

essensYs

Digital security for CRE

How to remain secure while
delivering your flexible
workspace strategy



Introduction



DAVID KINNAIRD

Senior Director of Customer Operations,
essensys



BRYN SADLER

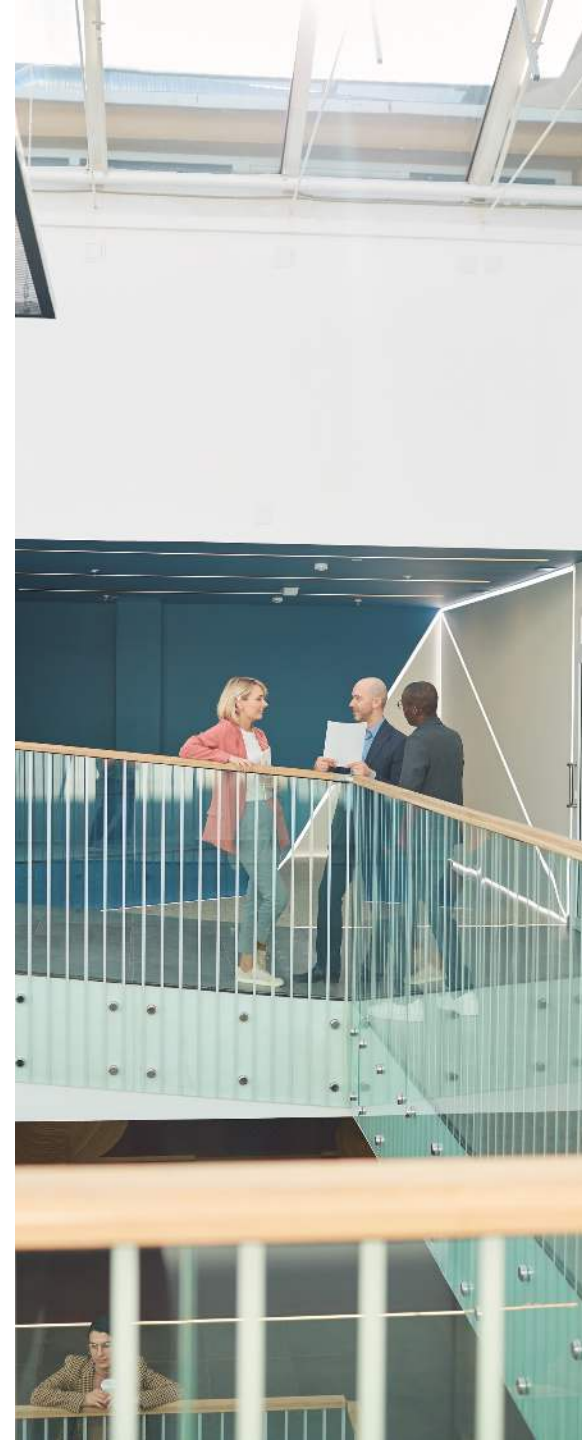
SVP, essensys labs

The term “flex” no longer refers only to coworking. Today, flexible workspace also incorporates the use of spec-suites and plug-and-play style office space. It’s no longer just about open-plan seating for individual occupiers as larger enterprises look to flexible space to meet their real estate needs.

As flexible workspace becomes the new office norm, occupier expectations of accessibility and security of digital services are more stringent. Corporate uptake of flexible space has resulted in stricter technical, security, and service-level requirements.

A lack of enterprise-grade technology with proven network security and compliance specifications is a deal-breaker for many corporate occupiers. But ensuring the right measures are in place isn’t just about acquiring corporate customers, but also about preserving brand reputation.

In this eBook, we outline the security practices landlords and flexible workspace operators need to run a secure and future-proofed operation that meets occupier demands.



