentissage automatique qui ont été présentées ne font pas vraiment d'apprentissage dans l'environnement du client. Il s'agit de modèles formés sur des échantillons de logiciels malveillants dans le cloud d'un fournisseur et sont téléchargés comme des signatures antivirus. Ce n'est pas particulièrement progressif en termes de sécurité. De plus, l'apprentissage automatique est aussi bon que l'information d'entrée que vous lui fournissez. Donc, si vos algorithmes d'apprentissage automatique ne sont pas bien conçus, les résultats ne seront pas très utiles.



UN ARTICLE RÉDIGÉ PAR
IDG News Service



/ TECHNOLOGIES

Ces 9 compétences Legacy qui sont toujours très demandées

Aujourd'hui encore, les entreprises ont besoin de compétences legacy pour maintenir les systèmes et les réseaux existants.

Les entreprises sont confrontées à un nouveau défi en raison d'un déficit de compétences grandissant. Il porte sur les compétences legacy destinées à mettre à jour les anciennes technologies. Les entreprises sont confrontées à la nécessité d'embaucher sur des compétences qui ont tendance à disparaître du fait des départs en retraite. La mise à jour d'anciennes technologies a entraîné une perte de ressources, au fur et à mesure que les employés chevronnés quittent le marché du travail, les entreprises peuvent se trouver privées de compétences qui sont maintenant considérées comme dépassées, mais restent nécessaires.

Un sondage de Computerworld a révélé que 35% des entreprises recherchent toujours des compétences en programmation pour soutenir les systèmes legacy critiques. Voici les neuf technologies de type legacy pour lesquelles les entreprises recherchent des compétences.

1. **DB2**

Les origines de DB2 remontent à IBM, aux années 70, et au lancement de DB2 (IBM Database 2) en 1983. DB2 a été initialement développé par IBM pour être une plate-forme spécifique à ses systèmes d'exploitation, mais dans les années 90, IBM a ouvert DB2 avec du code commun. Aujourd'hui, il fonctionne sur plusieurs plates-formes, y compris Linux, Unix et Windows, aidant les entreprises à gérer leur stockage sur site et dans le cloud.

C'est l'un des langages de programmation legacy les plus populaires pour les entreprises, 13% d'entre elles déclarant supporter toujours les plateformes DB2 et embaucher des spécialistes. Les administrateurs de base de données, les ingénieurs logiciels, les programmeurs et les développeurs de logiciels sont les candidats les plus évidents pour DB2.

2.

L'un des langages de programmation les plus connus, C, est un langage impératif à usage général qui date de 1969. C'est devenu un standard en 1989. Conçu comme un langage de programmation simple et de bas niveau qui fonctionne sur toutes les plates-formes, il est flexible et largement utilisable.

En conséquence, il est intégré dans une vaste gamme de matériels et de logiciels, allant des microcontrôleurs aux supercalculateurs. Il a engendré plusieurs autres langages, comme C++, Java, JavaScript, C#, Perl, Python ou Swift. Les ingénieurs en logiciel, en électricité, les développeurs et les programmeurs sont les plus susceptibles d'avoir des compétences C. 10% des entreprises ont déclaré avoir besoin d'embaucher des compétences en C.

3. COBOL

Cobol est synonyme de «langage orienté métier», c'est un langage de programmation informatique spécialement conçu pour les entreprises. Créé en 1959, Cobol est présent dans un large éventail de systèmes Legacy, et tandis qu'il est lentement remplacé par de nouveaux langages de programmation modernes, il est toujours indispensable pour maintenir les systèmes existants.

Développé en partie comme un langage de programmation portable pour le département de la Défense des États-Unis pour traiter les données, il a été adopté par les fabricants d'ordinateurs, ce qui a contribué à perpétuer le langage au fil des ans. Aujourd'hui, on le trouve le plus souvent dans l'industrie financière, dans le secteur public et dans les systèmes administratifs. Les compétences Cobol sont fréquentes chez les programmeurs et les développeurs, 9% des entreprises disent avoir toujours besoin de compétences Cobol.

4. Assembleur

Le langage d'assemblage, le plus souvent appelé langage assembleur, est un langage spécifique à un composant matériel. En tant que langage de programmation de bas niveau, c'est l'un des langages de programmation les plus basiques, il n'est pas portable sur tous les appareils. Il est généralement utilisé lorsque la vitesse est un facteur clé.

