

The Savills logo, consisting of the word "savills" in a red, lowercase, sans-serif font, positioned within a yellow square.

REPORT 2026

Le bureau sous haute surveillance

CYBERSÉCURITÉ, EXIGENCES CROISÉES
POUR UN IMMEUBLE INTELLIGENT

The background of the entire page is a dark, high-tech illustration. It depicts a futuristic cityscape where the buildings are represented by glowing, vertical circuit traces and microchips. The city is set against a backdrop of a complex, glowing circuit board pattern. The overall color palette is dark blue and black, with vibrant yellow and orange highlights from the glowing elements. In the center, a large, square microchip is prominently featured, surrounded by a dense network of circuit lines. The bottom of the image features a yellow rectangular box with the word "RESEARCH" in black, uppercase letters.

RESEARCH

Cybersécurité, exigences croisées pour un immeuble *intelligent*

Hollywood l'avait pressenti avant l'industrie immobilière. Dans le blockbuster *Skyscraper* (2018), The Pearl, tour hyperconnectée de Hong Kong censée incarner l'immeuble le plus sûr au monde, se transforme en piège mortel après un simple accès dérobé à son système de sécurité.



“

la cybersécurité n'est plus un sujet informatique parmi d'autres, elle est devenue un sujet de conception, d'exploitation, de gouvernance et de valorisation immobilières.

Le scénario n'est plus seulement du cinéma. La digitalisation des immeubles a changé la donne : **la cybersécurité n'est plus un sujet informatique parmi d'autres, elle est devenue un sujet de conception, d'exploitation, de gouvernance et de valorisation immobilières.**

Et l'enjeu est loin d'être anecdotique, tant en termes de cibles potentielles que de coûts. **75% des GTB^{*1} (Gestion Technique du Bâtiment) installées dans le monde présenteraient au moins une vulnérabilité** connue et référencée sur un de ses éléments. Ce sont autant

¹ Claroty, spécialiste états-unien de protection des systèmes cyber-physiques, opérant en Amérique, en Europe et dans la zone Asie-Pacifique. State of CPS Security 2025: Building Management System Exposures, 2025 (échantillon international ; plus de 467 000 équipements de GTB dans 529 organisations couvrant l'immobilier commercial, le retail, l'hôtellerie, les data centers, l'industriel et la santé).

de portes ouvertes aux hackers. Inquiétant quand on sait que les installations de GTB se multiplient, encouragées par la réglementation environnementale et énergétique.

Le coût d'une cyberattaque via l'infrastructure d'un immeuble peut quant à lui très vite se chiffrer en millions d'euros, pour les propriétaires comme pour les locataires.

Un incident cyber affectant la GTB d'un immeuble de bureaux Prime peut entraîner un coût technique de remise en état compris entre 30 et 60 €/m². Toutefois, lorsque l'on intègre la perturbation opérationnelle, les compensations locataires, les coûts de gestion de crise et les pertes potentielles de revenus pendant la période de reconstruction (3 à 6 mois), l'exposition économique totale peut devenir beaucoup plus conséquente.

Au-delà des coûts techniques,



l'enjeu principal réside dans l'indisponibilité partielle ou totale du bâtiment. L'incapacité à exploiter normalement les systèmes de CVC*, de contrôle d'accès ou d'automatisation peut conduire à une dégradation temporaire des conditions d'occupation, à des demandes de compensation de la part des locataires et à une mobilisation importante des équipes de gestion et d'exploitation.

Tout cela sans compter qu'un incident majeur peut également avoir un impact réputationnel difficile à quantifier par rapport aux conséquences opérationnelles et financières directes.

Les cyberattaques provoquent enfin une rupture d'activité chez l'utilisateur. Bonne nouvelle : sa durée moyenne se réduit. 55% des organisations touchées s'en remettent en moins d'une semaine.

16% y parviennent même en moins d'une journée alors qu'elles n'étaient que 22% dans ce cas en 2023. Mais 28% doivent encore composer avec une remédiation d'une semaine à un mois, et 17% avec plus d'un mois d'indisponibilité².

Ce constat, et les exigences croissantes qu'il induit, vont redessiner en profondeur la conception, l'exploitation et l'usage des immeubles de bureaux. « **Les bâtiments devront démontrer leur capacité à sécuriser les appareils connectés, les réseaux et les données, tout comme on attend déjà d'eux qu'ils garantissent l'efficacité énergétique et le confort des occupants** », résume Péroline Prévost-Manseau, Head of Agency and Workthere chez Savills France.

² Sophos : State of Ransomware 2026, Juillet 2026 (enquête menée auprès de 2 158 responsables IT et sécurité dans 17 pays)

75%

DES GTB (GESTION TECHNIQUE DU BÂTIMENT) INSTALLÉES DANS LE MONDE PRÉSENTERAIENT AU MOINS UNE VULNÉRABILITÉ

1. Conception des bâtiments : construire « *security by design* »

Architecture réseau dès la phase de design de l'immeuble : La segmentation réseau n'est plus une option de fin de chantier, c'est un prérequis de conception. Le nouveau réflexe : séparer par VLAN* les flux de GTB, de contrôle d'accès, de vidéosurveillance, de Wi-Fi invité et de données locataires. Sans cela, une simple machine à café connectée peut ouvrir la porte aux serveurs financiers d'un locataire.

Aucune statistique consolidée

ne mesure la part des immeubles de bureaux dotés d'une architecture VLAN en France. Le sujet est trop récent, trop technique, pour avoir fait l'objet d'une étude dédiée. Mais plusieurs indicateurs indirects permettent d'en cerner l'ampleur et la maturité :

- Le cadre normatif est tout juste né. L'ANSSI* a publié le 27 avril 2026 son premier guide dédié à la cybersécurité des GTB/GTC* (référence ANSSI-PA-110) :

26 recommandations, dont le cloisonnement et le filtrage des protocoles. Une doctrine aussi récente signifie que la segmentation par VLAN dès la conception reste une bonne pratique émergente, pas encore une norme de marché. La plupart des immeubles existants ont été conçus avant qu'elle n'existe.

- Le taux de « bâtiments connectés » donne un plafond. Seuls 16% des immeubles sont aujourd'hui équipés de GTB, loin des objectifs



du décret BACS*. Autrement dit : la cybersécurité GTB ne peut concerner, au mieux, qu'une fraction de ce sous-ensemble. Un immeuble sans GTB n'a pas cette surface d'attaque - mais n'en a pas non plus les bénéfices.

- Le calendrier du décret BACS donne le tempo :

- o Seuil de 290 kW de puissance CVC : conformité requise depuis le 8 janvier 2025.
- o Le seuil intermédiaire (70-290 kW) a été prorogé de 2027 à 2030 par un décret du 26 décembre 2025.

