

Guide des bonnes pratiques, 2024 : SLED

État et collectivités locales | Éducation | Défense/Aviation/Aérospatiale



La verticale SLED, telle que définie par Convergent, englobe l'État et les collectivités locales, l'éducation et l'aviation/aérospatiale. Bien que chacun de ces sous-secteurs soit certainement distinct, il y a plus de points communs que de variations lorsqu'il s'agit de sécurité. Ceci est illustré **par le défi que représente l'escalade des risques physiques et cybernétiques** qui oblige à donner la priorité à la planification de la sécurité et à l'atténuation des procédures pour toutes les entités SLED.

L'équipe SLED de Convergent propose des **stratégies de protection de haute sécurité, une mise en œuvre méthodique des programmes et des solutions complètes** axées sur la sécurité et l'efficacité opérationnelle dans ce secteur. Grâce à sa connaissance approfondie des menaces qui pèsent sur l'industrie et des exigences en matière de conformité réglementaire, et grâce à son personnel disposant de subventions et de ressources financières, Convergent peut déployer des systèmes intégrés qui fonctionnent dans le respect des contraintes de la planification budgétaire.

Incidents et risques liés à la sécurité de SLED

Les responsables de la sécurité dans l'espace SLED se concentrent sur le **maintien de la sécurité publique et sur l'utilisation de tous les fonds disponibles** pour mettre en place des systèmes qui facilitent leur capacité à le faire.

Cela dit, leur plus grand risque est d'adopter une attitude réactionnaire en matière de planification de la sécurité. Cette approche de fortune, qui consiste à s'attaquer à l'incident plutôt qu'à la situation dans son ensemble, est beaucoup trop fréquente. Par exemple, une école de la maternelle à la terminale peut être confrontée à un incident de harcèlement et réagir en ajoutant des caméras et des dispositifs de surveillance. Une administration locale peut être confrontée à une vague de vols et, par conséquent, installer un contrôle d'accès. Une fusillade peut donner lieu à la détection d'armes.

Au lieu d'aborder la sécurité de manière fragmentaire, il est important de l'envisager de manière holistique et de prendre en compte les objectifs à court et à long terme. La mise en œuvre d'un plan global permet d'éviter de nombreux incidents individuels qui conduisent à l'érosion de la marque, à des problèmes de réputation et à des risques juridiques.

Il est également utile de décomposer les choses par sous-verticale SLED afin de faciliter l'obtention d'informations précieuses spécifiques à l'entreprise en question.

L'État et les collectivités locales aujourd'hui et demain

Les gouvernements nationaux et locaux ont pour priorité d'assurer la sécurité de la communauté et de leurs employés. Au-delà des implications évidentes, ils doivent prendre en compte les effets sur la perception du public, l'embauche et le maintien en poste. Plus précisément, les municipalités gèrent une multitude de risques liés à la sécurité, notamment

- Criminalité
- Sécurité de la police et risques juridiques

- Populations migrantes et sans-abri
- Transports et sécurité des transports en commun

Cependant, d'autres problèmes sont en jeu. **Le vandalisme sur les biens et les cyber-menaces restent des risques critiques pour les municipalités, avec des conséquences importantes pour les contribuables.** Tous les défis en matière de sécurité peuvent être exacerbés par une mauvaise communication intra-agence et inter-agence qui, en fin de compte, entrave la capacité de la collectivité à gérer les incidents et à tirer pleinement parti des ressources financières.

L'éducation maintenant

Une planification cohérente

Comme nous l'avons indiqué, le risque le plus important pour les écoles de la maternelle à la terminale **reste l'absence de planification cohérente et holistique de la sécurité.** Beaucoup trop de districts ne disposent pas d'un plan stratégique global et achètent arbitrairement des équipements de sécurité sans se préoccuper de la manière dont ils compléteront les technologies en place. Le manque d'intégration des dispositifs et des équipements crée en fin de compte un système disparate qui ne fonctionne pas comme il le devrait.