Topics

- 1 Why security is a top priority
- 2 What to consider
- 3 Risk types
- 4 Impact on compliance
- 5 Network resiliency
- 6 Invest in the right tech

Providing secure networks in shared workspaces

When offering networks-as-a-service in shared environments, security is critical.
Here are some key things to consider:

01 A network that's available and resilient

- Resilient to equipment failures
- Resilient to human error

02 A network that's secure in itself

- Network equipment must remain up-to-date
- Equipment must be physically secure and tamper-proof

03 A network that's secure for users

- Physically secure so that only the Local Area Network (LAN) connections in a tenant's office space are provided with their network
- Segregation from other users, so that Occupier A's network remains separate from Occupier B's network, and so on
- Minimise the "blast radius" of any issues that may be created by a user, such as viruses or excessive consumption of bandwidth

Read on to discover how to achieve these critical elements and provide secure network connections for shared workspaces

Why security is a top priority

Traditionally, tenants of office space leases have been responsible for their digital security requirements. In a flexible workspace model, however, this responsibility shifts more towards the operator. Furthermore, as the market grows, the type of occupiers taking flexible office space is expanding and driving stricter security and IT requirements. For example, financial, legal and medical tenants must meet specific compliance requirements within their sectors, making security a table stake for these occupiers.



Flexible workspace began to flourish around the same time as fundamental technology shifts occurred. Companies started to move away from corporate networks, which could only be accessed remotely via a VPN (Virtual Private Network). In these networks, server infrastructure was managed by a company IT department and accessed with a company-issued phone and computer. They were generally locked down to the extent that even USB drives were inaccessible to prevent moving data away from corporate infrastructure without a trace.



The new paradigm is BYOD (Bring Your Own Device) which has employees, remote workers, contractors and other stakeholders using their own mobile devices and/or laptops. These users are now using completely cloud-based services to work on, store and access information. This opened the door for data vulnerabilities and breaches. Sharing across the cloud makes it easy for hackers to maliciously share commercial and confidential information. This shift to the public cloud combined with more relaxed tech policies and a shared workspace office, means the odds of a brand-shattering security breach skyrocket.

With companies today relying on SaaS software and storing more and more business-critical and sensitive data in the cloud, security considerations are even more critical. Leading flexible workspace providers are putting measures into place to secure digital assets and connectivity as a top business priority. Any type of security or network breach can threaten brand reputation and risk customer retention, not to mention the costly expense of damage control.

What to consider

Managing risk profiles

Different occupiers will have diverse risk profiles. But the more challenging element will be that many tenants won't understand or fully appreciate their risk profiles and how this relates to those of others within a flexible workspace environment. This is especially true of individuals and startups who don't have the benefit of dedicated security specialists within their organization. A flexible workspace provider's default position should be to assume that all tenants have stringent risk profiles and build their processes and infrastructure to support them.



01 Physical security

How are occupiers accessing locations across your workspace portfolio? Physical security is the absolute foundation for any security policy. Any element of physical access an attacker gains will help them compromise their target. Door access control is more than giving members and tenants a code that unlocks the door. On a basic level, it might do the trick. But it's critical for operators to enable user tracking functionality along with visitor management.

Providers often overlook the importance of door locks within the workspace. If you're charging for meeting room time, part of safeguarding your operation is to ensure these meeting rooms aren't being used without permission or when they're not meant to be used.

Keeping a close eye on visitors who enter your space is critical. It is easy to do with smart Guest WiFi tracking and visitor management technologies.

Flexible workspace providers should also consider the member experience of triple door access control; (1) access to the building, (2) to the workspace, and (3) to the meeting rooms. Is it seamless for the customer, secure for the business, and tracked to capture revenues?

From a network perspective, it's critical to prevent access to the physical infrastructure. Access to the IT or comms room must be restricted from unauthorized users and WAPs (Wireless Access Points) must be secure and physically out of reach to prevent tampering and theft.

What to consider

02 Infrastructure device security

Because of the agile and constantly changing nature of the sector, it's vital to stay on top of configurations and new software and updates for all devices connected to the network. The objective is to reduce vulnerabilities and security risks to devices on the infrastructure and to prevent threats and attacks. What's technically known as the system hardening process includes measures such as device configurations, configuration management, software and firmware management, device monitoring and access logs.

Behind the technical jargon, this means that as threats emerge, manufacturers issue updates to ensure that these devices remain secure. Any device providing network to your customers may need to be regularly updated, ideally in a way that is not disruptive to end-users.

It isn't easy to take responsibility for all customer devices connected, but all the devices and equipment under your control should be. These practices, along with back up configurations, device access, change logs, and adhering to vendor security recommendations, can prevent risks to your network.