Le sondage a révélé que 8% des entreprises ont encore besoin de compétences en assembleur. C'est l'un des premiers langages de programmation à utiliser le texte, donc l'inclure sur son CV peut également montrer que vous avez appris des langages de base en plus des langages modernes.

5.

Perl est une famille de langages de programmation Open Source, à usage général, qui ressemble au langage C. Elle est plus rapides que les langages structurés comme C et C++. Perl a été développé en 1987 mais la version la plus récente est venue en mai 2017, avec Perl 5. Il y a aussi un Perl 6, mais il fonctionne indépendamment de Perl 5, bien qu'il entre dans la famille Perl.

Perl a toujours une bonne position sur le marché, dans le domaine des langages de programmation Legacy, 5% des entreprises embauchent toujours pour cette compétence. Sans être importantes numériquement, les offres permettent aux candidats de mettre un pied dans une entreprise. Les ingénieurs logiciels, ceux liés à la conception, les développeurs de logiciels, les administrateurs système et les programmeurs sont les plus susceptibles d'avoir des compétences Perl sur leur CV.

6. Delphi et Pascal Object

Delphi et Pascal Object sont étroitement liés. Delphi utilisant le langage de programmation Pascal. Pascal Object est un langage de programmation de haut niveau, facile à utiliser, tandis que Pascal est plutôt un langage de programmation polyvalent de bas niveau. Il a été développé dans les années 90 et publié en 1995 pour Windows 3.1, générant de multiples versions, des itérations et des versions nouvelles au fil des années.

Seulement 3% des entreprises interrogées embauchent sur ce type de compétences. Les spécialistes Delphi se trouvent essentiellement chez les développeurs de logiciels, les ingénieurs et les programmeurs.

7. Fortran

Fortran, qui signifie Formula Translation, est conçu pour les algorithmes scientifiques, le plus souvent ceux utilisés par les ingénieurs et les mathématiciens pour l'ingénierie aérospatiale, mécanique et logicielle. Le langage de programmation le plus ancien de cette liste, Fortran, a été développé dans les années 50 par IBM et, pendant des décennies, était le langage de programmation dominant pour la prédiction météorologique, la physique et d'autres tâches de calcul haute performance.

Seulement 3% des répondants ont déclaré qu'ils cherchaient encore des profils Fortran, mais cela pourrait changer à mesure que les salariés les plus expérimentés changent d'emploi ou prennent leur retraite. Les ingénieurs logiciels, les ingénieurs aéronautiques et les ingénieurs en mécanique sont les candidats les plus susceptibles d'avoir des compétences Fortran sur leur CV.

8. REXX

Restructured Extended Executor (REXX) a été développé entre 1979 et 1982 par un employé d'IBM en tant que langage de programmation structuré, conçu pour être facile à apprendre et à lire. Il est le plus souvent utilisé comme langage de script et de macro, traitant des données et du texte, ou générant des rapports. Même les non-programmeurs peuvent apprendre et utiliser ce langage, ce qui en fait une option populaire pour les entreprises.

Ce n'est pas la compétence Legacy la plus demandée, avec seulement 3% des personnes interrogées qui embauchent des spécialistes REXX. Elle est le plus souvent associée à des programmeurs informatiques, des ingénieurs logiciels, des analystes de systèmes d'applications et des programmeurs Mainframe.

9. Pascal

Développé à la fin des années 1960, Pascal est un langage de programmation impératif et procédural conçu à l'origine pour l'enseignement des langages de programmation. Aujourd'hui, il a été remplacé par C, C++ et Java, mais il est toujours utilisé comme introduction à la programmation. Destiné à la programmation structurée, qui nécessite une grande attention aux détails, c'est devenu un langage populaire pour enseigner aux étudiants, moins pour être utilisé dans l'entreprise.

Seulement 2% des entreprises ont déclaré embaucher des spécialistes Pascal. Les ingénieurs logiciels et les développeurs de logiciels sont les candidats les plus proches de telles compétences.



UN ARTICLE RÉDIGÉ PAR

La rédaction de CIO Etats-Unis



/ STRATÉGIE

Les 12 plus grands problèmes auxquels doit faire face une DSI

De la cybersécurité au datamanagement, les DSI ont plus que leur part de préoccupations qui les empêchent de dormir la nuit.

Lorsque les DSI ne sont pas submergés par les données, ils se demandent qui les sécurise. Ils font face à la pression de la réduction des coûts tout en essayant de rester agiles face aux difficultés rencontrées par leurs sous-traitants et aux défis liés au transfert des données et de services vers le cloud. Pendant ce temps, de nouvelles menaces émergent qui nécessitent une réponse évolutive.