Le parc de bureaux équipé de GTB va donc s'élargir dans les prochaines années et avec lui, mécaniquement, le nombre d'immeubles exposés au risque cyber. D'où une pression croissante pour intégrer les recommandations de l'ANSSI dès l'installation.

Les foncières commencent à

en parler. Covivio le résume bien : les immeubles de bureaux sont devenus « smart », hyperconnectés, avec une GTB de plus en plus ouverte et l'arrivée de systèmes d'exploitation de bâtiment (BOS*) - le tout dans un contexte désormais majoritairement multi-locataires. Le ton, pédagogique, celui d'une prise de conscience, trahit un sujet encore traité comme une démarche volontaire différenciante, pas comme un standard vérifié et audité.

En croisant le parc de bureaux francilien, le taux de déclaration OPERAT³ et les seuils des décrets BACS⁴, on peut avancer que :

- Le parc soumis à l'obligation GTB (>290 kW, essentiellement les immeubles moyens à grands) représente probablement 60 à 75% de la surface totale du parc francilien, en partant du principe que les petites

unités (<1 000-2 000 m²) sont nombreuses en nombre mais pèsent moins en surface cumulée.

- Sur ce sous-ensemble, seule une fraction - inconnue, mais vraisemblablement très faible - répond aux critères de sécurisation réseau (segmentation VLAN, chiffrement, gouvernance RSSI*/OT*).

En clair : l'essentiel du parc francilien reste hors du périmètre de sécurisation cyber formalisé.

Non par choix, mais parce que la majorité des immeubles n'a pas encore de GTB au sens du décret - et que, pour la petite minorité qui en a une, la doctrine de sécurisation n'existe que depuis avril 2026.

³ Le taux de déclaration OPERAT (proxy de «parc suivi/piloté») : Le bilan OPERAT 2025 analyse environ 740 000 déclarations représentant 57 % de la surface du parc tertiaire assujetti, avec une progression par rapport aux 750 000 déclarations enregistrées fin 2023-début 2024 représentant 46 % du parc. À l'échelle nationale, les bureaux, avec l'enseignement, la santé, la logistique et le commerce, concentrent environ 80 % des surfaces et consommations déclarées, avec un ratio moyen de consommation de 110 kWh/m²/an pour les bureaux.

⁴ Les seuils du décret BACS (proxy de «parc GTB obligatoire») : Pour le seuil d'au moins 290 kW de puissance CVC, la conformité GTB est obligatoire depuis le 8 janvier 2025. Le seuil intermédiaire de 70-290 kW a été reporté de 2027 à 2030 par un décret du 26 décembre 2025.



Protocoles et équipements

certifiés : Les protocoles historiques du bâtiment - BACnet/IP, KNX, Modbus* - ont un point faible commun : ils n'ont pas prévu le chiffrement. Sans lui, les données transitent en clair, lisibles par quiconque intercepte le flux réseau. Résultat : le bâtiment est exposé aux attaques de type Man-in-the-Middle*, et le rebond depuis un poste utilisateur compromis devient un jeu d'enfant. D'où la bascule des nouveaux projets vers des capteurs et contrôleurs certifiés IEC 62443*, aux micrologiciels signés numériquement.

BACnet (*Building Automation and Control Network*) date des années 1990, une époque où les réseaux de bâtiment étaient physiquement isolés et où la cybersécurité n'était pas un sujet. Le protocole a été pensé pour faire dialoguer les équipements entre eux, pas pour protéger la confidentialité des échanges.

Concrètement :

- Les commandes envoyées ; « ouvrir la vanne de chauffage », « désactiver le badge d'accès X » ; circulent en clair sur le réseau ;
- Les identifiants de connexion aux automates transitent eux aussi sans protection ;

- N'importe qui ayant un accès physique ou logique au réseau technique (port Ethernet non protégé, Wi-Fi mal cloisonné, objet IoT* compromis) peut potentiellement lire ces échanges, voire les modifier.

D'où deux types d'attaques :
- L'écoute passive : un attaquant lit les échanges pour cartographier le système, comprendre son fonctionnement ou récupérer des identifiants ;

- Le Man-in-the-Middle : l'attaquant s'insère dans la communication et modifie les commandes à la volée - couper le chauffage, désactiver une alarme incendie, débloquer un accès - sans que le système puisse vérifier l'origine de l'ordre.

Une extension plus récente, BACnet/SC (*Secure Connect*), ajoute une couche de chiffrement TLS*. Mais son adoption reste partielle : elle exige souvent de remplacer ou mettre à jour des équipements existants.

Ces vulnérabilités ne sont pas qu'un risque théorique : une étude de Claroty portant sur plus de 467 000 équipements de GTB dans 529 organisations dans le monde montre que 75% d'entre elles exploitent au moins un équipement porteur d'une vulnérabilité déjà

recensée comme exploitée dans des attaques réelles, et 69% une vulnérabilité déjà mobilisée spécifiquement dans des attaques par rançongiciel⁵.

Convergence IT* / OT : La frontière entre réseau bureautique (IT) et réseau technique (OT - ascenseurs, CVC, sécurité incendie) doit se penser en amont, avec une architecture « security by design » plutôt qu'un rustinage après livraison.

Pour un immeuble de bureaux (hors industrie lourde), cette convergence se traduit concrètement par :

- Un inventaire exhaustif des équipements techniques connectés
- souvent inexistant aujourd'hui ;
- Une gouvernance partagée entre DSI*/RSSI et facility/property management, sans attendre une fusion complète des équipes ;
- Des clauses cyber systématiques dans les contrats de maintenance GTB et dans les baux, notamment multi-locataires ;
- Un cloisonnement maintenu sur les systèmes vitaux, même quand les données convergent.

Quatre chantiers sont à mener de front : technique, organisationnel, gouvernance, contractuel.

Côté technique :

- Segmentation et architecture réseau : au-delà du simple cloisonnement VLAN, la convergence IT/OT impose de définir des zones et des « conduits » - un modèle de défense en profondeur où chaque système technique (GTB, contrôle d'accès, vidéosurveillance, ascenseurs) est isolé, avec des points de passage strictement contrôlés vers le réseau IT.
- Inventaire des actifs, l'étape trop souvent négligée : recenser les équipements ne suffit pas, il faut aussi savoir ce qui tourne dessus - logiciels, firmwares, systèmes d'exploitation, côté IT comme côté OT. C'est ce défaut de visibilité qui a conduit certains régulateurs à envisager d'exiger une nomenclature logicielle (SBOM), à l'image des attaques par la chaîne d'approvisionnement - Sunburst/SolarWinds, Kaseya.
- Chiffrement et intégrité des données : un savoir-faire IT à appliquer en concertation avec l'OT, sans « plaquer » brutalement des standards conçus pour un autre monde — même logique que pour BACnet/SC.

