Jansta Associates
LIMITED

IMPLEMENTING TECHNOLOGY TRENDS

GUIDE NOTE

IMPLEMENTING CYBERSECURITY INTO THE INTEGRATED PHYSICAL SECURITY

+44 (0) 789 685 92 44
www.janstaassociateslimited.com
twitter.com/peter jansta
UK, Europe, Middle East & Asia

Table of Contents

1. INTRODUCTION 3
2. TECHNOLOGY TRENDS 4
   2.1 Hardening Guidelines 4
3. NETWORKS 5
   3.1 Dedicated Networks 5
   3.2 Converged Networks 5
4. ISO STANDARDS 6
5. DEPLOYMENT 6
6. CONCLUSION 6

1. INTRODUCTION

This document is part of the Implementing Technology Trends - Guide Note series, focusing on physical security, project management, electrical, control engineering, and telecoms sectors.

As the world is becoming interconnected, the interdisciplinary approach is essential. It is also clear that a simple application can be the best value on many occasions. The intent is to provide solutions that fit the purpose and simplify even the most complex systems.

The boundaries between physical security and cyber security are becoming ever so thin. Understanding current industry developments will help to deliver practical solutions.

This Guide Note will focus on the implementation of cybersecurity into the physical security solution.

The implementation process will depend on the country's regulator-specific requirements of the project stage. Integrated Security systems should meet minimum operational needs (Operational Requirements).

The below flowchart chart *(© JAL, Fig.1*) shows the typical process in the project management control environment when developing integrated security solutions. The chart captures the complete project life cycle.

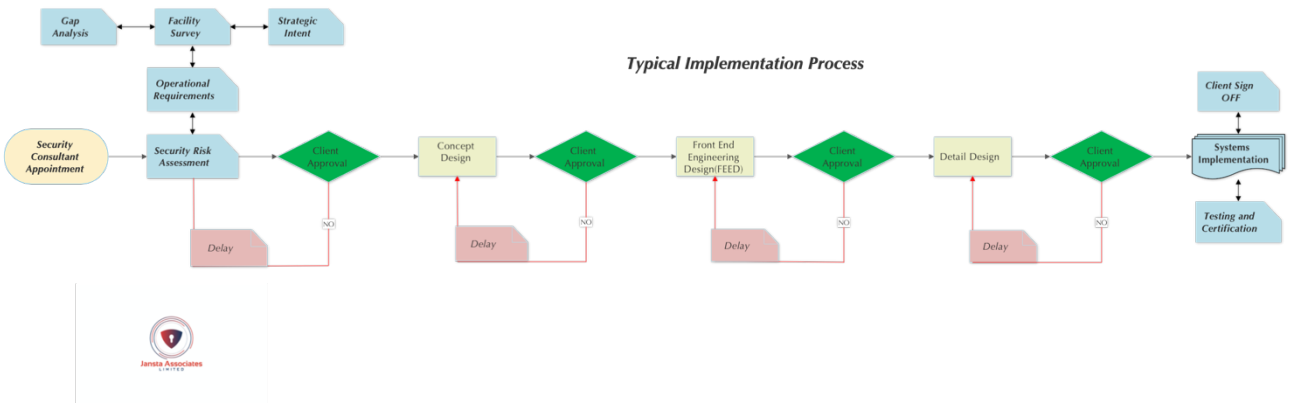

Fig.1 Typical Implementation Process

2. TECHNOLOGY TRENDS

This Guide Note will outline industry trends and how to effectively evaluate the project life cycle to develop suitable integrated physical security solutions whilst implementing cyber security best practices.

The convergence between physical and cyber is becoming ever so prominent. The cloud-based Access Control System and Video Surveillance are becoming cost-effective; hence users preferred options. For example, cloud storage for video, VMS, and SaaS.

The IT industry issues network hardening guides, and video surveillance is catching up with some manufacturers issuing guides and vulnerabilities updates. Whilst manufacturer-specific, these guides are based on main cybersecurity themes (see Fig.2).

