inner range

UNIFIED VIDEO, ACCESS & SECURITY SYSTEMS

THE POWER OF INTEGRATION: BUILDING ENDURING VALUE IN PHYSICAL SECURITY SYSTEMS

INNERRANGE.COM

INTRODUCTION

The last few years have seen dramatic changes, challenges and never-seen before circumstances – with Brexit and the pandemic being at the top of that list – that many businesses are still adapting to. And just when some sort of equilibrium has been reached in the market, the scales tip again and there are other economic challenges to deal with.

Taking a step back from the wider economic uncertainty, businesses still need to address issues closer to home, both those as consequences of said changes and those occurring organically. Skills shortages, supply chain disruptions, influx of new technologies, such as GenAI, regulatory changes, evolving cyber security threats, the rising cost of physical security… the list goes on.

In a nutshell, organisations are operating in a dynamic market where rising costs, regardless of cause, are a massive concern. One of the remedies is, of course, managing costs and ensuring whatever investments are being made in infrastructure, staff, etc, are delivering the right return.

The security market is no different. Security – both physical and digital – has risen as a priority in recent years and is now firmly a board-level issue. This is good news for organisations looking to improve security; with buy-in from the top, getting the right systems in place is made a little easier. This is demonstrated by the growth in the global physical security market; according to research, it was valued at $122.5 billion in 2024 and is anticipated to grow at a rate of 9% to reach $182.34 billion by 2029.

While this focus on security is good news for organisations and security teams, it also means that they are under increasing scrutiny to be cost efficient and deliver the promised return on investment.

?

THE QUESTION IS HOW

This paper looks at the converging worlds of physical and cyber security, the role of integrated security teams in securing the future and the strategic principles of maximising the longevity and value of security investments.

?

THE EVOLVING SECURITY LANDSCAPE

Physical security – security of sites and staff – has never been more important than it is today, influenced by issues such as regulatory compliance and rising crime rates. As an example, in England and Wales, according to the ONS, instances of fraud and theft were up 7% and 6% respectively in 2024, while computer misuse was up 12% from the previous year.

While digital crime occurs in cyberspace, very often it is the fact that bad actors gain physical access to buildings, offices and devices that pave the way for the crime to occur.

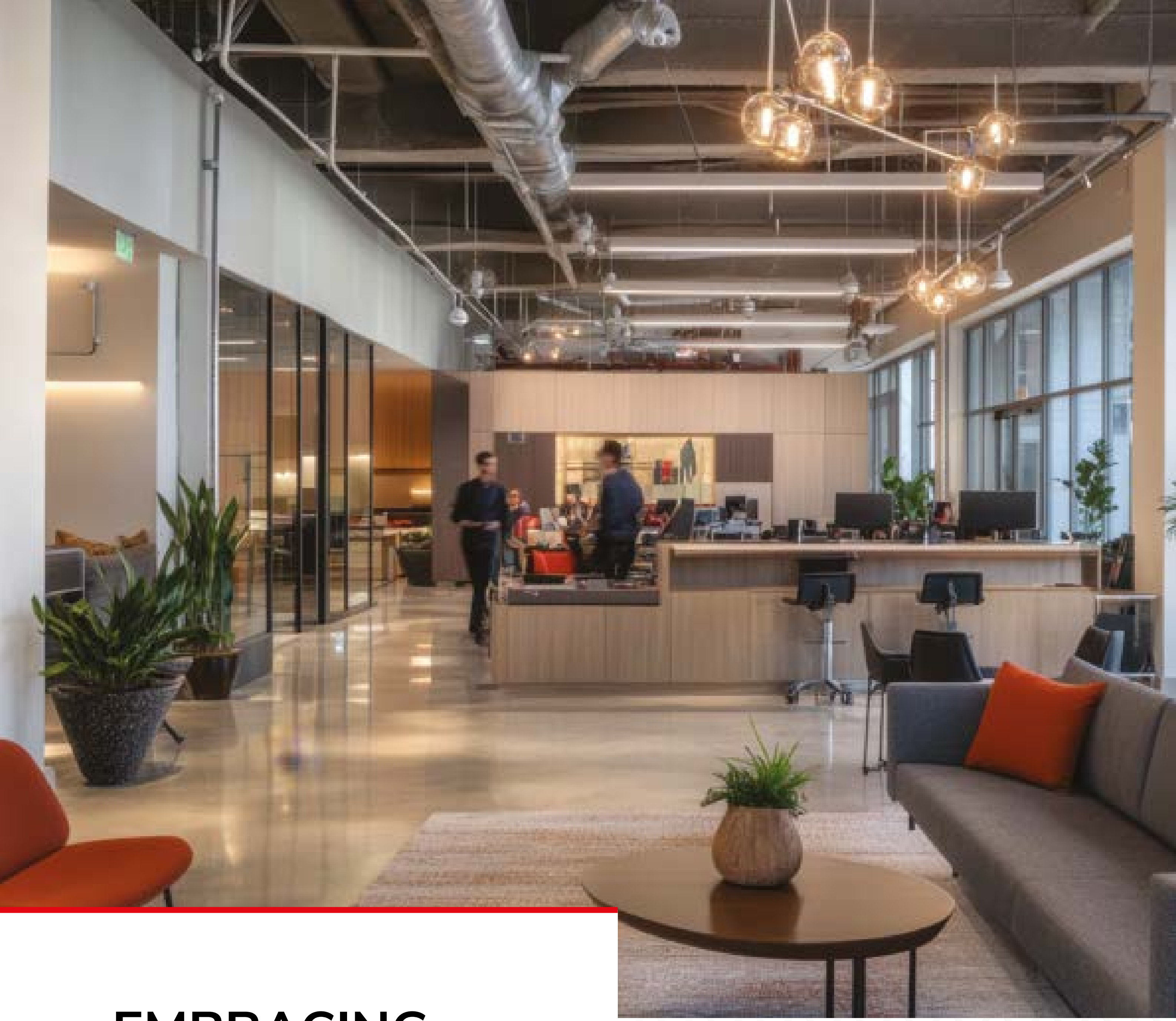
Coupled with a rapidly changing technology landscape – as much as AI can help a business, it can also help cyber criminals – and it is a perfect storm for organisations.