Côté organisation :

- Rapprocher deux cultures, pas les fusionner d'autorité : les équipes IT, sous la houlette de la DSI et du RSSI, doivent désormais s'intéresser aux systèmes techniques du bâtiment. Réciproquement, les équipes historiques de ces systèmes, dont la seule obligation était de les maintenir en état de marche,

voient peu d'intérêt à l'arrivée de l'IT dans leur périmètre - d'autant que ces installations ont souvent été financées sur des budgets métiers, sans lien avec l'IT.

- Des modèles progressifs plutôt qu'une fusion brutale : certaines organisations intègrent un référent IT dans l'équipe technique/OT, d'autres - plus rares - fusionnent directement les deux services. Dans tous les cas, c'est le travail concerté entre les équipes qui protège réellement contre le risque cyber.

EDF en donne un exemple éclairant même s'il est hors immobilier. Chez l'énergéticien, l'enjeu est d'avoir une gouvernance commune sur les sujets partagés (menace, trajectoires de sécurité) tout en maintenant le cloisonnement des environnements, selon un principe simple : plus un système est critique, plus il doit être isolé. Transposé à un immeuble de bureaux : gouvernance de sécurité unifiée, mais isolement physique maintenu pour les systèmes vitaux — sécurité incendie, contrôle d'accès.

Côté gouvernance :

- Élargir le périmètre du RSSI : la GTB doit intégrer le périmètre de cybersécurité global de l'organisation. Il faut nommer un responsable GTB/OT dédié ou étendre explicitement la mission du RSSI, et inclure la GTB dans l'analyse de risque et les plans de continuité d'activité.
- NIS2*, accélérateur de structuration : la directive agit comme un catalyseur de gouvernance et un levier de professionnalisation. Sécuriser ses opérations, c'est démontrer sa capacité à produire en conformité et inspirer confiance à

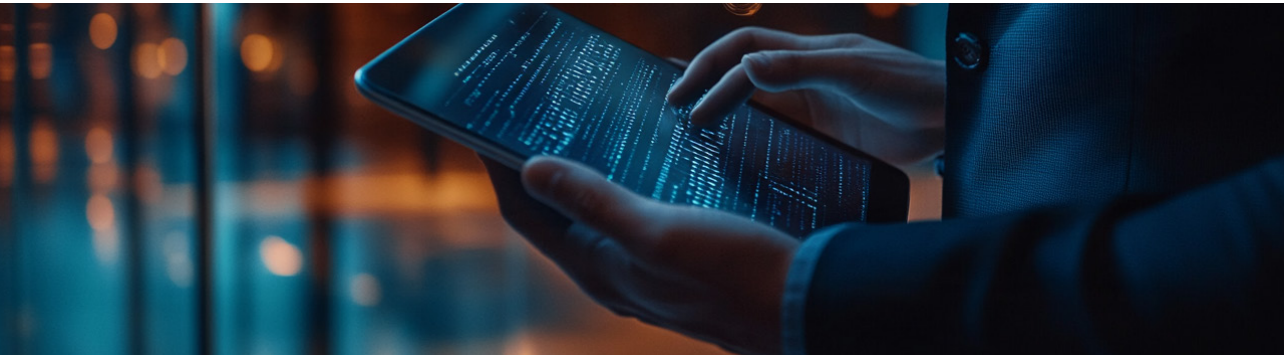
ses partenaires. À l'inverse, ignorer la convergence OT/IT fragilise l'entreprise au moment même où elle cherche à se transformer.

Côté contrats et achats :

Pour une foncière ou un asset manager, le point le plus actionnable est sans doute d'imposer des clauses de cybersécurité dans les appels d'offres - nomenclature logicielle (SBOM), journalisation des accès, plan de remédiation en cas d'incident - et d'intégrer la GTB dans les exercices de gestion de crise, avec une formation dédiée des équipes.

Impossible aujourd'hui de chiffrer combien d'immeubles ont formalisé cette convergence IT/OT en s'appuyant sur la norme IEC 62443 ou les recommandations ANSSI-PA-110. Une chose est sûre : ils sont ultra-minoritaires. Trop de propriétaires ne sont pas encore sensibilisés, et le temps de développement ou de restructuration d'un immeuble est trop long pour qu'il en soit autrement. Pour l'instant. Car les choses vont changer vite.

La prise de conscience est en marche. Un investisseur institutionnel international a par exemple récemment fait de la restructuration d'un actif parisien de 24 000 m² un cas pilote d'adaptation aux exigences de cybersécurité. Reste maintenant à confronter cette adaptation à la deuxième phase de la vie de l'immeuble : sa gestion et son exploitation.

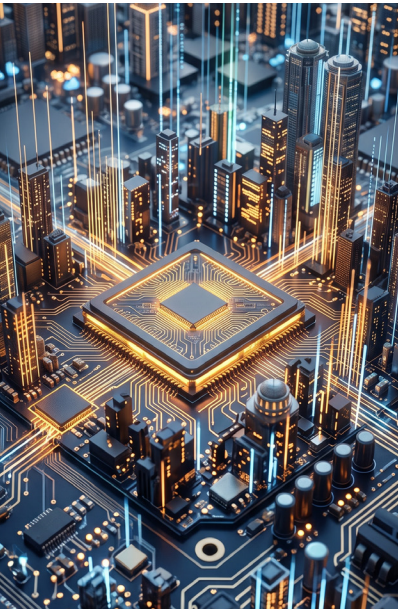


⁵ Claroty, op.cit. Le chiffre de 75% désigne les organisations dont au moins un équipement de GTB est affecté par une vulnérabilité «KEV» (Known Exploited Vulnerability) — c'est-à-dire une faille répertoriée, notamment dans le catalogue de l'agence américaine de cybersécurité CISA, comme ayant déjà été exploitée par des attaquants dans des attaques réelles documentées ailleurs que dans les équipements étudiés. Il mesure donc une exposition à un risque avéré par ailleurs, et non un piratage constaté dans ces bâtiments précis.

2. Gestion et exploitation : la cybersécurité au quotidien de *l'exploitation*

Pour ce propriétaire, ainsi que pour ses prestataires (dont Savills France, via son entité Property Management), ce déploiement passe désormais par phase d'audit et de vérification, par l'activation des services MSSP*, la gouvernance cyber-physique complète, le gap analysis et la coordination.

Plus largement, et au-delà de ce cas d'espèce, la gestion et l'exploitation des immeubles de bureaux s'apprennent à connaître de profondes évolutions sous l'effet des exigences de cybersécurité.