Cette approche fragmentaire de la conception et de la planification des systèmes de sécurité est souvent due à un financement incohérent et inadéquat de la part de l'État et des autorités locales. Les écoles primaires et secondaires dépendent spécifiquement des subventions de l'État et du gouvernement fédéral pour combler les déficits budgétaires, et le déficit de financement se creuse généralement avec le temps, ce qui accélère les problèmes de sécurité.

Communication

La sécurité des écoles primaires et secondaires est également affectée par l'absence de protocoles et de verbiages cohérents et uniformes en matière d'intervention d'urgence. Il est intéressant de noter que de nombreux districts à travers le pays utilisent encore un verbiage d'intervention d'urgence personnalisé ou unique pour les incidents qui se produisent sur le campus. **Cela peut poser des problèmes lorsque plusieurs districts scolaires relevant de la compétence d'un organisme d'intervention des forces de l'ordre ont des codes d'intervention différents ou, à l'inverse, lorsqu'un district est desservi par plusieurs juridictions lors d'une situation d'urgence.** Par exemple, le district A peut utiliser le "code rouge" pour un confinement et le "code jaune" pour un périmètre sécurisé, tandis que le district B utilise le "Hard Lockdown" pour un confinement et le "Soft Lockdown" pour un périmètre sécurisé. Cela peut créer une confusion générale et retarder la réponse lors d'un incident critique, où le temps est un facteur essentiel.

Les coupures de communication sont encore aggravées lorsque les districts adjacents et les agences de première intervention ne collaborent pas entre eux lors de la sélection et de l'achat d'outils et de technologies de sécurité et d'intervention en cas d'urgence. Souvent, les districts

sont convaincus de la capacité d'une technologie à communiquer directement avec les forces de l'ordre afin d'accélérer l'intervention d'urgence. Cela dit, il faut pour cela que les premières agences d'intervention comprennent parfaitement la technologie et maîtrisent leur capacité à la gérer. Si plusieurs districts scolaires relevant d'une même autorité policière ne choisissent pas un produit commun, les organismes de première intervention doivent gérer plusieurs systèmes lors d'un incident critique. Par exemple, le district A peut utiliser la technologie 1, qui assure l'interopérabilité avec son dispatching ou PSAP. Le dispatcheur doit se connecter et communiquer directement avec le district par le biais d'un canal ou d'un portail sécurisé. Le district B, quant à lui, peut utiliser un système technologique différent qui nécessite des identifiants de connexion au portail URL totalement différents, avec une notification par un canal différent. Cela crée un grand potentiel d'erreur humaine qui peut survenir lors d'une réponse à un incident critique.

Cybermenaces

Alors que la sécurité physique reste un point central pour les écoles primaires et secondaires, la cybersécurité est un risque de plus en plus important dans le secteur de l'éducation. Ce risque englobe les ransomwares, les violations de données, l'ingénierie sociale, le phishing et la cybersécurité de base. En substance, puisque la technologie de sécurité permet d'accéder ou de pénétrer sur Internet et dans les systèmes électroniques qui s'y trouvent, le besoin de dispositifs de "sécurité de la sécurité" est d'une importance cruciale.

L'éducation dans le futur

Une planification cohérente



Les écoles primaires et secondaires du pays commencent à **comprendre l'intérêt de développer leurs systèmes et opérations de sécurité** sur la base d'évaluations complexes de la sécurité, d'évaluations des risques pour la sécurité de l'entreprise ou de plans directeurs stratégiques. L'identification des besoins, des vulnérabilités, des actifs, des lacunes et des menaces d'un district est essentielle, mais la mise en œuvre de stratégies de sécurité multicouches axées sur la capacité de dissuader, de détecter, de retarder et de refuser ces vulnérabilités et menaces est primordiale. Une

approche méthodique peut garantir la capacité d'un district à pour atteindre les objectifs de sécurité à court et à long terme.