03 Network security

When it comes to network security, there are dozens of questions that operators must consider. For starters, is traffic over the network appropriately encrypted? Are tenants segregated from one another? Are WiFi passwords secure? Is the internal network secured from the outside world?

DIY connectivity can easily get operators and their occupiers into hot water. Ensuring that cable patching and switch port configurations are kept up to date is critical to prevent security risks to connected devices.

Secure WiFi networks encrypt and authorize access based on specific usernames and passwords rather than issuing a shared password common for WPA networks. What this means is that if an employee or a tenant leaves, staff can easily disable the user instead of having to change the WiFi password for all users on the network. A secure WiFi network provides user visibility and trackability. Gaining insight into who is on your network and keeping a footprint of activity helps to prevent unwanted security risks.



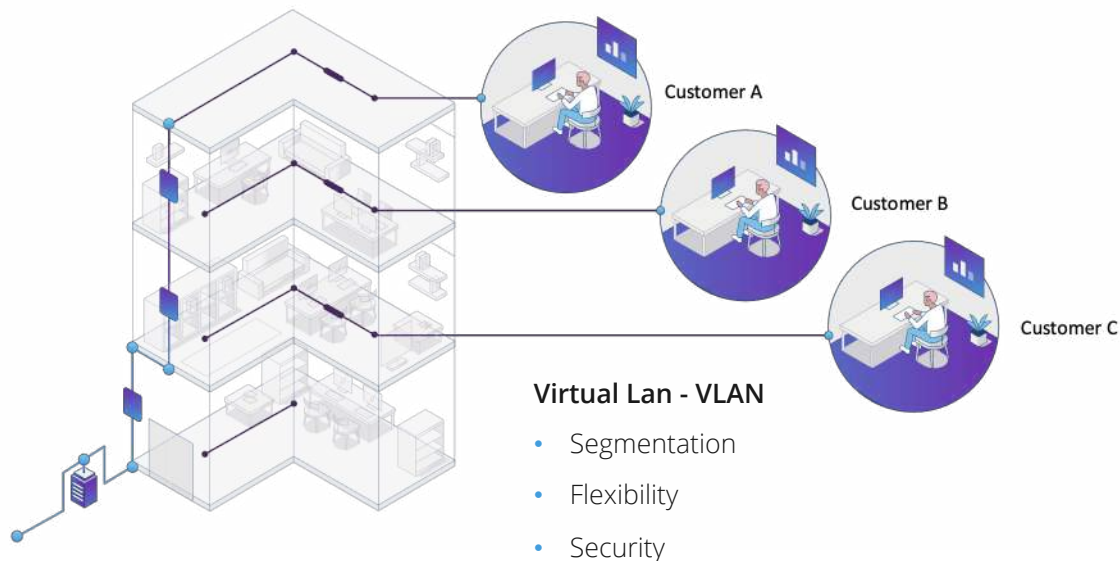
What to consider

04 End user device security

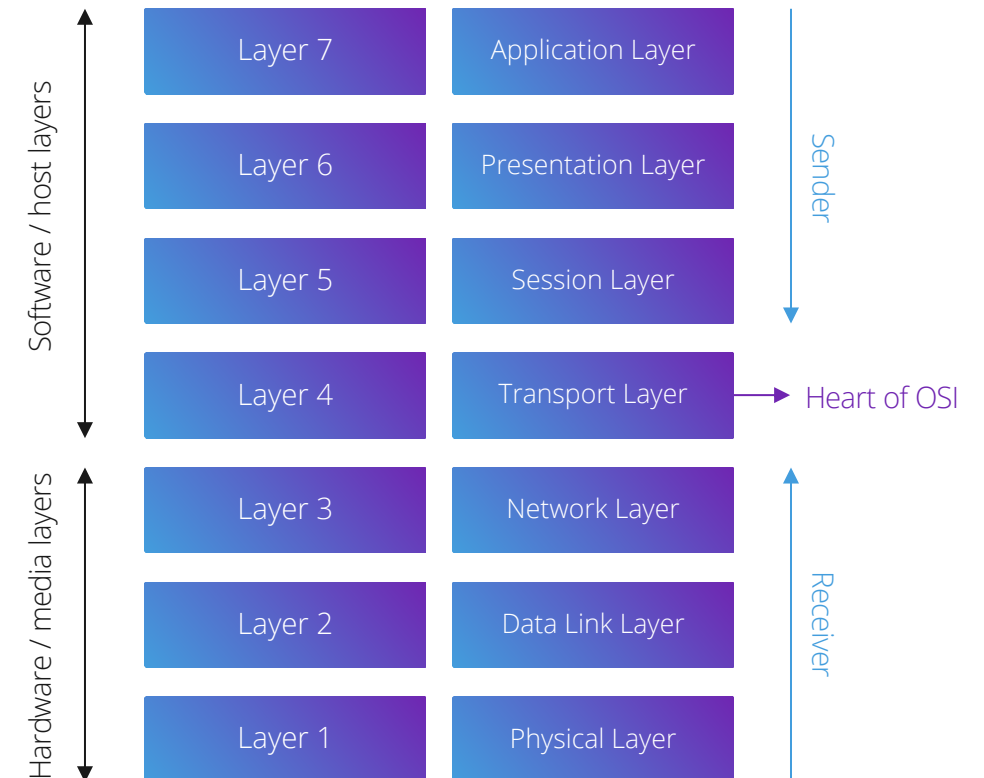
Keeping each end-user device secure is the responsibility of the device owner. However, operators should be aware of the impact that irresponsible or oblivious users can have on their network. Viruses can spread, use up bandwidth, block IP addresses and more.