Cadre réglementaire structurant : La directive européenne NIS2 est le principal levier réglementaire. Elle impose des exigences strictes en cybersécurité aux infrastructures connectées - notamment aux collectivités de plus de 30 000 habitants - sous peine de risques physiques, financiers et juridiques majeurs. Plus largement, elle renforce la cybersécurité des infrastructures critiques, y compris les bâtiments intelligents : les référentiels applicables incluent désormais ISO 27001*, IEC 62443, le RGPD* et les recommandations de l'ANSSI.

Gestion des accès et des identités : La gestion technique des bâtiments souffre d'une hygiène de sécurité historiquement faible. L'usage massif d'identifiants par défaut type « admin/admin » offre une porte d'entrée facile aux malwares, capable de mener à une prise de contrôle totale via l'API* d'administration. Les property managers doivent désormais imposer une gestion stricte des accès : identifiants uniques et tracés, authentification forte, supervision par le RSSI. Cela s'étend aux accès distants, au MFA*, à l'Identity & Access

Management, au monitoring et à la sécurisation des accès tiers.

L'onboarding et l'offboarding des mainteneurs, la suppression des accès en fin de contrat, la traçabilité et la gestion des comptes administrateurs doivent être encadrés par un acteur identifié contractuellement, pour limiter les risques.

Au-delà de cette gestion stricte des accès, l'impact sera bien plus large. Le property manager va devoir intégrer la cybersécurité au cycle normal de gestion technique de l'immeuble :

- **Contrats de maintenance** : des clauses cyber dans les marchés GTB, contrôle d'accès, CCTV*, ascenseurs, IoT, BOS - gestion des comptes, accès distants, patching, journalisation, notification des incidents, sauvegardes, suppression des accès en fin de contrat.
- **Onboarding/offboarding des prestataires** : aucun mainteneur ne devrait garder indéfiniment un accès distant après la fin de son contrat.
- **Travaux** : toute installation d'un équipement connecté devrait déclencher une question systématique dans le processus travaux : « *Comment cet équipement est-il raccordé au réseau, et qui assurera sa cybersécurité pendant son exploitation ?* »

• **Gestion des incidents** : un défaut GTB n'est plus forcément un simple incident technique. Une perte de communication, des consignes modifiées ou des équipements indisponibles peuvent exiger une qualification cyber.

- **PCA* immobilier** : prévoir des modes dégradés pour continuer à exploiter le bâtiment si certains systèmes numériques tombent.
- **Handover*** : les DOE* devraient bientôt inclure, au-delà des plans techniques, l'architecture réseau, l'inventaire des équipements connectés, les versions firmware/software, la matrice des accès, les sauvegardes et les responsabilités d'administration.
- **Pilotage fournisseurs** : le property manager devient le garant de l'existence et de l'application du processus — sans devenir lui-même RSSI ou opérateur cybersécurité.

Pour le property manager, la cybersécurité ne veut pas dire devenir expert informatique. Son rôle évolue vers celui d'un orchestrateur de la gouvernance cyber de l'immeuble : identifier les systèmes et leurs responsables, encadrer contractuellement les prestataires, contrôler les accès, organiser la remontée des incidents, s'assurer que les exigences du propriétaire sont bien appliquées tout au long du cycle de vie de l'actif.

Risques opérationnels concrets : Les cas réels de cyberattaques sur des entreprises, des administrations et des collectivités françaises ou étrangères ne manquent pas. Pour un actif tertiaire, l'équivalent serait un ransomware* paralysant les

ascenseurs, le contrôle d'accès ou la supervision incendie.

Une distinction s'impose :
- Les attaques sur la **GTB/OT physique** - ascenseurs, alarmes incendie, contrôle d'accès, CVC - restent rares, mais avec un potentiel de gravité élevé ;
- Les attaques sur les **systèmes IT/gestion locative** sont, elles, beaucoup plus fréquentes (avec par exemple celles dont ont été victimes le promoteur newyorkais Glenwood Management ou le courtier immobilier Premier Realty Group en 2025) - elles touchent la donnée plutôt que le bâtiment lui-même.

Le risque théorique le plus grave, selon un rapport de Lockton⁶, l'un des plus grands courtiers indépendants en assurances, qui dispose d'une pratique dédiée à l'immobilier et aux risques cyber : une attaque par ransomware sur un immeuble intelligent pourrait affecter le système d'alarme incendie ou désactiver les ascenseurs, avec des conséquences potentiellement fatales en cas d'urgence.

Les cas documentés existent, même si les attaques ciblant spécifiquement le bâtiment (BMS*/BAS*) restent rares comparées aux attaques classiques sur les systèmes IT/finance des sociétés immobilières.

Le cas de référence reste l'attaque BAS en Allemagne (2021), l'exemple le plus cité en cybersécurité immobilière.

Des cybercriminels ont pris le contrôle de centaines d'appareils KNX/BACnet - éclairage, détecteurs de mouvement, volets - dans un parc de bureaux allemand, et les ont « briqués » : tout a été effacé, sans fonctionnalité résiduelle. La société d'ingénierie gestionnaire a dû faire appel à des experts en cybersécurité industrielle (Limes Security) pour restaurer le système, en récupérant la clé de sécurité directement dans la mémoire d'un appareil compromis.

D'autres cas existent :
• **Paralysie de systèmes de property management** : plusieurs incidents ont été documentés où l'attaque a rendu impossible l'utilisation du système de gestion immobilière, bloquant paiements locataires, baux et plannings de maintenance - sans toucher aux équipements physiques.

• **Kaseya (2021)** : la cible directe n'était pas un immeuble de bureaux, mais cette attaque contre un fournisseur de logiciels de gestion IT a paralysé plus de 1 500 organisations dans le monde - illustrant le risque de supply chain pour les gestionnaires d'actifs qui externalisent leur GTB.

• **Alexandria Real Estate Equities**, foncière cotée américaine, reconnaît explicitement dans son rapport annuel 2025 que des attaques par ransomware sévères pourraient interrompre significativement ses opérations et pénaliser l'accès des locataires à ses immeubles. Un risque anticipé plutôt qu'un incident avéré - mais révélateur : le sujet est désormais matériel pour les REIT*.



⁶ Lockton : «Why ransomware attacks pose a unique threat to real estate», février 2022

3. Occupation et usages d'un immeuble connecté : entre exigence et confort

Attentes des locataires : Les grands utilisateurs - banques, cabinets d'avocats, groupes internationaux - intègrent désormais des clauses de cybersécurité dans leurs due diligences* immobilières : architecture réseau, cloisonnement entre locataires, politique d'accès aux systèmes techniques. Un critère de sélection d'actif désormais comparable à la performance énergétique.

