it is about you feeling **SAFE**

Risk Assessment

Introduction

- Physical Security
- Physical Security Planning
- The Security Triangle
- The Domains

Introduction – Physical Security

- The Physical (Environmental) Security domain addresses the threats, vulnerabilities, and countermeasures that can be utilized to physically protect an enterprise's resources and sensitive information. These resources include people, the facility in which they work, and the data, equipment, support systems, media, and supplies they utilize.

Introduction – Physical Security

- **Threats to physical security include:**
  - Interruption of services
  - Theft
  - Physical damage
  - Unauthorized disclosure
  - Loss of system integrity

Introduction – Physical Security

- **Primary consideration in physical security is that nothing should impede "life safety goals."**
  - Ex.: Don't lock the only fire exit door from the outside.
- **"Safety:" Deals with the protection of life and assets against fire, natural disasters, and devastating accidents.**
- **"Security:" Addresses vandalism, theft, and attacks by individuals.**

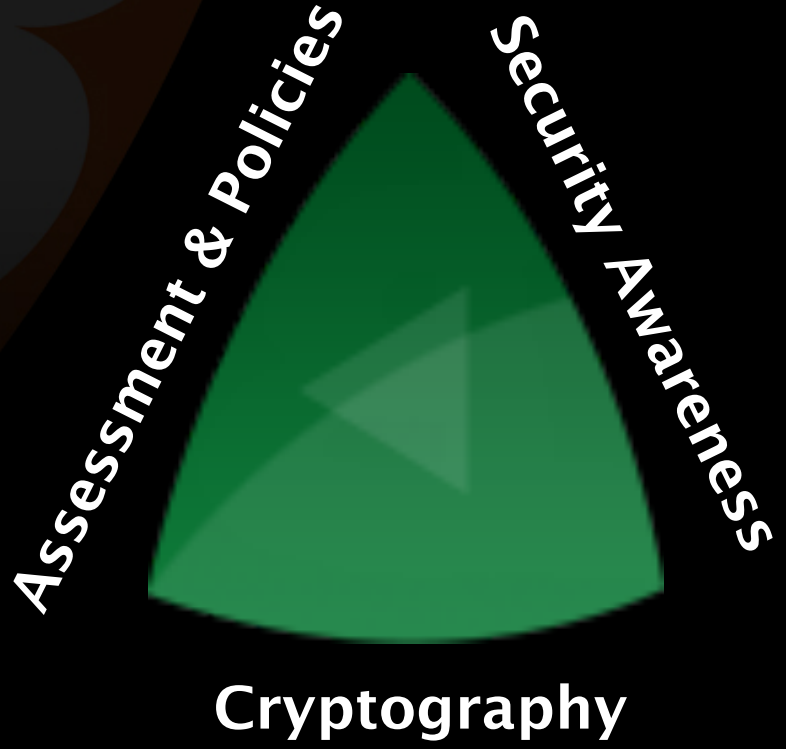
Physical Security Planning

- Physical security, like general information security, should be based on a layered defense model.
- Layers are implemented at the perimeter and moving toward an asset.
- Layers include: Deterrence, Delaying, Detection, Assessment, Response

Physical Security Planning

- **Threats fall into many categories:**
  - Natural environmental threats
    (e.g., floods, fire)
  - Supply system threats
    (e.g., power outages, communication interruptions)
  - Manmade threats
    (e.g., explosions, disgruntled employees, fraud)
  - Politically motivated threats
    (e.g., strikes, riots, civil disobedience)

Security Triangle



Risk Assessment - 1

- **Against what and who should I protect?**
  - Perform Risk Assessment
- **Be aware of terminology:**
  - Risk Identification (RI)
  - Risk Assessment (RASS = RI + ‘value’)
  - Risk Management (RM = How to protect)
  - Risk Analysis (RASS + RM)

Risk Assessment - 2

- **Some attention points:**
  - Different Risk Assessment/Analysis methodologies
  - Sometimes difficult to determine the ‘value’
  - Make sure that you’ve the right people, meaning:
    - Who know the business processes
    - Who have authority to decide

Security Policies

- Formalization of the Security Strategy and objectives
- High Level

Security Policies - 2

- **Project Security Policies:**
  - General description of the Project
  - Security around the Project
  - Security on the Project
  - Technical security settings (detection, alarms…)
- **Other important policies are, for example:**
  - Asset Classification
  - …

Security Policies – 3

- **Make sure that:**
  - The policy is supported by the System Owner
  - You avoid the ‘Ivory Tower Syndrome’
  - The policy is clearly communicated
  - The policy is useful and pragmatic

Security Procedures

- **Who is doing what, why and when?**
- **Important procedures are, for example:**
  - Boarding Process
  - Incident & Escalation
  - Back-up/Recovery
  - Change & Configuration Management
  - …

Security Standards

- Are we on our own?
- No, there are standards out there
- A set of best practices
- Can be a good starting point and prevents to re-invent the wheel
- However, be careful not to implement a security standard blindly…