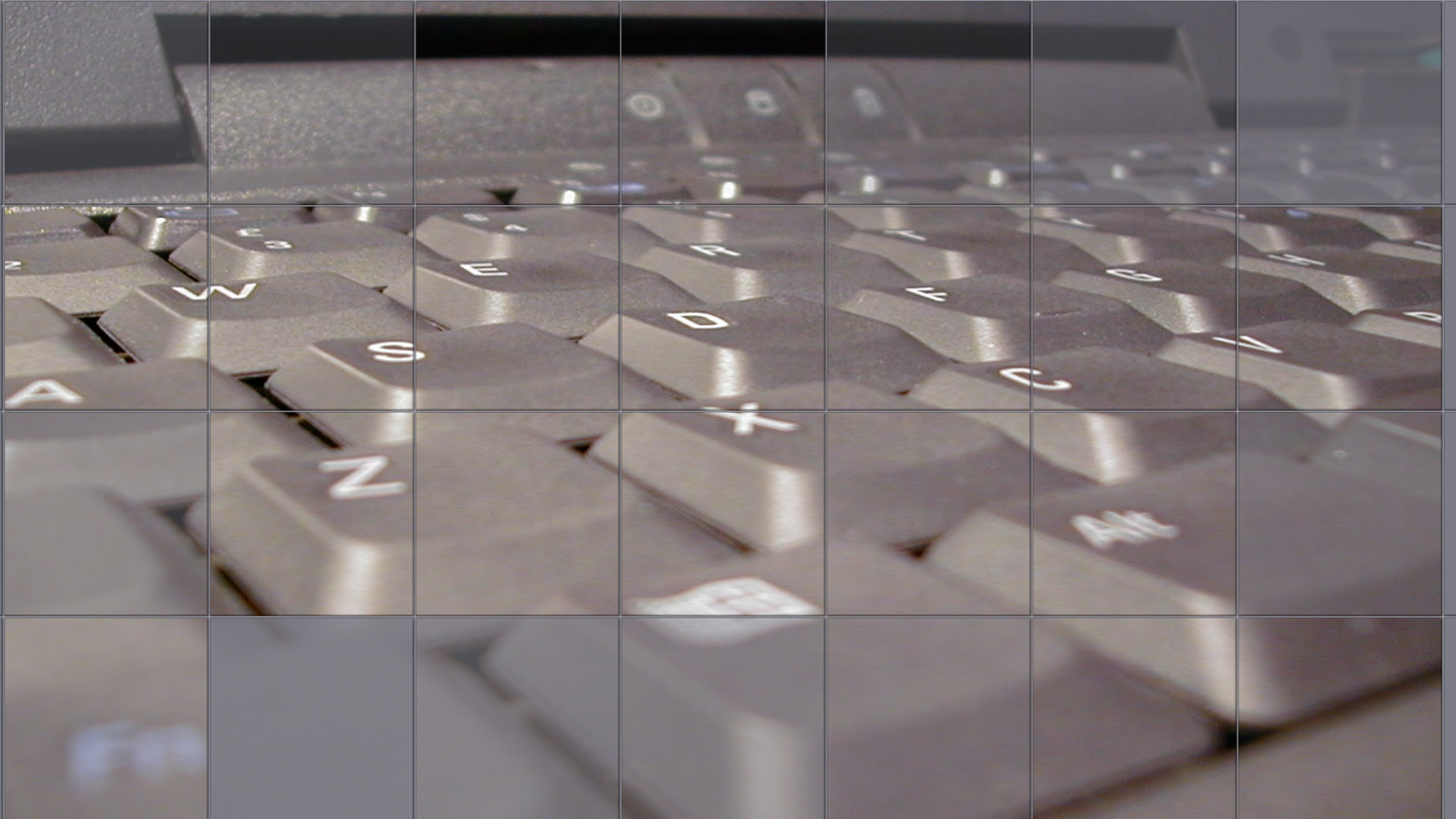


Infosec: What the Physical Security Practitioner Should Know

Aaron Hughes, CISSP
IAC SecureTech
www.iacsecuretech.com



Goals

Impossible to go into great depth on all procedures and permutations in 40 minutes.....