WiredScore l'a bien senti et accompagne plusieurs propriétaires immobiliers de premier plan en Europe à travers leur nouvelle offre Cyber Foundations. Cette évaluation de la cybersécurité spécifiquement conçue pour le secteur immobilier permet d'apporter davantage de clarté aux différentes parties prenantes - techniques comme non techniques - des politiques et procédures de cybersécurité des bâtiments et des technologies opérationnelles. Elle propose une approche structurée permettant à tous les bâtiments d'améliorer leur niveau global de cyber-résilience.

Le label SmartScore, lancé en avril 2021, intègre par ailleurs la cybersécurité dans son offre

de labellisation, afin d'aider les utilisateurs à évaluer les performances cyber des actifs immobiliers. L'écho est réel, même si les exemples viennent pour l'instant surtout du marché américain. L'immeuble 17xM, à Washington DC, est l'un des tous premiers actifs tertiaires labélisés SmartScore en Amérique du Nord - une labellisation qui a convaincu le cabinet d'avocats Gibson, Dunn & Crutcher LLP de signer un bail sur la moitié de l'immeuble, qui développe 31 000 m² sur 11 étages. Le promoteur Skanska avait construit le projet en connaissant précisément les exigences technologiques de ce type de locataire - une forme de « *build-to-suit* » technologique.

À New York, pour les salles de marché et les utilisateurs de la finance, du droit, de la santé ou de la production créative, la labellisation SmartScore Platinum est devenue un critère de sélection. Dans Midtown South et Hudson Yards, la labellisation WiredScore Platinum semble faire pencher la balance entre deux immeubles — particulièrement pour les cabinets d'avocats et les salles de marché : les garanties de double

entrée fibre optique réduisent le risque d'interruption, un facteur jugé plus déterminant que l'écart de loyer.

Les évolutions apportées aux baux sont, elles, plus difficiles à cerner : ces clauses, quand elles existent, restent des annexes techniques confidentielles de baux privés jamais publiées.

Ces exigences transforment aussi le processus de prise à bail : la due diligence cybersécurité allonge et complique les délais de négociation, avec de nouvelles exigences documentaires côté bailleur — inventaire des équipements connectés, preuves d'audits de sécurité, garanties de double raccordement fibre — absentes des due diligences immobilières classiques. Pour les locataires réglementés (finance, avocats, santé), cette vérification s'ajoute désormais aux due diligences juridiques et financières habituelles, et peut devenir un facteur de retard si l'immeuble visé manque de documentation.

Multi-tenant et cloisonnement : Dans les immeubles multi-locataires, l'enjeu est d'éviter toute contamination croisée entre les

réseaux techniques du propriétaire et les systèmes d'information des occupants. Un sujet qui touche directement les baux et leurs clauses techniques - d'autant que les attentes diffèrent selon que le locataire héberge ses données dans le cloud ou sur des réseaux qu'il contrôle. D'où l'intérêt, pour les propriétaires, de proposer des réseaux et signaux Wi-Fi distincts par locataire.

Concrètement, pour l'utilisateur final, cela se traduit par plus de friction : impossible de se connecter simplement au réseau de l'immeuble sans validation préalable, contrôle renforcé sur les objets IoT personnels, authentification forte parfois exigée pour des usages aussi basiques que réserver une salle de réunion. Une friction nécessaire côté sécurité, mais à anticiper dès la conception de l'expérience utilisateur afin de ne pas entraver l'adoption des outils numériques mis à disposition des occupants.

Sensibilisation et montée en compétence des utilisateurs : Au-delà des dispositifs techniques, l'humain reste le vecteur d'attaque le

plus courant : identifiants par défaut jamais changés, mots de passe faibles, hameçonnage. D'où une sensibilisation à deux niveaux : les équipes d'exploitation technique, historiquement peu formées, doivent recevoir une formation dédiée à l'hygiène numérique ; les occupants eux-mêmes deviennent une cible de sensibilisation croissante, pour limiter les risques liés aux équipements personnels connectés ou au partage d'identifiants.

Applications d'expérience locataire et données personnelles : Les applications d'expérience locataire - réservation de salles, gestion des services, contrôle d'accès - simplifient l'usage quotidien de l'immeuble. Mais elles génèrent, en contrepartie, une nouvelle collecte de données personnelles : déplacements, horaires de présence, préférences d'usage. Une collecte à encadrer par des politiques de confidentialité conformes au RGPD - un point que les locataires réglementés (avocats, santé) examinent de près avant de déployer ces outils à l'échelle de leurs équipes. Le sujet rejoint celui de la gouvernance

des données générées par les systèmes techniques du bâtiment.

Un équilibre à trouver entre sécurité et fluidité d'usage : Le fil conducteur de ces évolutions doit être de trouver l'équilibre entre sécurisation et fluidité d'usage. Les solutions les plus abouties (identifiants mobiles, biométrie) visent justement à renforcer la sécurité sans dégrader l'expérience : accès mains libres, révocation instantanée des droits, suppression du contact physique.

Mais cet équilibre reste fragile. Des contrôles mal calibrés génèrent des frictions, des sollicitations répétées du support technique et, in fine, un risque de contournement des procédures par les utilisateurs eux-mêmes. À l'inverse, un défaut de contrôle expose l'immeuble à un incident. Une tension qui invite les property managers à traiter la cybersécurité non comme une contrainte isolée, mais comme un critère à part entière de l'expérience occupant.

¹ Le taux de déclaration OPERAT (proxy de « parc suivi/piloté ») : Le bilan OPERAT 2025 analyse environ 740 000 déclarations représentant 57 % de la surface du parc tertiaire assujetti, avec une progression par rapport aux 750 000 déclarations enregistrées fin 2023-début 2024 représentant 46 % du parc. À l'échelle nationale, les bureaux, avec l'enseignement, la santé, la logistique et le commerce, concentrent environ 80 % des surfaces et consommations déclarées, avec un ratio moyen de consommation de 110 kWh/m²/an pour les bureaux.

² Les seuils du décret BACS (proxy de « parc GTB obligatoire ») : Pour le seuil d'au moins 290 kW de puissance CVC, la conformité GTB est



Conclusion : implications sur le marché immobilier et *le cas parisien*

La cybersécurité s'apprête à devenir un nouveau facteur de différenciation des actifs — en valorisation comme en obsolescence :

- Valorisation : un immeuble « cyber-sécurisé » - GTB segmentée, certifications, gouvernance IT/OT documentée — pourrait devenir un argument de prime locative ou d'investissement, en particulier pour les actifs premium destinés aux locataires réglementés (finance, santé, secteur public).

- Obsolescence technique : les immeubles équipés de GTB anciennes, aux protocoles non chiffrés, pourraient nécessiter des capex de mise à niveau ; un facteur à intégrer aux analyses de vacance et d'obsolescence, aux côtés du critère énergétique.

Paris illustre déjà concrètement cette dynamique.

