

# PHYSICAL SECURITY ISSUES

*Jack Mattera, CFCE, CFE*  
*Director*

Copywrite Intelysis 2004



# Need to Determine/Understand

- Principles behind security measures
- What level of security is required



# What is it we are trying to protect?

- People
  - Employees
  - Visitors
  - Shareholders



# Our Physical Assets

- Servers
- Workstations
- Portables
- Network Hardware
- Communications Hardware



# Our Physical Assets

- Records and Files
- Internal documents
- Inventory of goods



# Our Intellectual Assets (Information)

- Intellectual Property
  - Proprietary Technologies
  - Business Plans
  - Sales data
  - Financial Information
  - Marketing Plans
  - and virtually everything you need to compete.



# Why are Intellectual Assets Difficult to Secure?

- Because Sensitive Information can be anywhere...
  - Paper Files and Documents
  - Servers, Desktops, Laptops, PDAs – or somewhere in transit
  - The heads of authorized users, primarily your employees.



# Things to take into consideration

- Physical Security:
  - Guards
  - Card Access Systems
  - Cameras
  - Asset monitoring
  - Primarily HR or facilities function



# Tomorrow's Security Solution:

- **Corporate Security = Physical Security + Information Security + *Operations Security***
  - *OP Sec* secures key information that is sought by competitors/those wishing to do you harm.
  - All three areas must integrate to provide adequate and thorough security for today's businesses.



# Security Fundamentals

- Access Control
- Monitoring and Detection



# Traditional Security Measures

- Know your employees
- Restrict Access
- Audit Access
- Secure Hardcopy
- Wipe Obsolete Drives



# Know Your Employees

- Conduct background checks before hiring
  - Scale inquiry to level of access
  - Consider periodic updates of employees in sensitive positions
- Require same level for contractors with access to same data



# Have Appropriate Policies in place

- Allow for monitoring of “problem employees”
  - E-mail, Web Access, Files
  - Restrict physical access
    - Segment premises into areas of access
    - Not unlike cyber security



# Restrict Access

- General
  - Access to all parts of the office
  - Require visitors to sign in
    - Issue ID badges and require they be worn
  - Escort all visitors



# Restrict Access

- General
  - Use proximity card for entry
  - Run audit trail to log entry
  - Create/enforce policy against tailgating
  - Consider video at entry points
    - Both interior and exterior



# Restrict Access

- High security areas
  - Server or computer room/ Data Center
  - Network hardware
    - Routers/gateways/etc.
  - Communications hardware
    - Phone/data closets
- Video entrance to any sensitive areas



# High Security Areas

- File/Records storage rooms
- Executive suite
- R&D facility
- HR area



# Audit Access

- Allow for audit capability on all access points
- Periodic review of data collected
- Allow for sufficient resources
  - Archives
  - Remote access
  - 24/7/365 coverage



# Secure Hardcopy

- Create/enforce clean desk policy
  - Periodic inspection
- Create/enforce shredding policy
  - Crosscut – not strip
  - Can't shred enough
- Beware of discarded manuals/employee directories, etc.



# Issue in Physical Site Survey

- First must determine
  - Who will need to access facility
  - Are there regulatory issues
  - What is corporate security culture



# Issues in Physical Site Survey

- Entry Points to facility/restricted areas
  - Lighting
    - What will it be used for
  - Choke Point
    - Badge/ID
    - Barrier
  - Guards
    - Armed?
    - Uniformed?



- Cameras
  - What is it you are trying to capture
  - Overt/Covert
  - Open/Protected
  - Record/Review
    - Who/Where
- Electronics to record access/egress
  - Audit Trails



- Physical search of belongings
  - Employees and/or visitors
  - Mail/Deliveries
    - In/Out
- Doors
  - Hollow Core/ solid wood or steel?
  - Fire rated
  - Alarmed
    - General
    - Prop alarm



- Policies

- Challenge Visitors?

- Polite offer to help
- To whom to report strangers

- Tailgating

- Access in general

- Levels or access

- Items leaving building

- Checked
- Signed out/property pass



# Sensitive/Restricted Data

- How is it stored/secured
- How is it disposed
  - Shredder
  - Hard Drives forensically wiped
  - Other computer media



# Facility Cleaning/Maintenance

- When are these services performed
- Who are they performed by



# Questions????

Jack Mattera

Intelysis

950 Kings Highway North ~ Suite 202

Cherry Hill, NJ 08034

Office: 856-667-4180 x.222

Fax: 856-667-4203

24 Hour: 1-877-774-1307

E-mail: [jmattera@intelysis.com](mailto:jmattera@intelysis.com)

Web: [www.intelysis.com](http://www.intelysis.com)