Ensuring that the network has appropriate segregation and monitoring to contain and identify compromised devices is a security best practice.

Real-time bandwidth and protocol monitoring along with enterprise-grade network segregation are key measures to manage security risks to your flexible workspace network infrastructure. This means that ideally, each customer should be segregated into their own virtual network – a Virtual Local Area Network or VLAN.



Layers of network infrastructure



Risk types

Security is a process, not a product. You can buy a lock for your door, but if you don't lock it when you leave the premises, it won't stop intruders. There are two categories of risk: targeted and untargeted.

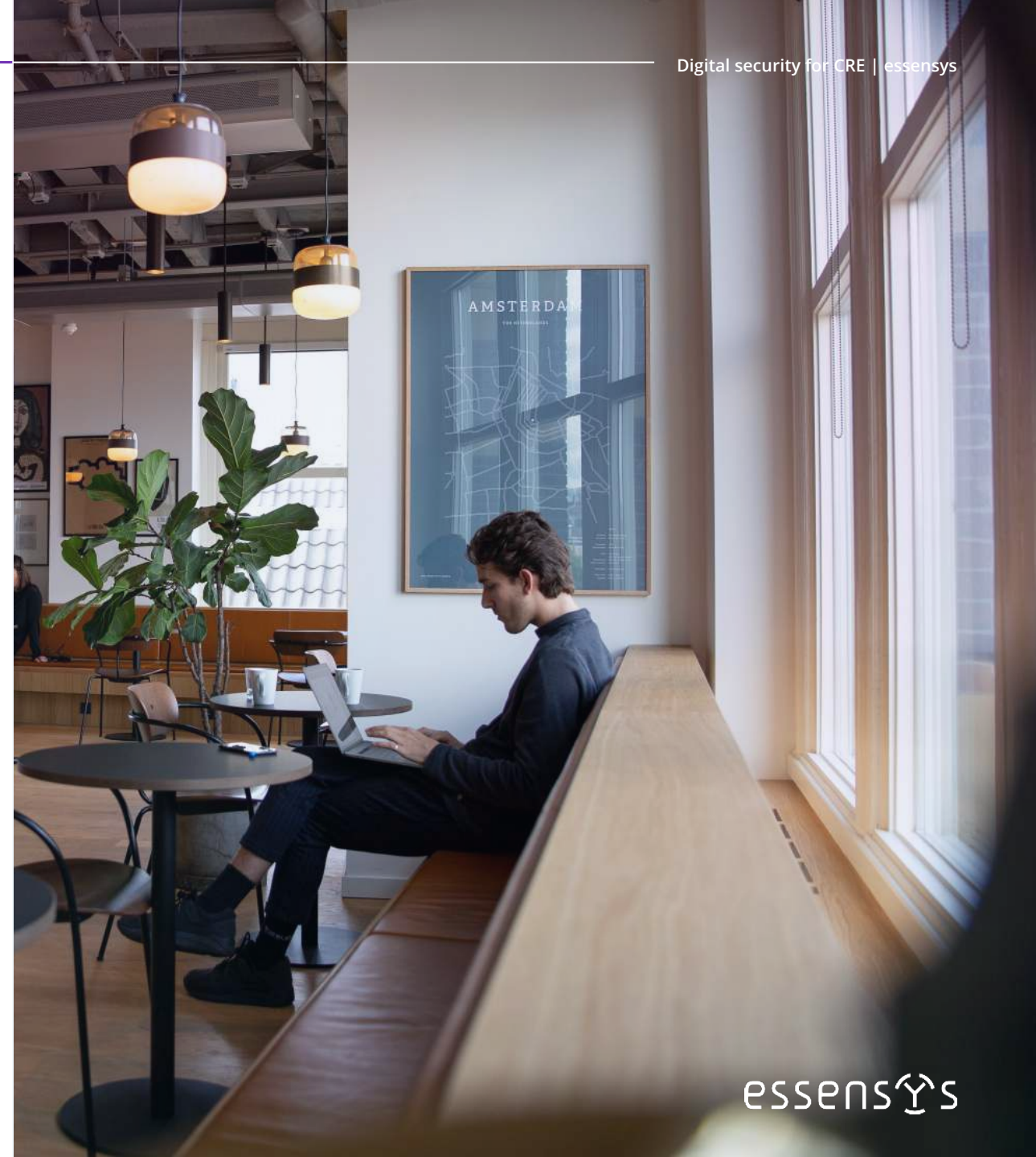
A targeted risk could be a malicious agent actively trying to hack other users' devices.