Understand commonly overlooked but critical logical security components and how they relate to physical security

Understand general overview of information security and physical security tie-ins

Understand an easy method for understanding real-world connections between physical security and logical security

Put information in context with real scenarios

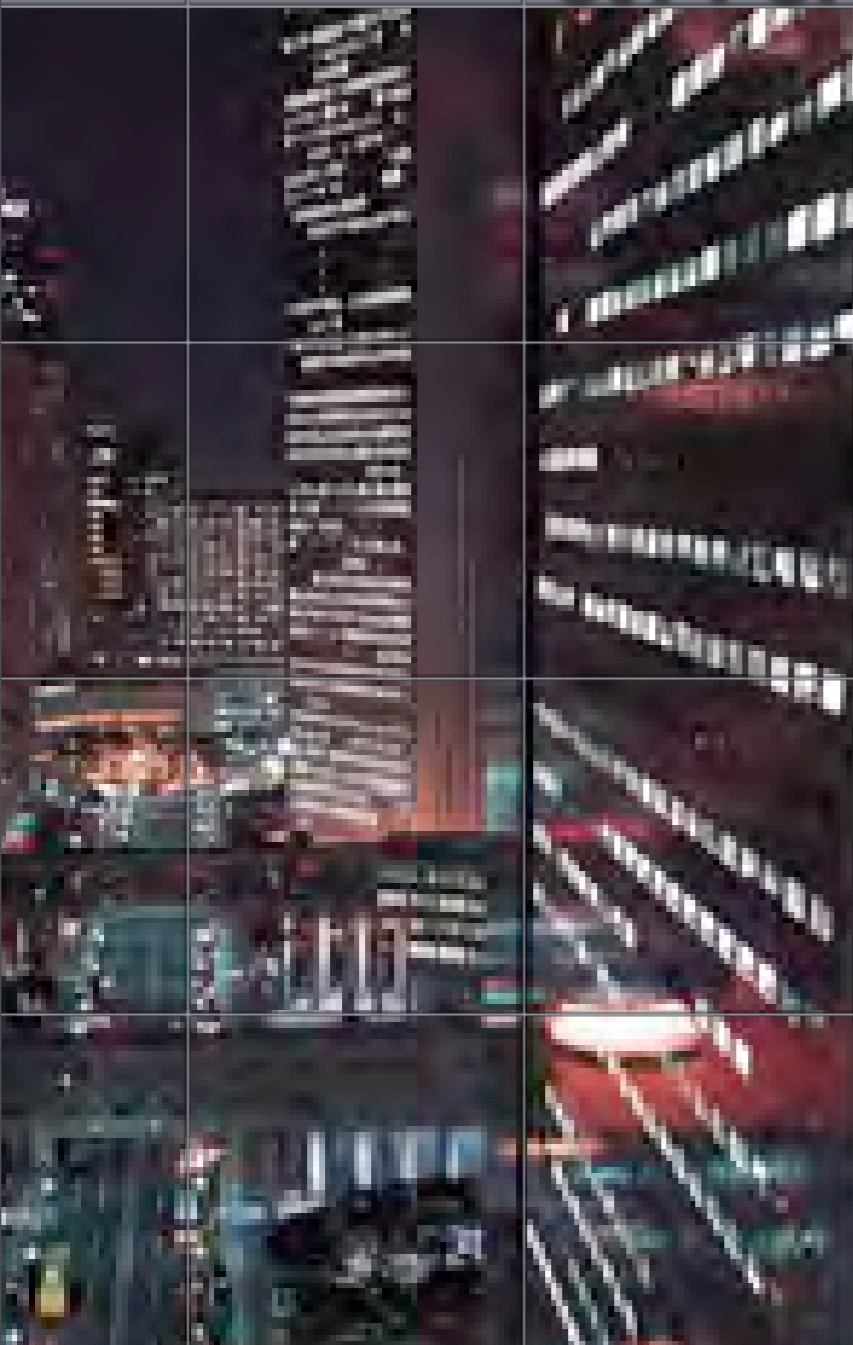
Goals

Why Does This Matter To You?

Overcome the “historic disconnect”.

Increase communication and support
between the two sides.

Similarities between Physical and Logical Security



- Risk

 - Must assume *SOME* risk.