The result is an evolved view of security, with changes to requirements and expectations of hardware and software solutions. From new systems to retrofitting existing systems, two themes are key: effectiveness and cost-efficiency.

In a perfect world organisations would have unlimited budgets to spend on beefing up security; but in reality, bigger organisations typically have bigger budgets and smaller businesses find themselves being left behind in terms of skills, money and solutions.

The fact is: every business, regardless of size, has something worth stealing. Whether that is intellectual property, customer details, or physical items. And the solution to protecting those items, again regardless of size of business, is having a security ecosystem that is fit for purpose and adaptable.

There has long been a shift in industry from single point solutions to a more unified approach; moving beyond siloed systems to using integrated systems to get the most out of the ecosystem's functionality and optimising investment.



EMBRACING INTEGRATION

The need to view security as an interconnected ecosystem rather than a collection of standalone products has really come to the fore over the last decade. In a typical office building playing host to co-working spaces, for example, the integration of access control, CCTV, lift management and building automation creates an easy to use and easy to manage security environment – this is especially important considering the number of staff, visitors and contractors coming through the doors, as well as the number of companies within the building itself.

THE BENEFITS OF SUCH INTEGRATIONS INCLUDE:

- Enhanced situational awareness through unified data and control
- Improved operational efficiency for security personnel
- Greater flexibility to adapt to future needs and technologies
- Streamlined management and reporting
- Breaking down data silos for better insights

CONSIDERATIONS FOR INTEGRATION

When designing or upgrading security systems with a focus on long-term value and adaptability, the ability to integrate various hardware and software components is paramount. In environments such as datacentres, for example, where requirements evolve depending on clients, this flexibility is vital.

However, successful integration isn't simply about connecting different devices; it requires careful consideration of several key factors to ensure a cohesive, efficient, and future-proof security ecosystem.

THESE CRUCIAL CONSIDERATIONS INCLUDE:

ADHERENCE TO OPEN STANDARDS:

- INTEROPERABILITY: Prioritise systems and devices that adhere to widely recognised open standards within the security industry. These standards (like ONVIF for video surveillance or specific protocols for access control) facilitate communication and data exchange between products from different manufacturers. This avoids vendor lock-in and provides greater flexibility in choosing best-of-breed solutions.
- REDUCED INTEGRATION COSTS: Open standards often simplify the integration process, reducing the need for custom development and complex workarounds, ultimately lowering integration costs.
- FUTURE COMPATIBILITY: Systems built on open standards are more likely to remain compatible with future technologies and updates within the industry.
- INCREASED CHOICE AND COMPETITION: Supporting open standards encourages a competitive market, giving organisations a wider range of compatible products to choose from.

