INTA365

Trusted Expert Consulting.

Planning for Success:

5 Key Stages in Upgrading a Major Security System

INTA-INSIGHTS 2024

About INTA365

INTA365 is a leading security consultancy firm with over two decades of experience, specialising in complex, high-end systems for public spaces, government sectors, national security, and the NHS. Recognised by respected industry bodies like the Chartered Management Institute and The Security Institute, we offer expert solutions that integrate cutting-edge technology and innovative thinking. Our TRAQ system and transparent project management approach ensure clients stay in control, maximising their return on investment. From product design to maintenance, INTA365 delivers robust, reliable security strategies tailored to the unique needs of our clients.

What to learn more about INTA365?

www.inta365.com

Contents

Foreword

Dear Reader,

At INA365, we know that upgrading a major security system can seem daunting, but it's a crucial step in ensuring your organisation remains resilient in an ever-evolving security landscape. Whether you're dealing with outdated technology, changing operational requirements, or the need for enhanced compliance, a well-planned upgrade can make all the difference in protecting your assets and operations.

In this guide, we aim to provide you with a practical, step-by-step approach to upgrading your security system, focusing on the **five key stages** that will ensure a smooth and successful transition. If you're reading this, you already recognise the importance of keeping your security systems up-to-date and future-proofing them for the challenges ahead. This insight paper is designed not just to inform but to empower you to make well-informed decisions with confidence.

Throughout this guide, we've drawn from our extensive experience working with organisations across industries. We'll outline proven strategies, highlight critical considerations, and share best practices to help you navigate each phase of the upgrade—from identifying when a system needs upgrading to making the most of new features post-implementation.

Our goal is simple: to make this process as seamless as possible for you. We're here to guide you through every step, ensuring your upgraded system delivers the security, efficiency, and long-term performance your organisation deserves.

Sincerely,

The INA365 Team

Introduction

Upgrading a major security system is a complex yet crucial process for ensuring your organisation's long-term safety and operational efficiency. From identifying the need for an upgrade to managing the integration of multiple systems and contractors, every step requires careful planning and execution. At INA365, we understand the challenges involved in such projects and have guided numerous businesses through seamless upgrades. This industry insight outlines the five key stages for successfully upgrading a security system, enriched with practical advice, expert insights, and considerations to ensure your organisation remains secure, compliant, and future-ready.

Stage 1: Recognising the Need for an Upgrade

Identifying the Signs

The first step in upgrading any major security system is recognising when the existing setup no longer meets your operational or security needs. Several indicators might signal that it's time for an upgrade:

Technological Obsolescence: Many legacy systems may be outdated, making them more vulnerable to security threats or cyber-attacks. If your system is five years or older, chances are it's missing key features like AI analytics or cloud integration.

Operational Inefficiencies: If operators are struggling with slow response times, unintuitive interfaces, or incompatible components like CCTV and access control systems, these inefficiencies can seriously hinder security.

Compliance Issues: New regulations such as GDPR or local security standards may mean that your system is no longer compliant, exposing your organisation to legal and financial risks.

Fact:

According to a study by IFSEC Global, 47% of businesses have experienced a security breach due to outdated systems, leading to significant financial and operational repercussions.

Practical Steps

System Audit: Evaluate the current system's performance, scalability, and any gaps in security.

Industry Benchmarking: Compare your system's capabilities against current industry standards and best practices.

Technological Assessment: Keep track of trends such as AI-enhanced analytics, cloud-based access control, and integration with IoT devices.

Stage 2: Gathering Ideas and Future Needs

Engaging Stakeholders

A successful upgrade is driven by the collective input of internal and external stakeholders who have varying perspectives on how the system should perform now and in the future.

Internal Involvement

Security Teams: They understand the day-to-day usability of the system and can provide practical feedback on what works and what doesn't.

IT and Technical Teams: As the backbone of system integration, these teams ensure that any upgrade fits within the organisation's broader infrastructure, including cloud platforms, network configurations, and data security requirements.

Executive Leadership: Their involvement ensures that the upgrade aligns with corporate strategies, budgets, and long-term risk management goals.

External Involvement

Security Vendors and Consultants: Consultants bring in-depth knowledge of the latest security technologies and best practices. Their insights are crucial for identifying which solutions fit your operational needs.

Regulatory Bodies: Ensuring that the system upgrade complies with current regulations, such as those set by GDPR, is essential to avoid penalties.

Practical Steps

Workshops and Brainstorming Sessions: Conduct collaborative sessions with various departments to gather insights on system weaknesses and future security needs.

Scenario Planning: Develop hypothetical situations to understand how the upgraded system could respond to future threats and challenges.