Qu'il s'agisse de recruter des professionnels qualifiés ou de les éviter, une large gamme de problèmes technologiques ou humains donne des sueurs froides aux professionnels de l'informatique. Nos confrères de CIO US ont recueilli des idées venues d'experts, de la direction, de recruteurs et d'équipes terrain afin d'identifier les préoccupations les plus pressantes d'aujourd'hui et la façon de les gérer.

1. La sécurité de l'IoT

Une récente étude de Forrester a révélé que 82% des entreprises luttent pour identifier et sécuriser les périphériques connectés au réseau. La plupart ne savent même pas qui est responsable de la gestion de ces appareils. « Plus de la moitié des personnes interrogées (54%) ont déclaré redouter ce sujet de sécurité de l'IoT », indique l'étude.

Csaba Krasznay, évangéliste sécurité chez Balabit, explique qu'avec des éléments faibles traditionnels comme les utilisateurs, les DSI doivent penser à de nouvelles menaces émergentes. « En 2018, explique-t-il, les mesures de sécurité devraient être plus étroitement axées sur les utilisateurs et la question de leur identité. La surveillance comportementale peut détecter les cybercriminels même les plus intelligents qui se cachent derrière des identifiants à privilège, en discernant les déviations dans les comportements de base, même sur la base de traits biométriques minuscules tels que la vitesse de frappe ou les fautes d'orthographe communes ! »

2. Le recyclage

Environ 40 % des employés disent qu'ils ne disposent pas de la formation dont ils ont besoin pour être efficace dans leur travail, selon un récent sondage CompTIA, organisme américain de certification. « *De nombreuses entreprises pensent que le suivi de la technologie et de ses évolutions relève d'une démarche de chaque employé* », explique Viktor Andonov de DataArt Bulgaria. « *Ce qui était possible dans les années 80 et 90, ne l'est plus au 21^{ème} siècle, la complexité des plateformes a énormément augmenté. La formation sur le tas et le fait d'apprendre à travailler avec de nouveaux cadres est extrêmement difficile lorsque les employés ont des projets en cours très prenants* ».

Selon Todd Thibodeaux, président et chef de la direction de CompTIA, la plupart des organisations éprouvent des difficultés à trouver du personnel technique qualifié. Les former rapidement est tout aussi intimidant. « *La bonne nouvelle pour les employeurs, c'est que la majorité des professionnels de l'informatique aiment ce qu'ils font* », explique Todd Thibodeaux. « *Leurs emplois leur procurent un sentiment d'accomplissement personnel. Leurs compétences et leurs talents sont mis à profit. Ils voient des opportunités de croissance et de développement dans leur carrière et ils sont généralement satisfaits de leur rémunération et de leurs avantages* ».

La reconversion est un atout considérable, affirme Todd Thibodeaux. « *Les professionnels de l'informatique aimeraient avoir plus de ressources pour la formation et plus de possibilités d'orientation professionnelle et d'avancement professionnel. Ils souhaitent également avoir accès à plus d'outils et interagir avec davantage de technologies et d'applications* ». Le problème n'est pas nouveau.



3. La surcharge des données

Les méthodes actuelles d'analyse des données échouent fréquemment à montrer l'impact réel sur l'activité commerciale, remarque Mike Sanchez, CISO de United Data Technologies. « *Les cadres dirigeants et les membres du conseil d'administration devraient être en mesure de décider de la meilleure façon d'allouer les ressources et les investissements dans des stratégies de remédiation qui peuvent réduire les dépenses opérationnelles ou le risque réel de l'entreprise, voire les deux. Il y a trop de données disponibles et les gens ne savent pas ce qu'ils devraient suivre pour améliorer leurs positions globales en matière de cybersécurité. Les indicateurs de performance clés doivent indiquer l'histoire dans un format de tableau de bord simple.* »

4. Les manques de compétences

Bonnes nouvelles, le nombre d'offres d'emploi IT continue d'augmenter. Le mauvais ? Il n'y a pas assez d'experts formés avec les compétences nécessaires pour les remplir, en particulier en matière de sécurité. « *Notre dernière analyse sur les emplois provenant de diverses sources montre qu'au troisième trimestre de 2017, les employeurs américains ont proposé près de 604 000 emplois dans l'IT* », explique Todd Thibodeaux de CompTIA. « *En ce qui concerne les emplois liés à la cybersécurité, nous avons comblé l'écart au cours de la dernière année, mais pas autant que ce qui doit être fait.* »