ROBUST AND WELL-DOCUMENTED APIS (APPLICATION PROGRAMMING INTERFACES):

- SEAMLESS COMMUNICATION: Even with open standards, well-designed and documented APIs are crucial for deeper levels of integration and customised functionality. APIs allow different software platforms and hardware devices to “talk” to each other and exchange data in a structured way.
- CUSTOMISATION AND EXTENSIBILITY: Robust APIs enable organisations and their integration partners to build custom integrations that address specific operational needs and workflows.
- SIMPLIFIED DEVELOPMENT: Clear and comprehensive API documentation makes it easier for developers to create and maintain integrations, saving time and resources.
- SECURITY CONSIDERATIONS FOR APIS: Ensure that APIs are secured with proper authentication, authorisation, and encryption mechanisms to prevent unauthorised access and data breaches during integration.

FUTURE-PROOFING AND SCALABILITY:

- MODULAR DESIGN: Opt for security systems with a modular design that allows for the addition of new components and functionalities without requiring a complete system overhaul. This ensures the system can adapt to evolving needs and technological advancements.
- SOFTWARE UPDATES AND SUPPORT: Consider the vendor’s track record and commitment to providing regular software updates and long-term support for their hardware and software. This ensures ongoing compatibility and access to new features and security patches.
- SCALABILITY: The chosen systems should be able to scale easily to accommodate future growth in the organisation’s size, number of locations, or security requirements. Consider the system’s capacity for adding more devices, users, and integrations.
- EMBRACING EMERGING TECHNOLOGIES: While avoiding specific product mentions, consider whether the underlying architecture of the potential systems is designed to integrate with future technologies like AI-powered analytics, IoT devices, and advanced communication protocols.

DATA MANAGEMENT AND INTEROPERABILITY:

- DATA FORMAT COMPATIBILITY: Ensure that the different systems being integrated can handle and exchange data in compatible formats. Data mapping and transformation capabilities might be necessary.
- CENTRALISED DATA MANAGEMENT: Aim for solutions that can feed data into a centralised security management platform, providing a unified view of all security events and information.
- DATA ANALYTICS AND REPORTING: Consider whether the integrated system will allow for comprehensive data analytics and reporting across different security domains, providing valuable insights for risk assessment and operational improvements.

CYBERSECURITY BY DESIGN:

- SECURE HARDWARE FOUNDATIONS: When considering integration, prioritise hardware manufacturers with a strong commitment to cybersecurity in their product design. This includes secure boot processes, firmware integrity checks, and robust device hardening.
- SECURE COMMUNICATION PROTOCOLS: Ensure that the communication channels used for integration employ secure protocols (e.g., HTTPS, TLS/SSL) to protect data in transit between systems.
- PRINCIPLE OF LEAST PRIVILEGE: When integrating systems, ensure that each integrated component only has the necessary permissions and access to the data and functionalities it requires.

PLANNING AND EXPERTISE:

- COMPREHENSIVE NEEDS ASSESSMENT: Before embarking on any integration project, conduct a thorough assessment of the organisation’s current and future security needs, identifying key integration requirements.
- STRATEGIC PARTNERSHIPS: Engage with experienced security consultants and integrators who have a proven track record of successfully integrating diverse security systems. Their expertise is crucial for navigating the complexities of integration and ensuring a robust and effective solution.
- PHASED IMPLEMENTATION: For large or complex integration projects, consider a phased implementation approach to minimise disruption and allow for thorough testing and validation at each stage.

THE VALUE OF STRATEGIC PARTNERSHIPS

Robust security – on both the physical and digital front – is a team sport. Not only does it require buy-in and effort from all involved, from management, to IT and security, to individual members of staff, it also requires working with the right partners. Whether working with consultants, integrators or distributors, working with someone who understands the business, its challenges and requirements can often determine the difference between success and failure. Importantly, it is about getting the best systems in place and ensuring optimised value for the short and longer term. In the life sciences industry, as an example, access control forms part of a larger security strategy including guarding valuable intellectual property and keeping staff safe from harm.

QUALITIES OF A STRATEGIC PARTNER:

- Deep understanding of the client's specific sector and challenges
- Proactive approach to identifying future needs and opportunities
- Expertise in the latest security advancements and integration possibilities
- Commitment to long-term support and guidance
- A collaborative approach to building tailored solutions

Ultimately, the right strategic partner is one that can help organisations avoid short-sighted solutions and plan for the future.

INTEGRATING CYBER RESILIENCE INTO PHYSICAL SECURITY

The cyber threat poses an increasing risk to organisations. In the past organisations in high-risk industries such as financial services were seen as the prominent targets. Today, however, any business regardless of size (as previously mentioned) or industry is at risk. While the threats do vary – ransomware, data breach, DDoS attack – the damage to reputation, customer trust and the bottom line is serious.

As more businesses merge their physical and digital security programmes, it is increasingly important to think about key elements like integration, cost-efficiency, return on investment, and long-term performance. Well-designed physical security systems can contribute significantly to a stronger overall cyber security posture.