Publié fin 2026, le rapport Insights 2026 de WiredScore introduit un nouveau Global Cities Resilience Index, qui évalue la cyber-résilience de plus de 40 villes dans le monde à partir des données de labellisation WiredScore et SmartScore. Un indice qui ne mesure pas le parc de bureaux dans son ensemble, mais seulement les 1 652 immeubles labellisés WiredScore/SmartScore de l'échantillon — les villes n'y figurant que si elles atteignent un seuil minimum de labellisations.

Deux réserves s'imposent donc

pour lire les résultats parisiens :

- Comparabilité limitée : le score parisien reflète la performance des immeubles labellisés WiredScore dans la capitale - un sous-ensemble premium et récent - et non la moyenne du parc de bureaux francilien.

- Auto-sélection des « meilleurs élèves » : les propriétaires qui engagent une démarche de labellisation sont, par essence, déjà ceux qui investissent le plus dans la connectivité et la résilience de leurs actifs. L'échantillon capte une frange volontairement engagée, pas la moyenne du marché.

Ces réserves posées, les données restent instructives. Dans le référentiel SmartScore, la cyber-résilience correspond à la moyenne de quatre catégories : accès et navigation, cybersécurité, gestion des données, sûreté et sécurité. Paris affiche de bons fondamentaux sur les indicateurs de gouvernance - gestion des données (74%) et sûreté et sécurité (90%) — devançant Londres sur ces deux critères, au même niveau que Barcelone et Berlin. Le score global de cyber-résilience parisien (61%) est en revanche pénalisé par deux catégories plus opérationnelles : la cybersécurité (43%) et l'accès et la navigation (60%)

- identifiées par WiredScore comme des axes d'investissement ciblés et rapidement actionnables (sécurisation des contrôles d'accès physique et des technologies opérationnelles).

Ce diagnostic ciblé recoupe un constat plus large : Paris, comme Berlin et Munich, est explicitement cité dans Insights 2026 comme étant en retrait sur les piliers numérique et cyber par rapport à des marchés plus matures comme Madrid — un écart qui s'explique notamment par le vieillissement du parc immobilier.

Moins que d'une sous-performance parisienne, ces résultats témoignent d'un parc disposant déjà de solides fondamentaux de gouvernance, avec une trajectoire d'amélioration concentrée sur un nombre restreint de leviers opérationnels. Si Paris a de bons élèves, ils sont encore trop peu nombreux.

Chez Savills, nous suivons ce sujet de près depuis plusieurs mois, au travers de nos échanges avec investisseurs, property managers et locataires. Nous continuerons à documenter cette transformation à mesure qu'elle redessine la conception, la gestion et l'occupation des immeubles de bureaux.

3 QUESTIONS À NATALIA TURKIEWICZ,
DIRECTOR OF BUSINESS DEVELOPMENT WIREDSCORE



01
Que recouvre le volet cybersécurité du label SmartScore ?

La catégorie Cybersécurité vise à garantir que les bâtiments disposent d'une stratégie de cybersécurité complète et d'une conception réseau sécurisée, afin d'offrir aux occupants un environnement de bâtiment intelligent sûr et fiable, dans lequel les données et les opérations sont protégées. Le secteur immobilier prend progressivement conscience que le risque cyber ne se limite plus aux environnements informatiques (IT) des entreprises. Il s'étend désormais à l'ensemble des technologies qui assurent le fonctionnement de nos bâtiments : systèmes de gestion technique du bâtiment, contrôle d'accès, vidéosurveillance, ainsi qu'au nombre croissant d'équipements connectés qui sous-tendent les opérations modernes. Au cours de la dernière décennie, l'adoption des technologies de smart building a connu des progrès rapides : davantage de données, davantage d'automatisation et une amélioration de l'expérience utilisateur. Mais cette transformation numérique a également créé de nouveaux points d'entrée potentiels pour les cyberattaquants. Comparés aux ordinateurs portables et aux smartphones, les systèmes technologiques des bâtiments ne sont connectés à Internet que depuis relativement peu de temps. Ils rejoignent pourtant un environnement numérique déjà mature, dans lequel les acteurs malveillants disposent de méthodes très sophistiquées pour

identifier et exploiter les équipements vulnérables. Nous évaluons la cyber-résilience à travers les trois piliers suivants : - Gestion des équipements : Il s'agit de savoir précisément quelles technologies sont présentes au sein d'un actif immobilier et qui est responsable du maintien de la cybersécurité de chaque équipement. À mesure que le nombre de technologies installées augmente, disposer d'une visibilité complète et d'un modèle clair de responsabilités devient essentiel pour mettre en œuvre une stratégie de cybersécurité crédible. - Gouvernance : Il s'agit d'intégrer les technologies du bâtiment aux politiques, aux processus de gestion des risques et aux programmes de formation déjà en place pour les ordinateurs portables et les téléphones professionnels. Sans cet alignement, les systèmes du bâtiment restent en dehors des structures habituelles de responsabilité, créant ainsi des angles morts dans la gestion des risques. - Mesures de protection : La mise en place de mesures de cybersécurité consiste à anticiper les problèmes plutôt qu'à réagir une fois qu'un incident s'est produit. Les fondamentaux sont essentiels. Des pratiques opérationnelles simples, comme la bonne gestion des identifiants et des accès, peuvent faire une réelle différence. Il est surprenant de constater à quel point l'application rigoureuse et systématique de ces principes de base permet déjà de se situer bien au-dessus de la majorité du marché.

02
Selon les données d'Insights 2026, Paris obtient de bons résultats sur la gouvernance (gestion des données, sûreté et sécurité) mais reste en retrait sur la cybersécurité et l'accès et la navigation. Quelles recommandations concrètes formuleriez-vous aux investisseurs et property managers franciliens pour progresser sur ces deux axes ?

Dans le cadre de nos recherches, nous avons été surpris par le manque de visibilité du secteur immobilier sur le nombre d'équipements technologiques installés au sein des bâtiments. La première étape fondamentale consiste donc à améliorer la gestion des équipements : savoir précisément quels équipements sont présents dans le bâtiment, qui est responsable de leur maintenance, qui peut y accéder, et si - et comment - ils sont connectés au reste du réseau du bâtiment ainsi qu'à Internet. À partir de cette base, les bâtiments peuvent mettre en œuvre plus efficacement des mesures visant à renforcer leur cyber-résilience et, plus largement, la résilience globale de leur infrastructure technologique.

03
Comment la dynamique observée en France se compare-t-elle à celle des autres grands marchés européens et nord-américains ?