These could be users within your own company or an occupier's company, for example, a disgruntled employee. Enterprise-grade technology such as firewalling and VLAN segregation protects occupiers from targeted attacks from other users on the same infrastructure. Every company, regardless of size, should have a device policy in place. There is little that can be done at the network level to prevent attacks that originate within the same organization.

Untargeted risks are things such as malware and viruses, which spread by themselves, can infect anything, and have a more significant impact on the user and the network.

These types of security hacks slow down computers or make them glitchy and consume internet bandwidth. Viruses can harvest user passwords, encrypt files on the system, and even hold the user ransom to retrieve data.

To prevent against untargeted attacks, IT departments should enforce and educate their staff on security best practices. For example, updating antivirus software on devices and training users to recognize and not open suspicious email attachments can save a company a lot of trouble.



Impact on compliance

Compliance includes the measures you put in place to meet best practices or regulations.

This can include certifications, such as:

- SOC2: Design and implementation of cybersecurity controls
- ISO9001: International standard for Quality Management
- ISO27001: International standard for Information Security

Compliance can exist as a bare minimum requirement to align with industry norms and governance and will often be mandated by law. Security regulations frequently impact banks and payment processors, but as more and more companies process personal data, wider-reaching legislation is more prevalent. For example, GDPR in the EU (and for data moving in and out of the EU) and HIPPA in the USA.

Network security requirements that can safely transmit occupiers' data over your infrastructure is often mandated from a head office and is a dealbreaker for many occupiers. They simply won't sign if the technology doesn't meet their enterprise compliance and best practice regulations and policies.



Network resiliency

Resiliency is a broad term that relates to both redundancy and security. Fundamentally, resiliency refers to the ability to keep operating or to resist risks that can threaten network availability. Below are three examples of these risks and how to mitigate them:

1. Network Device Failure

Sometimes things break. The best approach to mitigate this risk is to expect and plan for device failure and where appropriate build in redundancy. That way, if a device or component does fail, another one can cover its task. To prevent hardware device failure, network solutions must be designed with redundant circuits that connect to at least two distinct data centers and highlight redundant core network devices and interconnects.