Stage 3: Reviewing Operational Requirements

Reassessing Your Needs

Revisiting the original operational requirements of your security system is essential to ensure that the new system meets both current and future demands. Over time, operational goals can shift, and technologies evolve, making it necessary to determine whether the existing system is still suitable.

Key Considerations

Does the System Meet Current Operational Needs?: Organisations grow, threats evolve, and new compliance requirements emerge. For example, the need for enhanced perimeter controls or more advanced CCTV systems may now be critical.

New Features and Technologies: Consider upgrading to systems that support modern capabilities, such as facial recognition, AI-driven analytics, and remote monitoring.

Fact:

According to a Gartner report, businesses that re-align their security systems with updated operational requirements reduce security breaches by 25%

Practical Steps

Operational Needs Analysis: Work with your internal stakeholders to reassess your operational requirements and align the security system accordingly.

Feature Review: Identify whether the current system's features are still relevant and decide if new functionalities, like biometric access control, should be included.

Stage 4: Scenario and Workflow Planning

Setting Realistic Expectations

One of the most crucial stages in a security system upgrade is establishing realistic expectations regarding timelines, budgets, and potential operational disruptions. Scenario planning and workflow modelling help ensure that all stakeholders are on the same page.

Key Elements

Realistic Timelines: Develop a clear schedule by breaking down the upgrade into phases, such as equipment installation, testing, and training. This ensures that deadlines are achievable and measurable.

Operational Disruption: Every upgrade comes with some degree of disruption. Workflow planning helps in forecasting potential downtime and preparing contingency plans to minimise operational impact.

Budgeting: By detailing each phase of the upgrade, from hardware acquisition to staff training, you can establish an accurate budget, factoring in potential hidden costs like system integration or network upgrades.

Example

When upgrading the security system for a large university campus, scenario planning revealed that scheduling the upgrade during summer, when student traffic was low, reduced operational disruptions by 40%, minimising the impact on daily operations.

Practical Steps

Workflow Modelling: Collaborate with consultants to model every stage of the project and identify potential bottlenecks.

Workshops: Use scenario workshops to identify and mitigate risks, ensuring that budgets and timelines are maintained.

Fact:

A McKinsey study found that 60% of security upgrade projects exceed their budgets due to insufficient early-stage scenario planning.

Stage 5: Implementation and Supporting Infrastructure

Implementing the Upgrade

While installing a new security system is crucial, the success of the upgrade relies heavily on having a **comprehensive technical solution** in place and working with the right contractors to ensure a seamless integration. This phase involves not only rolling out the new technology but also ensuring it functions optimally within your existing infrastructure and future operational plans.

Developing a Technical Solution

A successful upgrade requires a tailored technical solution that integrates seamlessly with existing infrastructure, ensuring that your security systems—such as CCTV, access control, fire detection, and more—are working in sync. The new solution must be robust enough to handle the current demands while being scalable to accommodate future needs, such as adding AI-based video analytics or cloud-based management systems.

Key elements of creating a strong technical solution include:

Ensuring compatibility: Make sure the upgraded system is compatible with both new and existing technology, especially if you're integrating various subsystems like alarms, video surveillance, and access control.

Assessing network requirements: Modern systems require increased bandwidth and secure, scalable networks. If your current infrastructure is outdated, you may need to upgrade your network to fully support the new system's capabilities.

Future-proofing: Ensure that the system can evolve with future advancements and organisational growth. This might include adding features like real-time monitoring, advanced analytics, or facial recognition in the future.

Finding the Right Contractor

Choosing the right contractor is essential for ensuring the technical solution is implemented correctly and within the set timelines. The contractor should not only be proficient in installation but also knowledgeable in integrating complex systems while minimising operational disruption.

Factors to consider when selecting a contractor

Experience with similar projects: Ensure the contractor has a track record of successfully upgrading security systems similar in size and scope to yours. Ask for references and review case studies from their previous clients.

Integration expertise: Contractors with a deep understanding of both legacy systems and modern technology are essential for ensuring the new solution works harmoniously with your existing infrastructure.

Project management capabilities: A strong contractor will provide clear communication, detailed timelines, and flexibility, ensuring the upgrade process runs smoothly from start to finish.

Vendor and third-party coordination: They should also coordinate with other service providers like IT support teams, fire detection contractors, or lift service providers to ensure every part of the system is integrated and functional.

Practical Steps

Technical Solution Review: Conduct a thorough assessment of the system design and ensure it aligns with your operational needs.

Contractor Selection: Choose a contractor based on their experience, expertise in system integration, and ability to provide long-term support.

By focusing on creating a detailed technical solution and selecting the right contractors, you can ensure the security system upgrade delivers on its full potential while minimising disruptions during implementation.