La France, et plus particulièrement l'Île-de-France, connaît une adoption croissante du Smart Building et de la labellisation SmartScore. Paris dispose néanmoins encore d'une marge de progression, notamment en matière de résilience digitale et cyber. Un constat que l'on retrouve dans plusieurs grandes métropoles européennes, notamment en raison d'un parc immobilier plus ancien. Certains marchés matures démontrent toutefois qu'il est possible d'atteindre des niveaux élevés de résilience : c'est notamment le cas de Madrid en Europe ou de Chicago en Amérique du Nord. Plus largement, nos données mettent en évidence une forte dynamique en Asie-Pacifique et au Moyen-Orient, où les infrastructures digitales sont davantage pensées et intégrées dès la conception des bâtiments.

Glossaire

Cybersécurité et bâtiments connectés

Classé par ordre alphabétique

ANSSI (Agence Nationale de la Sécurité des Systèmes d'Information) : Autorité française de référence en cybersécurité, qui émet recommandations et alertes notamment sur les infrastructures critiques.

API (Application Programming Interface) : Interface logicielle qui permet à deux systèmes informatiques de communiquer et d'échanger des données ou des commandes de façon standardisée — par exemple entre une GTB et son logiciel de supervision.

BACnet/IP, KNX, Modbus : Protocoles de communication standards utilisés par les équipements techniques du bâtiment (automates, capteurs, contrôleurs) pour dialoguer entre eux. Ce sont des protocoles anciens, conçus avant les enjeux cyber actuels, souvent sans chiffrement natif.

BACS (Building Automation and Control Systems) : Cadre réglementaire européen, transposé en France par le décret du même nom, qui impose l'installation de systèmes d'automatisation et de contrôle du bâtiment au-delà de certains seuils de puissance CVC (chauffage, ventilation et climatisation). À ne pas confondre avec BAS (Building Automation System), qui désigne l'équipement lui-même.

BAS (Building Automation System) : Voir GTB

BMS en anglais (Building Management System) : Voir GTB

BOS (Building Operating System) : Système d'exploitation ou plateforme logicielle centrale qui agrège et pilote l'ensemble des systèmes techniques d'un bâtiment (CVC, éclairage, sécurité, accès, énergie) au sein d'une interface unique. C'est l'équivalent d'un « cerveau » numérique du bâtiment, souvent présenté comme une couche au-dessus de la GTB classique pour permettre l'interopérabilité entre systèmes de fournisseurs différents.

CCTP (Cahier des Clauses Techniques Particulières) : Document contractuel français, pièce centrale d'un marché ou d'un appel d'offres, qui détaille les spécifications techniques précises d'une prestation ou d'un ouvrage (matériaux, normes, performances attendues, méthodes). En property management, il encadre par exemple les contrats de maintenance technique, de nettoyage, de sécurité ou de travaux, en fixant noir sur blanc ce qui est exigé du prestataire.

CCTV (Closed-Circuit Television) : Système de vidéosurveillance en circuit fermé (caméras + enregistrement + supervision) utilisé pour la sécurité physique d'un immeuble : contrôle des accès, surveillance des parties communes, parkings, halls. De plus en plus connecté aux réseaux IP du bâtiment, ce qui en fait un point d'entrée potentiel à sécuriser (lien avec le MSSP).

CVC (Chauffage, Ventilation et Climatisation) : Ensemble des équipements et systèmes qui régulent la température, la qualité de l'air et le confort thermique d'un bâtiment : - **Chauffage** : chaudières, pompes à chaleur, radiateurs - **Ventilation** : renouvellement de l'air, extraction, VMC (ventilation mécanique contrôlée) - **Climatisation** : refroidissement, groupes froids CVC est l'équivalent français de l'acronyme anglais HVAC (Heating,

Ventilation, and Air Conditioning). **DBO (Design-Build-Operate)** : Modèle contractuel où un même prestataire (souvent un groupement) est en charge à la fois de la conception, de la construction et de l'exploitation d'un actif ou d'un système sur une durée donnée. Utilisé notamment sur des infrastructures ou équipements techniques d'un immeuble (CVC, énergie, etc.) pour éviter la multiplication d'intervenants entre la phase travaux et la phase exploitation. **DOE (Dossier des Ouvrages Exécutés)** : Document contractuel français remis en fin de chantier par le maître d'œuvre/entreprise, qui rassemble l'ensemble des plans et documents techniques correspondant à l'état réel de construction de l'ouvrage (souvent différent des plans initiaux). Il sert de référence pour la maintenance et l'exploitation ultérieure du bâtiment — un peu l'équivalent du « as-built » en anglais, et le pendant du CCTP mais en fin de projet plutôt qu'en amont. **DSI (Direction des Systèmes d'Information)** : Direction en charge de l'infrastructure informatique et des systèmes d'information d'une organisation, historiquement distincte des équipes techniques/facility en charge de la GTB. **Due diligence** (parfois traduite par audit préalable ou diligence raisonnable) : Processus de vérification et d'analyse approfondie qu'une partie mène avant de conclure une transaction, pour s'assurer qu'elle dispose de toutes les informations pertinentes et identifier les risques éventuels avant de s'engager. **Dans le contexte immobilier**, la due diligence désigne l'ensemble des vérifications qu'un futur locataire

obligatoire depuis le 8 janvier 2025. Le seuil intermédiaire de 70-290 kW a été reporté de 2027 à 2030 par un décret du 26 décembre 2025.

(ou investisseur) effectue sur un immeuble avant de signer un bail ou de finaliser une acquisition. Elle porte traditionnellement sur les aspects à l'état juridique du bien, à son état technique et structurel, aux aspects financiers et aux aspects environnementaux. La cybersécurité devient un nouveau volet de cette due diligence pour les grands locataires

GTB (Gestion Technique du Bâtiment) : Système centralisé qui pilote et supervise les équipements techniques d'un immeuble (chauffage, ventilation, climatisation, éclairage, sécurité incendie). Parfois appelé GTC (Gestion Technique Centralisée) ou BMS en anglais (Building Management System). Aux Etats-Unis, l'acronyme BAS (Building Automation System) est aussi couramment utilisé, mettant l'accent sur l'aspect "automatisation" (les automates qui pilotent directement les équipements).

GTC (Gestion Technique Centralisée) : Système de supervision technique proche de la GTB, parfois utilisé de façon interchangeable, mais généralement circonscrit à un lot technique unique (par exemple le seul chauffage) plutôt qu'à l'ensemble des équipements du bâtiment.

Handover : Phase de remise/transfert d'un actif ou d'un système entre deux parties — par exemple du promoteur/constructeur vers le property manager ou de l'exploitant sortant vers l'exploitant entrant. Comprend la transmission de la documentation technique, des clés d'accès, des contrats en cours, des garanties, et souvent une période de formation ou d'accompagnement pour assurer la continuité d'exploitation.

IEC 62443 : Norme internationale de cybersécurité dédiée aux systèmes industriels et d'automatisation (donc applicable aux GTB), couvrant la certification des équipements et des micrologiciels.