Un financement approprié étant essentiel pour soutenir cette approche, les écoles primaires et secondaires auront tout intérêt à travailler avec des partenaires de confiance pour compléter leurs ressources internes en matière de rédaction de demandes de subventions. En particulier, l'équipe SLED de Convergent offre une assistance de bout en bout en matière de subventions et de financement. Cela inclut une aide professionnelle à la rédaction et à l'amélioration des propositions de subventions.

Sécurité à plusieurs niveaux

L'Alliance des partenaires pour des écoles plus sûres (PASS K-12) propose des conseils et des bonnes pratiques en matière de sécurité scolaire.

En suivant leurs recommandations, de nombreuses écoles adoptent déjà une approche multicouche de la sécurité, qui devrait se renforcer dans les années à venir. Le renforcement de cinq couches physiques permet de faire face à un large éventail de menaces, car chaque couche successive fournit des composants spécifiques pour dissuader, détecter/retarder et répondre aux comportements adverses dans le cas où les autres couches sont contournées ou violées.

Chaque couche comprend des éléments de protection de base de la sécurité :

- Politiques et procédures
- Personnel (rôles et formation)
- Architecture
- Communication
- Contrôle d'accès
- Vidéosurveillance
- Détection et alarme

Et il existe des niveaux de sécurité à l'intérieur de chaque couche. En termes simples, **le premier niveau fournit de bonnes protections de base, tandis que le dernier niveau promet l'approche la plus complète de la sécurité de la maternelle à la 12e année.** De nombreuses écoles seront incapables de mettre en œuvre des mesures au-delà des premier et deuxième niveaux, ou n'en auront pas besoin. Convergent fournit aux administrateurs des écoles les outils dont ils ont besoin pour peuvent utiliser pour évaluer leur niveau de risque, identifier leurs besoins en matière de sécurité et, après avoir pris en compte les ressources et le financement disponibles, élaborer des plans de sécurité sur mesure qui intègrent les meilleures pratiques et procédures. N'oubliez pas que si les approches de sécurité à plusieurs niveaux peuvent être coûteuses, les lignes directrices du PASS comprennent des recommandations et des considérations pratiques peu ou pas coûteuses.

Communication

Les écoles de la maternelle à la terminale bénéficieront de l'adoption de protocoles d'intervention d'urgence uniformes et cohérents, conformes aux meilleures pratiques du secteur, tels que le protocole d'intervention standard (PIS) de la fondation I Love U Guys. Adopté à ce jour par 36 000 écoles dans tout le pays, ce protocole utilise une terminologie et un verbiage communs qui sont cohérents pour les premiers intervenants, les écoles et les communautés. Ainsi, lorsqu'un incident se produit, les organismes de première intervention peuvent mieux comprendre et gérer la situation avec plus de clarté. On s'attend à ce que d'autres systèmes scolaires se joignent à l'initiative au fur et à mesure que la nouvelle se répand. Si un incident continue d'évoluer, les districts adjacents peuvent également être amenés à mettre en œuvre des mesures renforcées.

Cybermenaces

En réponse à la cybermenace, **les districts scolaires devraient consacrer davantage de ressources** à la sensibilisation, à la formation et au renforcement des équipements. Ce dernier point devrait commencer par l'évaluation des caméras et autres dispositifs de sécurité physique qui peuvent avoir des identifiants de connexion par défaut, des microprogrammes obsolètes ou une visibilité dangereuse sur les points d'accès ouverts/visiteurs.

Aviation Now

Les aéroports sont confrontés à une recrudescence des violations de leur périmètre. Cela peut entraîner la fermeture de l'aéroport et des amendes de la part de la FAA et de la TSA, ce qui peut s'avérer très coûteux. Par conséquent, les installations renforcent la détection des intrusions à l'aide de caméras, de radars, de lidars et de technologies de détection des clôtures. L'IA joue un rôle dans la gestion des fausses alarmes.



La menace interne est également mieux connue, ce qui a incité la TSA à instituer des mandats de filtrage des employés et des formations spéciales. Il s'agit notamment de la cyberformation et des protocoles visant à renforcer les meilleures pratiques et les protections des appareils à l'aide de logiciels spécialisés.