Les entreprises vont devoir prendre des décisions difficiles sur la façon de combler les besoins en personnel. « *Quelles fonctions pourraient être externalisées auprès d'un fournisseur de solutions technologiques ?* » se demande ainsi Todd Thibodeaux. « *De nombreuses entreprises estiment que la passation des marchés avec un partenaire technologique pour certaines tâches routinières et continues peut libérer des équipes techniques internes pour qu'elles se concentrent sur des activités plus avancées et stratégiques pour l'entreprise.* »

5. Innovation et transformation numérique

Selon les chiffres du Gartner, environ deux tiers des chefs d'entreprise pensent que leurs entreprises doivent accélérer leur transformation numérique ou perdre du terrain face à leurs concurrents. La plupart des entreprises continueront sur la même voie jusqu'à ce qu'elles soient obligées de faire autrement, explique Merrick Olives, directeur-associé de la société de conseil en cloud computing Candid Partners.

« Lier les dépenses informatiques à des capacités commerciales stratégiques et à la compétitivité est essentiel », explique Merrick Olives. « Les modèles de financement basés sur les flux de valeur, par opposition au financement par projet, deviennent de plus en plus efficaces pour satisfaire les objectifs du Comex. Les structures de coûts et l'efficacité des processus legacy par rapport à une capacité agile sont très différentes, l'agilité est moins chère et beaucoup plus efficace ».

6. Des budgets serrés

Près de la moitié des informaticiens et la même proportion parmi les secteurs d'activité ont déclaré que les budgets constituaient un obstacle à la sécurisation de l'IoT, selon un rapport de Forrester du mois de novembre 2017. Todd Thibodeaux de CompTIA estime que « la question est de savoir si l'entreprise veut grandir et prospérer ou se laisser distancer par ses concurrents. Au fur et à mesure que les entreprises deviennent plus numériques, la technologie passe de l'ombre à la lumière où elle devient le principal moteur pour atteindre les objectifs de long terme. Des professionnels de l'informatique qualifiés, formés et certifiés sont essentiels pour rentabiliser les investissements dans la technologie. Ils ont l'expertise nécessaire pour relier l'architecture informatique aux objectifs généraux de l'entreprise et peuvent fournir les conseils dont les décideurs ont besoin pour rendre des arbitrages lors de la mise au point du projet ».

7. Trouver de nouvelles sources de revenus

Ian Murray, vice-président de la société de logiciels de gestion des dépenses télécom Tangoe, affirme que même si le paysage des affaires est en constante évolution, le principe de base de la réalisation d'un bénéfice reste le même. Selon Mike Fuhrman, chef de produit chez Peak 10 ViaWest, fournisseur d'infrastructures informatiques hybrides, « ce qui a changé, c'est l'importance accordée à la génération directe de revenus sur le parcours du DSI ».

« Peut-être que je suis old school, mais je ne pense pas que le DSI devrait s'inquiéter de générer directement des revenus », explique Mike Fuhrman. « Je commence à voir cela apparaître de plus en plus parmi mes pairs. Pour rester pertinents en tant que DSI, beaucoup travaillent dans cet objectif. Bien qu'il y ait des avantages à penser de cette façon, cela peut aussi être une manière de dévier de sa trajectoire. La place du DSI est de se concentrer sur ses projets et d'utiliser une plate-forme automatisée à grande échelle. Nous devons rester concentrés sur la réduction des coûts et l'adaptation au marché. Voilà comment un DSI devrait se concentrer sur les revenus. »

8. La mise à niveau des systèmes legacy

Le cabinet de recrutement Robert Half a édité l'été dernier un rapport qui a révélé que près d'un quart des DSI était préoccupé d'abord par la mise à niveau des systèmes existants pour améliorer l'efficacité. « C'est un élément majeure, en particulier dans plusieurs secteurs où un grand nombre de systèmes obsolètes ou en fin de vie sont encore utilisés pour stocker des données ou des applications stratégiques », explique Mike Sanchez, de United Data Technologies. « Ces systèmes ne sont plus pris en charge par leurs fabricants respectifs et ne peuvent donc plus être corrigés avec la dernière version des mises à jour, laissant ces systèmes vulnérables. Ils peuvent être interconnectés à d'autres réseaux, ce qui permet aux vulnérabilités de s'étendre vers l'extérieur et d'inclure ces systèmes interconnectés dans les attaques ».