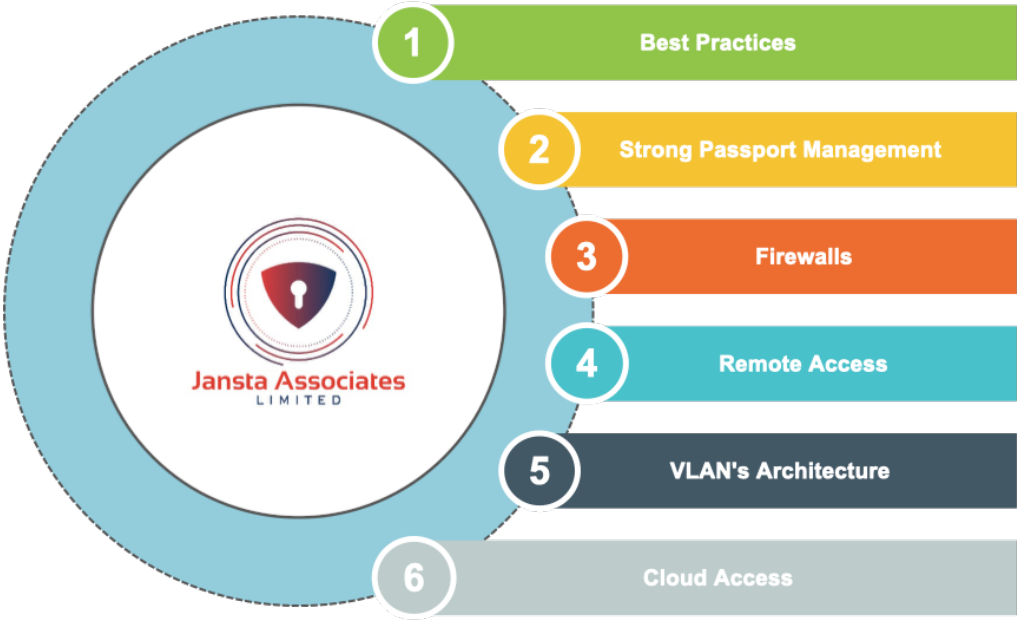

Fig.2 Cybersecurity Themes

If the site and manufacturer-specific countermeasures are well documented and included in the security policy, they should remain effective.

2.1 Hardening Guidelines

In addition to software, the components of installation typically include hardware devices, such as:

- Cameras
- Encoders
- Networking products
- Storage systems
- Servers and client computers (physical or virtual machines)
- Mobile devices, smartphones

Including hardware devices to harden VMS installation is essential. For example, cameras often have default passwords. Some manufacturers publish these passwords online so that they're easy for customers to find. Unfortunately, that means the passwords are also available to attackers.

Cyber Security researchers discover and report on vulnerabilities.[1] They are often providing a summary of the vulnerabilities and their severity. Manufactures issue extensive vulnerabilities reports and guides and provide learning platforms.[2] The emphasis is also on the supply chain and collaboration.

3. NETWORKS

Shall we use an existing network or deploy a new one? This is a critical choice when designing the solution. For example, Access Control Systems is typically a low bandwidth application; the impact on shared and converged networks is much less of an issue than on a video surveillance system.

3.1 Dedicated Networks

Often driven by the client's policy, reduced cyber concerns, best practices, and more control. Dedicated networks will have a higher price tag attached.

Surveillance equipment installed on a dedicated network becomes more difficult to access. To overcome this, VMS servers and NVRs are often equipped with more than one network interface, one used to connect to the camera LAN and another used to connect to the facility's general network. This method makes cameras on the dedicated LAN inaccessible to the main network, but the video may be viewed via the NVR.

Using dedicated networks may also require additional connections and configuration for remote access, as VPNs used for the general network may not have a route to the camera network. This may require a separate VPN setup or cloud connectivity if available.

3.2 Converged Networks

Converged networks share network resources between services like surveillance cameras, VoIP telephones, and general data traffic like email. This may be cost-effective when there are existing PoE ports to add surveillance equipment; however, there will be contention for resources. Many networks were not designed to handle the demands of continuous video surveillance streaming. Local IT policy will retain control.

[1] https://www.nozominetworks.com/blog/new-axis-os-security-research-aided-by-transparent-design/
[2] https://www.axis.com/support/product-security

4. ISO STANDARDS

The standards are becoming increasingly fractured between classical ICS, plus Industrial Internet of Things (IIoT) and Internet of Things (IoT), CCTV, BMS, and other monitoring devices. IT is equally becoming fractured with mobile (iOS and Android) diverging from IT plus outliers such as "wearables".

The attack surface is exponentially increasing. The classic Purdue model (structural model for Industrial Control System (ICS) security, concerning physical processes, sensors, supervisory controls, operations, and logistics) is becoming more challenging for segmentation to protect ICS.

So, there is a need to think holistically whilst also understanding the specific security requirements for each technology domain, including those reliant upon third parties, I.e., SaaS, PaaS and IaaS, hosted services, etc.

5. DEPLOYMENT

The deployment process is critical when developing a new or upgrading the integrated physical security solution.

Changes in how the business operates and risks associated with the security solution can't be overlooked. A complete refurbishment is not always the most feasible option for an outdated security solution. A dedicated network is often the preferred option in some countries stipulated by the legislation. The key to successful transformation is managing the stages and simplifying complex solutions.

Cybersecurity has become a vital issue, with published vulnerabilities, hacks, and botnets rising. Significant vulnerabilities have been reported in multiple manufacturers in the past few years.

Because of the severity of these incidents and their increasing frequency, users must understand the basics of cyber security for surveillance systems and how to protect against simple attacks at the very least. Cybersecurity issues have also contributed to government action against multiple manufacturers.

6. CONCLUSION

The key to successful transformation is managing the stages and simplifying complex solutions. To achieve the desired output, a clear objective and planning are essential.

Developing robust and practical integrated security solutions requires a multidisciplinary approach whereby implementing cybersecurity from the inception to the end of the project.

*At **Jansta Associates Limited**, we serve our clients with various engineering consulting services. So, if you are thinking of deploying new technology, designing, or updating the system, we can help you navigate this complex subject.*

+44 (0) 789 685 92 44
www.janstaassociateslimited.com
twitter.com/peter jansta
UK, Europe, Middle East & Asia