Physical security around a business, such as access control, CCTV, intruder detection, plays a vital role in protecting infrastructure from internal and external bad actors – be it in a data centre, office building or laboratory. In addition, hardware and software used to secure physical premises and controlling staff and visitor movement need to be resilient and secure from the cyber threat itself.

KEY CONSIDERATIONS WHEN INTEGRATION CYBER RESILIENCE INTO PHYSICAL SECURITY, INCLUDE:

- The increasing network connectivity of physical security devices
- Potential attack vectors targeting physical security systems
- The importance of secure design principles in hardware
- Strategies for mitigating cyber risks in physical security deployments (e.g. secure data storage, encryption, hardening guidelines)

CONCLUSION

Organisation today face myriad threats brought on by a volatile economic climate and increasingly sophisticated threats. As a result, the pursuit of robust and cost-effective security has rightly ascended to the highest levels of organisational priority. The path to achieving enduring value in physical security lies not in isolated deployments, but in the strategic embrace of intelligent integration.

The convergence of the physical and digital realms demands a holistic perspective, one that breaks down traditional silos and fosters a unified security ecosystem. By thoughtfully considering open standards, leveraging robust APIs, and prioritising future-proofing, organisations can build adaptable infrastructures capable of evolving alongside their needs and the ever-changing threat landscape.

Furthermore, the importance of selecting the right strategic partners cannot be overstated. These experts provide invaluable guidance in navigating complexity, identifying opportunities for synergy, and ensuring that security investments deliver optimal value, both now and in the years to come.

Finally, the integration of cyber resilience into the very fabric of physical security design is no longer an option, but a necessity. Protecting physical infrastructure and the systems that govern it from cyber threats is paramount in safeguarding the entire organisation.

Ultimately, the journey towards a truly secure and resilient future is paved with intelligent integration, strategic partnerships, and a deep understanding of the interconnected nature of physical and cyber security. By embracing these principles, organisations can move beyond simply reacting to threats and proactively build security systems that deliver lasting value, protect their assets, and empower them to navigate the uncertainties of tomorrow with confidence.

ABOUT
INNER RANGE

Inner Range – integrated security systems protecting people, possessions and property

Inner Range is a global leader in unified video, access and security systems. With a 35+ year heritage, the company has an established reputation for best-in-class security solutions and outstanding customer support.

From entry-level to enterprise, Inner Range provides an end-to-end security solution capable of addressing the most difficult building management needs – with video management, access control and intruder alarm functionality all controlled and managed from one platform.

Inner Range is innovation focused, with solutions evolving to meet industry trends and exceed customer needs – notably through its Integriti, Integriti High Security, and Inception ranges.

Inner Range has 150,000 installations in over 30 countries, serving customers across vertical markets. Its systems can be found securing commercial buildings, high-end residential sites, hospitals, datacentres, colleges and universities, pharmaceutical companies, and critical national infrastructure.

With its head office and R&D facility in Melbourne, Australia, Inner Range is proudly a Wesco-Anixter company.

INDUSTRY SNAPSHOTS –
HOW INNER RANGE CAN HELP

DATACENTRES

Providing robust access control, CCTV and intrusion detection for multi-tenanted datacentre sites.

- Ease of management for security teams
- Managing permissions for customers onto and within site – partitioned sites to isolate users from other customers
- Meeting industry regulation
- Integrated environmental controls to monitor HVAC or fire detection

COMMERCIAL BUILDINGS / CO-WORKING SPACES

Monitoring and management for large office buildings hosting multiple companies.

- Ease of use – on- and offboarding employees, contractors and visitors
- Intruder detection and ensuring right of access to lifts, floors and offices
- Building entry and lobby control
- Smart building – water, HVAC, car parking, lift control

HIGH-END RETAIL

From new sites to updating existing sites, providing a unified platform to ensure safety of staff and customers, and prevent theft.

- Intrusion detection to secure sites outside trading hours
- Managing movement of staff and contractors within restricted areas
- Real-time alerts (duress and location information) to notify stakeholders
- Validating credentials for contractors
- Maximising profitability via sophisticated solutions, people counting, heat maps and facial recognition

LIFE SCIENCES

A unified security solution with CCTV, access control and intrusion detection to protect staff and valuable intellectual property.

- Centralised management to ensure efficiency of security
- Help meet regulation and compliance
- Scalable to meet changing needs, growth and expansion
- Securing access to equipment, pharmaceuticals, controlled areas

GET IN TOUCH

For more information on how Inner Range can help secure your business, please get in touch with us today.
Email: ireurope@innerrange.co.uk Phone: +44 (0) 845 470 5000 www.innerrange.co.uk