9. Le manque d'agilité

Les organisations qui visent à incorporer des méthodes agiles éprouvent des difficultés et évoluent dans une sorte de modèle hybride qui intègre des pratiques agiles mais aussi des méthodes dites en « cascade » plus linéaires. En bref, le pire des deux mondes. Pour Ian Murray de Tangoe, « les développeurs codent des fiches techniques spécifiques avec peu de compréhension conceptuelle sur la façon dont ce bouton ou cette fonctionnalité s'intègre dans l'expérience globale de l'utilisateur. Une approche disciplinée est nécessaire pour réussir. »

Ian Murray évoque des mises à jour récentes d'Apple iOS, qui corrigeaient certains bugs et en introduisaient d'autres. « Ce problème affecte les entreprises, grandes et petites », explique-t-il, conduisant à des mises à jour qui peuvent corriger les failles de sécurité et inclure de nouvelles fonctionnalités, mais aussi créer des casse-têtes bien connus des utilisateurs.



10. Les risques d'externalisation

Le déficit de compétences amènera de nombreuses organisations à rechercher une aide extérieure. Mais ces solutions parfois nécessaires peuvent entraîner des problèmes de fiabilité et de sécurité. « Notre objectif principal est de tenir les promesses que nous faisons à chaque client », explique Mike Sanchez.

« Vous construisez votre réputation et vos affaires sur ce point critique. En externalisant votre travail, la qualité du livrable est parfois à la merci de l'entreprise sous-traitée. Compte tenu de la nature sensible des projets que nous gérons, nous utilisons des évaluations strictes de fournisseurs tiers pour évaluer les partenaires dans le cas où un projet nous obligerait à envisager d'externaliser certaines, ou toutes les tâches requises. »

En plus des problèmes de qualité, l'externalisation ouvre des menaces de sécurité bien connues. « Les menaces spécifiques, qui devraient être prioritaires pour les DSI, viennent de l'initié et le sous-traitant », explique French Caldwell, chef évangéliste chez MetricStream et ancien conseiller de la Maison Blanche pour la cybersécurité. « Jusqu'à ce que nous puissions nous passer des mots de passe pour les informations d'identification, les humains continueront à être la plus grande menace. »

11. Des pièges dans la migration vers le cloud

À mesure que davantage de données et de services sont transférés vers le cloud, un risque potentiel est de considérer celui-ci comme une entité publique unique, déclare Bask Iyer, DSI de VMware et Président de Dell Digital. « L'informatique doit également prendre en compte les solutions cloud et / ou multi-cloud privées pour évaluer ce qui est le mieux adapté à l'activité. Cela garantit le choix et évite le verrouillage par un seul fournisseur. Le service informatique doit également déterminer quelles applications doivent être utilisées et dans quel cloud. Avec la montée en puissance de l'IoT, il faut plus de puissance à la périphérie, de sorte que les services informatiques doivent élargir leurs options pour le cloud ».

Les DSI ne peuvent pas transférer la responsabilité de sécuriser leurs données et leurs applications chez un hébergeur, dit Mike Sanchez. « Les organisations doivent définir des contrôles de sécurité pour protéger leurs données dans le cloud de la même manière qu'ils le font pour leur propre site. De nombreuses organisations n'appliquent pas ces normes et supposent que l'hébergeur fournit toutes les garanties dont elles ont besoin. »



12. Les multiples vulnérabilités de sécurité

Selon Larry Lunetta, vice-président de la division Aruba de Hewlett-Packard, les cauchemars de sécurité se poursuivront cette année. « *Les futurs thèmes d'actualité feront cohabiter des informations d'identification légitimes comme point de départ d'une attaque qui peut prendre des jours, des semaines ou même des mois avant d'émerger et finalement causer des dommages* », explique Larry Lunetta.

« *Ces attaques peuvent commencer par un utilisateur qui clique sur la mauvaise pièce jointe, un employé mécontent qui devient un voyou, ou une suite de mots de passe faibles ou de partage d'informations d'identification entre collègues.* »

De nouvelles techniques de détection comportementale seront nécessaires en 2018 pour contrer les menaces. « *De plus en plus, les organisations utilisent des systèmes d'analyse comportementale des utilisateurs et des entités pour identifier les petits changements de comportement des utilisateurs et des périphériques connectés au réseau qui sont souvent révélateurs d'une attaque en gestation* ».



UN ARTICLE RÉDIGÉ PAR

La rédaction de CIO Etats-Unis