L'aviation du futur

Le secteur de l'aviation est susceptible d'adopter une myriade de technologies pour optimiser la sécurité, notamment le PSIM et des systèmes de sonorisation plus avancés. Outre les exigences en matière de gestion des risques, il est également nécessaire d'améliorer l'efficacité opérationnelle. Les technologies Lidar/capteurs, par exemple, peuvent contribuer à la fois à la sécurité et à la gestion des flux (du trottoir à la porte ou de la porte au trottoir) et constituer une source de revenus.

Le coût des attaques physiques ou cybernétiques

Les entités SLED peuvent subir des pertes importantes **à la suite d'une intrusion physique ou cybernétique**, dont les plus préoccupantes sont les suivantes :

1. **Vie humaine**

Il est évident que le résultat le plus inquiétant d'une attaque physique est la perte de vies

humaines. Malheureusement, les exemples sont trop nombreux pour être cités dans l'espace public.

2. Réputation/confiance

Les écoles et les entités publiques prospèrent grâce à la confiance de la communauté. Un manque apparent de préparation à un incident de sécurité peut considérablement éroder leur réputation. Cela peut inciter les citoyens à changer d'école, à voter pour la destitution d'une personne ou même à déménager.

Risques futurs les plus menaçants

Tout en gérant les menaces physiques, toutes les entités SLED doivent veiller à ce que les solutions ne créent pas d'autres problèmes tels que le risque cybernétique à l'avenir. En particulier, des protections doivent être mises en place pour que les équipements de sécurité physique ne deviennent pas un vecteur de cyber-menaces. De nombreux organismes publics, districts scolaires, services de sécurité des campus et administrations locales ne disposent pas du personnel nécessaire pour gérer et entretenir les systèmes de protection contre les cyberrisques et autres risques. Ils doivent donc s'en remettre aux mesures de protection des fournisseurs. En fin de compte, le fait de renforcer et de simplifier la solution pour l'utilisateur permet de minimiser l'impact sur les opérations quotidiennes et d'optimiser les protections.

Contre-mesures en matière de technologie de sécurité

Beaucoup d'espaces publics sont ouverts par nature, et il est donc courant d'y trouver des personnes qui ne sont pas nécessairement "invitées". Ces entités accueillent souvent des visiteurs en plus des employés, du grand public et des étudiants. **Le libre accès peut sembler incompatible avec la sécurité, mais les deux peuvent coexister si la technologie de sécurité est entièrement intégrée dans une plateforme transparente** qui permet une réponse optimale et des rapports médico-légaux.

Convergent relève ce défi grâce à une approche consultative de l'évaluation des systèmes et des besoins, en se concentrant sur l'identification des plus grandes lacunes et/ou des plus grands besoins du client, en s'appuyant sur nos propres lignes directrices et sur les meilleures pratiques du secteur, telles que le PASS pour des écoles plus sûres. Nous trouvons les solutions technologiques appropriées, en tirant parti de notre expérience pour déterminer l'approche la plus pragmatique pour aller du point A au point B avec un système de sécurité particulier.

L'équipe de Convergent SLED identifie facilement les lacunes en matière d'exposition aux risques et sait comment trouver les solutions appropriées. Et comme nous sommes indépendants de tout partenaire, nos clients bénéficient d'options spécifiques à leurs besoins. Nos solutions sont complétées par des recommandations de processus, comme en témoignent les exemples suivants :

Exemple 1

Défi : Prévention de la criminalité

Recommandation d'équipement : LPR, caméras,

Détails : Convergint recommande que les demandes de licences commerciales mentionnent l'obligation du propriétaire de coopérer avec la police dans le cadre d'enquêtes ou de fédérer ses caméras. Cela permettra d'accélérer la réponse, la résolution des crimes et la connaissance de la situation.