Supporting Infrastructure

Network Upgrades: Modern security systems require robust network support, particularly if they rely on cloud storage or AI-powered analytics. If your existing IT infrastructure is outdated, the system upgrade may fail to deliver its full potential. For example, high-definition CCTV systems and advanced access control systems demand substantial bandwidth and secure, scalable networks.

Key Contractors

Lift Service Integration: For buildings with integrated access control in lifts, ensure coordination with lift service providers to enable seamless floor-specific access.

Fire Detection Systems: Ensure that your fire detection system integrates with your access control for emergency exits, door release mechanisms, and evacuation procedures.

Example

A commercial property upgraded its access control system, but without an IT infrastructure capable of handling the new bandwidth demands of high-definition CCTV, the system faced frequent slowdowns. A network audit and upgrade resolved this issue.

Practical Steps

Infrastructure Audit: Assess whether your current network infrastructure can handle the demands of new technologies. Identify areas where IT systems, data networks, and bandwidth may need upgrading.

Coordinate Contractors: Engage with lift service, fire detection, and other key contractors early in the planning process to ensure seamless integration of all building systems.

Fact:

According to TechTarget, 54% of businesses that upgraded their security systems needed to also upgrade their network infrastructure to support the new technology.

Maximising System Potential and Aftercare

Once the system is implemented, the work doesn't stop there. It's essential to ensure that all staff are trained to utilise the system fully and that ongoing support is in place.

Training: Many organisations fail to leverage all the features of their new system simply due to a lack of training. Proper education on new capabilities like AI video analytics, real-time alert systems, or cloud-based management ensures you maximise system performance.

Aftercare and Support: Post-upgrade support is crucial to the system's long-term success. Ensure that the system provider offers ongoing maintenance, updates, and technical support to address any issues that arise.

Fact:

Security InfoWatch found that businesses that invest in post-upgrade training and ongoing support improve system efficiency by 30%.

Active Insights: Practical Tips for Success

Audit Your Current System: Identify inefficiencies and vulnerabilities before upgrading.

Engage All Stakeholders: From security teams to IT departments, make sure all relevant parties are involved in planning.

Plan for Operational Disruption: Use scenario and workflow planning to predict and manage operational downtime.

Ensure Network Readiness: Conduct a thorough infrastructure audit to ensure your network can handle the upgraded system.

Invest in Training and Aftercare: Maximise the system's features by ensuring all staff are well-trained, and secure ongoing support for maintenance.

Balanced Considerations: Opposing Views

While upgrading a security system offers many benefits, it's essential to also consider potential drawbacks:

Cost vs. Immediate Benefits: Some organisations may find that the cost of upgrading exceeds the short-term benefits, especially if their current system is still functioning well.

Disruption Risks: Even with thorough planning, system upgrades can cause operational disruptions that affect business continuity.

Staff Resistance: Implementing new technologies may face pushback if not adequately supported by training, especially if staff are resistant to change or the system is complex to operate.

Conclusion

Upgrading a major security system is an intricate process that requires meticulous planning, collaboration, and future-proofing to ensure both operational and technical success. By following the five key stages outlined in this guide—recognising the need for an upgrade, gathering ideas, reviewing operational requirements, conducting scenario planning, and implementing the system with supporting infrastructure—you'll be able to achieve a seamless and effective upgrade.

At INA365, we specialise in managing every step of this complex process. From conducting system audits and coordinating contractors to providing workflow workshops and post-upgrade support, our team of experienced consultants ensures that your upgrade is aligned with your operational needs, regulatory requirements, and future scalability. We'll help you navigate potential disruptions, maximise the capabilities of your new system, and ensure its longevity through ongoing support and maintenance.

Contact INA365 today to discuss how we can assist with your security system upgrade and provide a tailored solution that ensures both operational efficiency and the security of your organisation well into the future.

About The Author:

Chris Lakin | chris.lakin@inta365.com

With over 25 years of experience in the security industry, Chris Lakin has held a variety of roles, from product management at a pioneering CCTV manufacturer to owning and operating a successful systems integrator company. His extensive expertise spans all major mission-critical markets, including airports and hospitals, making him an invaluable asset to the INTA365 team. This diverse range of skills and experiences positions Chris at the forefront of delivering innovative and reliable security solutions.

Disclaimer:

This document is intended for informational purposes only. While every effort has been made to ensure the accuracy of the information provided, we do not make any representations or warranties of any kind, express or implied, about the completeness, accuracy, reliability, or suitability of the data, references, or sources cited. Any reliance placed on such information is strictly at your own risk. Furthermore, any references to organisations, individuals, or scenarios are purely hypothetical and not intended to represent any specific entity. The inclusion of examples or case studies is for illustrative purposes only, and any resemblance to real persons or businesses is entirely coincidental.