2. Device security compromise

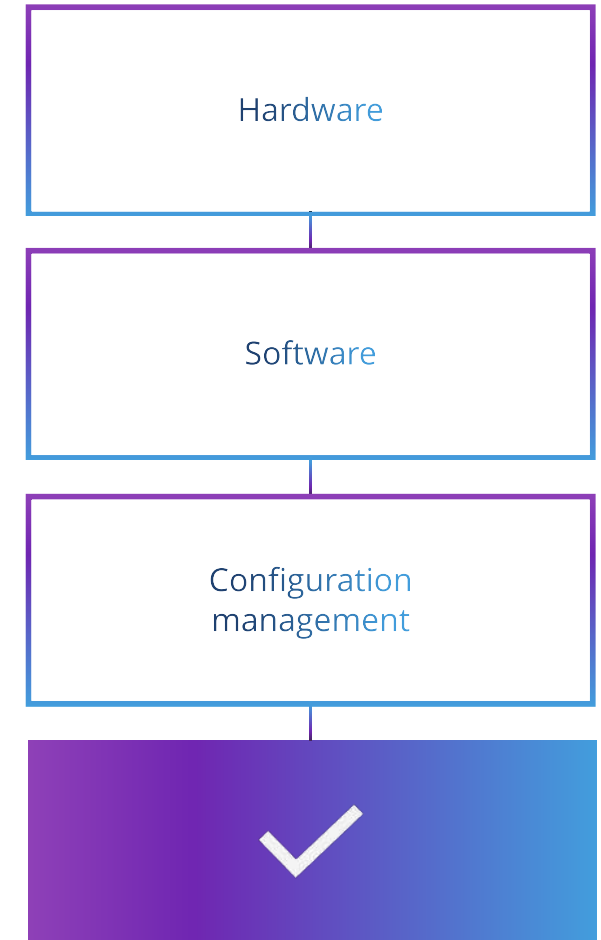
If an attacker gains access to the configuration interface of a device, they would be able to alter that configuration and affect the way it performs its function. A case in point is a story published on Wired.com back in 2015 about a Jeep that was hacked while in motion on the highway. While it was a controlled demonstration, it is validation that device security is critical.

It is essential to ensure that device access is restricted as much as possible, that device configurations are hardened to industry standards, that software and firmware are kept up to date to prevent security vulnerabilities, and that access of authorized users is controlled and audited.

3. Capacity management

Changing usage patterns can impact the resiliency of a solution. Examples of this include a large new tenant moving into a flexible workspace and requiring a large amount of internet bandwidth. Their usage requirement could reach the existing circuit capacity and cause congestion problems or poor performance if a large number of their employees attempt to use a single wireless access point.

Business or mission-critical devices should be supported by wired connections to avoid the potential limitations of WiFi and ensure continuity.



Invest in the right tech


Security can be frustrating, interesting and challenging at the same time. Its very nature is to make things harder to do, which is why landlords and flexible workspace operators often neglect it or take shortcuts. Unfortunately, it's unavoidable if you want to run an efficient and future-proofed operation and meet occupiers' expectations.

The best approach is to automate security processes and best practices where possible and make setting up and maintaining access to locations and systems as seamless as possible for your staff. Centralizing all of your tech services, such as wireless and wired connectivity, door access control and room booking, together into a single system facilitates the management of both users and devices on your network.

Of course, taking the appropriate security precautions and being on top of best practices has an investment cost associated with it. These include hardware costs such as network devices and access control systems, software costs and costs to make sure that staff are well trained. But the investment is well worth it and business critical.

Return on security investment is more difficult to measure. However, people often underestimate the financial burden of a security breach until they experience one. The impact goes beyond just eliminating the threat and getting your network up and running again. Once a security breach occurs, the damage to your brand is done. For a flexible workspace operator, the most significant ROI concern will be securing larger, more sophisticated tenants that require a stringent degree of security when they move in. If you cannot demonstrate that your tech stack will deliver on their requirements, you'll undoubtedly lose the business.

Given the number of high-profile data breaches in recent years, digital security has become even more of a table-stakes requirement for the growing market of flexible workspace occupiers. Security is now a top priority for ambitious and fast-growth operators who understand the importance of future-proofing their business, preserving brand reputation and retaining customers.



“People often underestimate the financial burden of a security breach until they experience one”

Bryn Sadler, SVP, essensys labs

About essensys

essensys is a leading global software and technology company designed to deliver digitally enabled spaces, buildings and portfolios.

Founded in 2006, and listed on the AIM market of the London Stock Exchange since 2019, essensys is active in North America, UK, Europe and APAC, serving customers across 270+ cities.

The essensys Platform connects, controls, and automates digital services, enabling our customers to create seamless in-building experiences.

Contact us at:



[@essensys](#)



essensys.tech



tellmemore@essensys.tech



Digital security for CRE | essensys