Exemple 2

Défi : Sécurité des agents, relations publiques/gestion de la perception

Recommandation relative à l'équipement : Caméras corporelles

Détails : Convergint recommande que tous les agents portent une caméra corporelle afin de garantir leur capacité à relayer les détails de l'incident du point de vue de l'agent. Cela réduira les chances d'une fausse plainte contre un agent de police.

Exemple 3

Défi : Gestion de l'enfermement

Recommandation en matière d'équipement : Caméras de surveillance, contrôle d'accès et alarmes anti-panique

Détails : Convergint recommande un contrôle d'accès dans les centres de détention afin d'envoyer des alertes au superviseur interne pour qu'il vérifie l'état du prisonnier à intervalles réguliers. Les badges de contrôle d'accès permettent de vérifier les entrées. Le VMS peut être intégré au contrôle d'accès afin de visualiser les contrôles et de s'assurer que les prisonniers et les gardiens sont protégés.

Améliorer l'efficacité du personnel de sécurité/réduire les coûts

Efficacité du personnel

Les équipements de sécurité peuvent être un multiplicateur de force qui améliore l'efficacité globale du plan de sécurité, mais ils peuvent aussi ajouter une complexité qui n'est pas facilement absorbée par les ressources du client. Par la suite, tout équipement ajoute un mandat pour une évaluation approfondie. Par exemple, l'ajout de caméras peut se traduire par une réduction du nombre de gardes sur place, ce qui améliore l'efficacité. Cela dit, un trop grand nombre de caméras nécessitera des opérations de surveillance plus sophistiquées, comme un centre de commandement et de contrôle doté d'un personnel complet.

Aucun équipement d'un plan de sécurité ne doit être considéré comme une installation autonome. Un système de détection des vapeurs dans les toilettes d'une école ou un système de détection des tireurs dans un établissement public peut sembler une solution convaincante à un problème très urgent, **mais il ne sera pas d'une efficacité optimale s'il n'est pas entretenu, testé, contrôlé et intégré** au système dans son ensemble. L'intégration est particulièrement importante. Si une agence dispose d'un système de vidéosurveillance, d'un système d'alarme et d'un contrôle d'accès, mais qu'ils ne sont pas intégrés dans une seule et même vitre, le personnel de sécurité devra travailler à partir de trois postes de travail différents uniquement pour surveiller les systèmes. C'est clairement inefficace.

Réduction des coûts

Le retour sur investissement de toute dépense technologique dépend des dépenses d'investissement initiales et des dépenses d'exploitation courantes. Il est important de prendre en compte non seulement les dépenses initiales, mais aussi le temps et les ressources nécessaires à la gestion et à la maintenance de ces systèmes. Le personnel est un élément essentiel de cette équation.

Toute décision d'investissement technologique doit tenir compte à la fois des finances et des objectifs généraux de l'entreprise. Les entités publiques se concentrent généralement davantage sur la réduction des incidents de sécurité que sur la maximisation des profits, mais d'autres besoins commerciaux entrent en ligne de compte. Tous doivent être examinés afin d'obtenir un meilleur retour sur l'investissement dans les technologies de sécurité. Par exemple, les interphones et les communications de masse mais aussi de faciliter les capacités de communication par diffusion pour la gestion des visiteurs. Les avantages vont au-delà de la sécurité.

Gestion du budget de la sécurité

La budgétisation est souvent un défi pour l'entité publique, et les subventions sont une excellente solution pour financer des dépenses importantes en matière de sécurité. Cela dit, de nombreux clients de SLED sont dépassés par le processus d'identification des possibilités de financement et par les démarches à effectuer. Convergent a donc mis en place une équipe chargée des subventions et du financement afin de guider et d'aider ses clients dans le processus d'obtention de fonds pour les dépenses de sécurité.

En outre, nous pouvons soutenir l'argument selon lequel les ressources financières et/ou humaines doivent être engagées par d'autres départements pour garantir la réussite des programmes de sécurité. Le financement interdépartemental peut compléter les subventions, et l'engagement de personnel peut faire toute la différence dans l'obtention d'une subvention. Les organisations bien intégrées sont bien accueillies par les décideurs en matière de subventions.