IoT (Internet of Things) : Ensemble des objets et capteurs connectés déployés dans un bâtiment (compteurs, capteurs de température/occupation, éclairage

connecté, ascenseurs, GTB/BMS) qui communiquent entre eux et remontent des données via le réseau. Pilier des smart buildings, mais chaque objet connecté est aussi une surface d'attaque supplémentaire en matière de cybersécurité.

ISO 27001 : Norme internationale de référence pour les systèmes de management de la sécurité de l'information (SMSI), applicable à l'échelle de toute une organisation.

IT / OT : Information Technology (réseau bureautique, données d'entreprise, messagerie) vs Operational Technology (réseau technique pilotant les équipements physiques du bâtiment : ascenseurs, CVC, contrôle d'accès). L'OT est une catégorie plus large que la GTB qui désigne tout système informatique pilotant des équipements physiques et des processus (par opposition à l'IT classique, qui gère les données, emails, ERP, etc.). Dans l'immobilier, l'OT recouvre la GTB mais aussi les sous-systèmes spécialisés comme :

- Les automates de CVC (protocoles BACnet, KNX, Modbus)
- Les systèmes de contrôle d'accès et badges
- Les ascenseurs et leurs automates
- La détection incendie/désenfumage
- Les compteurs énergétiques intelligents

La convergence IT/OT désigne l'interconnexion croissante de ces deux mondes historiquement séparés.

MFA (Multi-Factor Authentication) : Mécanisme de sécurité exigeant au moins deux preuves d'identité différentes pour accéder à un système, au lieu d'un simple mot de passe. Ces preuves combinent généralement :

- Ce que l'utilisateur sait — un mot de passe ou code PIN
- Ce que l'utilisateur possède — un téléphone (code SMS, application d'authentification comme Google Authenticator) ou une clé de sécurité physique (type YubiKey)
- Ce que l'utilisateur est — une empreinte digitale ou reconnaissance faciale (biométrie)

Man-in-the-Middle (MITM) : Type

d'attaque où un pirate s'insère entre deux systèmes qui communiquent pour intercepter ou modifier les échanges, souvent facilité par l'absence de chiffrement.

MQTT (Message Queuing Telemetry Transport) : Protocole de messagerie léger utilisé pour les objets connectés (IoT), notamment dans les bâtiments intelligents.

MSSP (Managed Security Service Provider) : Prestataire externe qui gère la sécurité (le plus souvent informatique/cyber, mais parfois aussi physique) d'un bâtiment ou d'un système pour le compte du propriétaire ou de l'exploitant : supervision des accès, détection d'intrusion, surveillance des systèmes connectés du bâtiment (GTB/BMS), réponse aux incidents. Le terme monte en importance avec la digitalisation des smart buildings, où les systèmes techniques (contrôle d'accès, CVC, ascenseurs) sont de plus en plus connectés et donc exposés à des risques cyber.

Network Operator (opérateur réseau) : Désigne l'entité qui exploite et maintient l'infrastructure réseau d'un immeuble ou d'un site : câblage, connectivité télécom/fibre, parfois réseaux IoT dédiés aux équipements techniques du bâtiment. Peut être un opérateur télécom classique ou un prestataire spécialisé dans les réseaux internes (LAN) d'un actif tertiaire.

NIS2 (Network and Information Security Directive 2) : Directive européenne renforçant les obligations de cybersécurité pour les infrastructures critiques et certaines entités (dont les collectivités et opérateurs de services essentiels), avec des sanctions en cas de non-conformité.

OIV (Opérateur d'Importance Vitale) : Statut réglementaire français désignant les entités dont l'activité est jugée indispensable à la nation, soumises à des obligations de cybersécurité renforcées.

OPERAT (Observatoire de la Performance Énergétique, de la Rénovation et des Actions du Tertiaire) : Plateforme de l'ADEME sur laquelle les propriétaires et exploitants d'immeubles tertiaires

déclarent chaque année leurs consommations énergétiques, dans le cadre du dispositif Éco Energie Tertiaire.

OT (Operational Technology) : Voir IT / OT

PCA (Plan de Continuité d'Activité) : Ensemble de procédures et de modes dégradés permettant à une organisation de continuer à fonctionner en cas d'incident majeur, y compris une cyberattaque.

Ransomware : Logiciel malveillant qui chiffre ou bloque l'accès à un système (ou à des données) et exige une rançon pour le débloquer.

REIT (Real Estate Investment Trust) : Équivalent américain d'une foncière cotée, soumise à des obligations de distribution de revenus à ses actionnaires.

RGPD (Règlement Général sur la Protection des Données) : Cadre européen encadrant la collecte et le traitement des données personnelles (pertinent pour les données collectées par les capteurs et systèmes d'accès des bâtiments).

RSSI (Responsable de la Sécurité des Systèmes d'Information) : Fonction en charge de la gouvernance cyber au sein d'une

organisation ou d'un actif immobilier.

SBOM (Software Bill of Materials, ou nomenclature logicielle) : Liste exhaustive des composants logiciels — bibliothèques, dépendances, versions — qui entrent dans la composition d'un logiciel ou d'un firmware. Elle permet de savoir rapidement si un équipement embarque un composant vulnérable, à l'image des attaques par la chaîne d'approvisionnement logicielle (Sunburst/SolarWinds, Kaseya).

TLS (Transport Layer Security) : Protocole de chiffrement qui sécurise les échanges de données entre deux systèmes sur un réseau, empêchant leur lecture ou leur modification par un tiers.

VLAN (Virtual Local Area Network) : Réseau local virtuel permettant de cloisonner logiquement différents flux de trafic (GTB, Wi-Fi invité, données locataires) sur une même infrastructure physique, sans qu'ils puissent communiquer entre eux.





Savills Team

Décryptages, tendances, perspectives du secteur de l'immobilier tertiaire, nos équipes de recherche spécialisées vous donnent un aperçu des tendances actuelles du marché et des prévisions pour vous aider à prendre les bonnes décisions en matière immobilière.



SAVILLS BUREAUX



Péroline Prévost-Manseau

Head of Agency France & Workthere
+33 6 82 30 29 32
peroline.manseau@savills.fr



Sabina Garevski

Head of Property Management
+33 6 82 82 70 17
sgarevski@savills.fr

SAVILLS RESEARCH



Cyril Robert

Head of Research
+33 6 11 82 13 88
cyril.robert@savills.fr



Justine Réchaux

Associate - Research Consultant
+33 6 14 87 92 30
justine.rechaux@savills.fr

Source des photos

@Adobe Stock @Gemini @Midjourney
Certaines images ont été générées et/ou retouchées à l'aide de l'intelligence artificielle.