Princess Juliana International Airport

CYBER SECURITY IMPLEMENTATION AT PJIAE

- Challenges and Real-World Applications

Presented By: **JHONNY S. VALDEZ**
SYSTEM INTEGRATION AND CORE INFRASTRUCTURE MANAGER

www.sxmairport.com jvaldez@sxmairport.com

Date **05/05/2025**

INTRODUCTION

- Brief overview of:
- The importance of cybersecurity in any organization
- The regulatory environment (e.g., NIST, ISO 27001, GDPR, HIPAA, etc.)
- Goal: Ensure compliance and protect critical assets

HERE'S A BRIEF DESCRIPTION OF EACH FRAMEWORK AND REGULATION:

1. NIST Cybersecurity Framework (NIST CSF)

- Developed by: National Institute of Standards and Technology (USA)
- Purpose: Provides a flexible, risk-based approach to managing and reducing cybersecurity risks.
- Core Functions: Identify, Protect, Detect, Respond, Recover
- Used by: Primarily U.S. critical infrastructure sectors but widely adopted globally as a best-practice model.

2. GDPR (General Data Protection Regulation)

- Developed by: European Union
- Purpose: Regulates how organizations collect, store, and process personal data of EU citizens.
- Key Principles: Data minimization, consent, transparency, right to access, right to be forgotten.
- Applies to: Any organization (even outside the EU) handling EU citizens' data.

HERE'S A BRIEF DESCRIPTION OF EACH FRAMEWORK AND REGULATION:

3. ISO/IEC 27001

- Developed by: International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC)
- Purpose: Specifies requirements for establishing, implementing, maintaining, and continually improving an information security management system (ISMS).
- Focus: Risk management and data confidentiality, integrity, and availability.
- Used by: Organizations worldwide aiming to demonstrate commitment to security through certification.

4. HIPAA (Health Insurance Portability and Accountability Act)

- Developed by: U.S. Department of Health and Human Services (HHS)
- Purpose: Protects sensitive patient health information from being disclosed without the patient's consent or knowledge.
- Key Rules: Privacy Rule, Security Rule, Breach Notification Rule
- Applies to: Healthcare providers, health plans, and business associates in the U.S.

KEY REGULATIONS/ GUIDELINES FOLLOWED CIA TRIAD

- NIST Cybersecurity Framework (CSF)
- ISO/IEC 27001
- GDPR / CCPA / HIPAA (depending on your sector)
- Internal policies aligned with best practices

Confidentiality	Integrity	Availability
Ensuring information is accessible only to authorized individuals.	Protecting data from unauthorized alterations.	Ensuring systems and data are accessible when needed.

IMPLEMENTATION APPROACH

IMPLEMENT

- Risk assessment and gap analysis
- Security policies and procedures
- Regular training and awareness programs
- Deployment of technical controls (firewalls, SIEM, MFA)
- Compliance audits

Challenges Encountered

- Frameworks can be overly broad or vague
- High implementation and maintenance costs
- Lack of skilled personnel
- Integrating new tools into legacy systems
- Employee resistance or lack of awareness

Overcoming the Challenges

- Prioritizing based on risk
- Leveraging government or vendor-provided templates and tools
- Using phased implementation and continuous improvement
- Outsourcing where necessary (MSSPs)

Benefits Realized

- Reduced security incidents
- Increased trust and compliance readiness
- Better visibility into system vulnerabilities
- Culture of security awareness

Lessons Learned

- One-size-fits-all doesn't work—customization is key
- Communication and training are as important as tech
- Continuous monitoring is essential

COMMON VULNERABILITIES

- Human error.
- Weak passwords.
- Outdated software and systems.
- Poor network security configurations.

CONCLUSION

- Regulations offer structure but must be adapted
- Ongoing effort needed for full maturity
- Cybersecurity = people + processes + technology

Q&A
ANY QUESTION?

Princess Juliana
International Airport