En fin de compte, si le client peut aider à répondre aux besoins d'autres parties de l'organisation au-delà de la sûreté et de la sécurité, il est plus susceptible d'obtenir le soutien nécessaire de tous les services. Cela ouvre la voie à de futures relations, à des engagements récurrents et à une approche plus proactive des investissements en matière de sécurité.

Les véhicules sous contrat en option

Les États, les villes, les comtés, les écoles primaires et secondaires et les établissements d'enseignement supérieur peuvent profiter des véhicules contractuels pour obtenir les dernières technologies innovantes à des prix compétitifs afin d'améliorer la sûreté et la sécurité générales. Les bons produits et les systèmes soigneusement conçus peuvent accroître l'efficacité et améliorer les opérations.

Les véhicules contractuels facilitent le processus d'achat et de budgétisation grâce à des prix prénégociés pour des offres concurrentielles garanties par des contrats d'appel d'offres. **Un véhicule contractuel est essentiellement une méthode rationalisée que les gouvernements nationaux et locaux utilisent pour acheter des biens et des services, des iPads aux ascenseurs.** Les contrats d'achat coopératif de Convergent garantissent notre capacité à obtenir des prix compétitifs pour nos clients.



En fin de compte, l'exploitation du pouvoir d'achat collectif de plusieurs organisations permet aux agences de garantir des prix compétitifs pour les produits et les services. En outre, le regroupement des besoins de tous les clients permet de normaliser les produits et les services, ce qui améliore la cohérence et l'efficacité des achats. Les coûts administratifs sont réduits du fait que les efforts sont partagés entre les entités. Les instruments contractuels de Convergent sont nombreux et ils facilitent tous les achats.

Utiliser les technologies de sécurité pour améliorer la compétitivité des entreprises ou des marques

La sécurité ne se limite pas à un seul aspect du bilan. La sécurité est une proposition vendable. Des espaces publics plus sûrs soutiennent la marque et la réputation de la ville. Cela attire à son tour les entreprises, les résidents et les visiteurs. La valeur est également présente pour les écoles. **Les collèges et les universités utilisent la question de la sécurité comme principal argument de vente pour recruter des étudiants et s'assurer le soutien de leurs parents.** La conclusion : un programme de sécurité bien fait peut faire une différence significative dans l'expérience du client et se prêter par la suite à une promotion en faveur de résultats commerciaux ciblés.

Résumé des recommandations, 2024

Les décideurs en matière de sécurité du SLED s'efforcent continuellement d'atteindre des objectifs à court et à long terme et, par conséquent, examinent les solutions qui pourraient être intégrées à leur plan actuel dans le respect des budgets prévus. Il est essentiel de commencer par la fin. C'est **pourquoi nous les invitons à prendre du recul et à collaborer avec un partenaire qui comprend l'espace.** La mise en place d'un plan de sécurité holistique sur 5 ans, voire sur 10 ans, est inestimable, même si certains des éléments inclus dans ce plan ne sont jamais mis en œuvre. Tous les défis doivent être pris en compte afin de découvrir toutes les solutions potentielles. Une feuille de route stratégique élimine les risques inhérents à la réaction et garantit une approche plus mesurée de la gestion des menaces. La première étape de la réussite est une évaluation complète de la sécurité. Il ne s'agit pas d'un poste budgétaire important et, en fin de compte, les bénéfices sont innombrables, à commencer par un meilleur contrôle des risques les plus importants pour les clients SLED : la planification réactionnelle et l'incapacité à réaliser une véritable intégration pour obtenir les meilleurs résultats.

L'équipe SLED de Convergent est prête à aider ses clients, qu'il s'agisse d'études complètes d'évaluation des sites de gestion des risques de sécurité de l'entreprise (ESRM) ou de solutions créatives et technologiquement puissantes en matière de subventions et d'aide au financement. Notre succès est attesté par celui de nos clients.