- Avoid the "Money Pit"

 - A point of diminishing returns exists

- Technology Support

 - Policy and Procedure is Key to success.

Security Balance Model



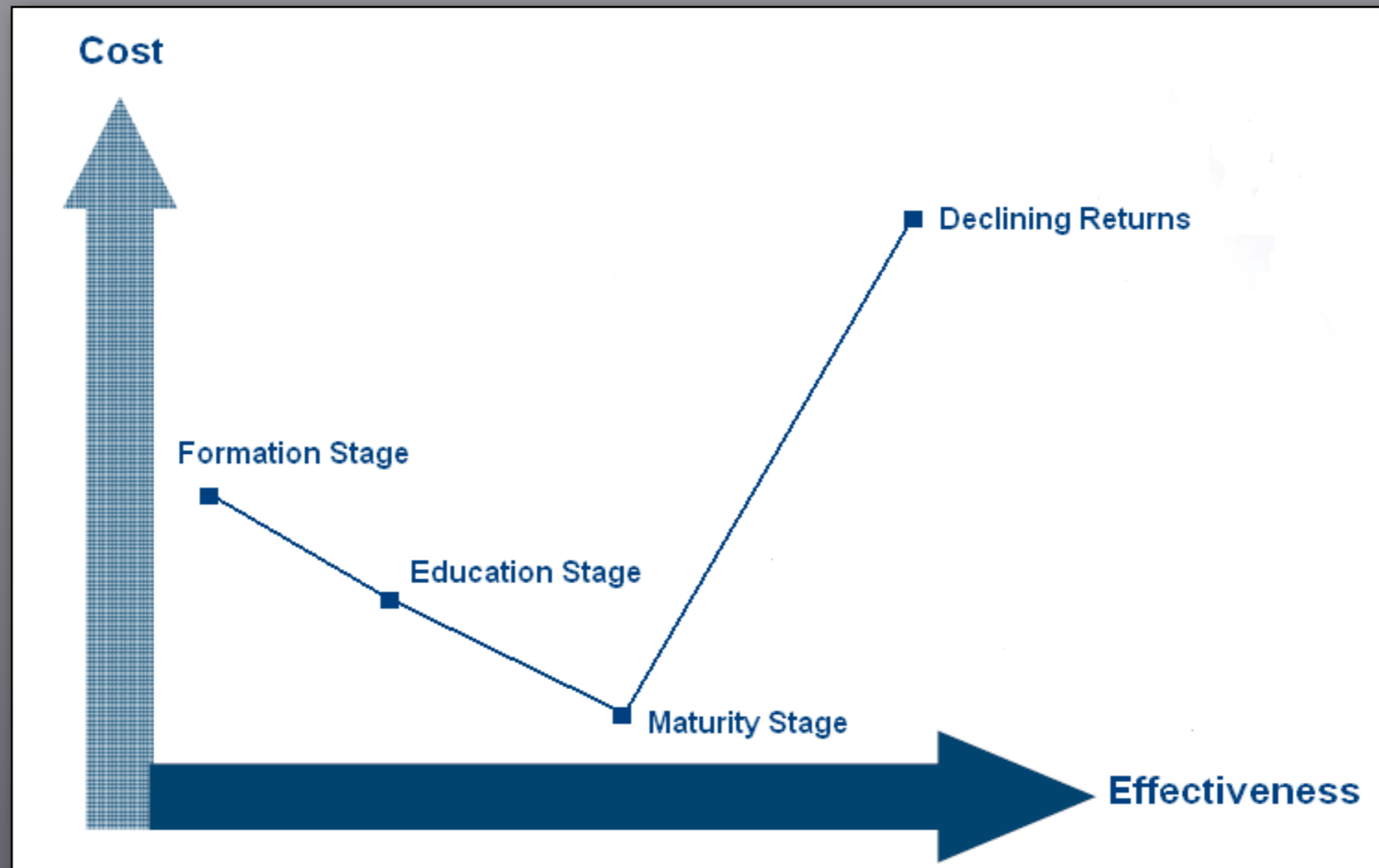
Determine the Balance Point

- Education
- Policy and Procedure

Maintain the Balance Point

- Technology that supports Policy & Procedure
- Consistent Monitoring and Response

“Point of Diminishing Return”

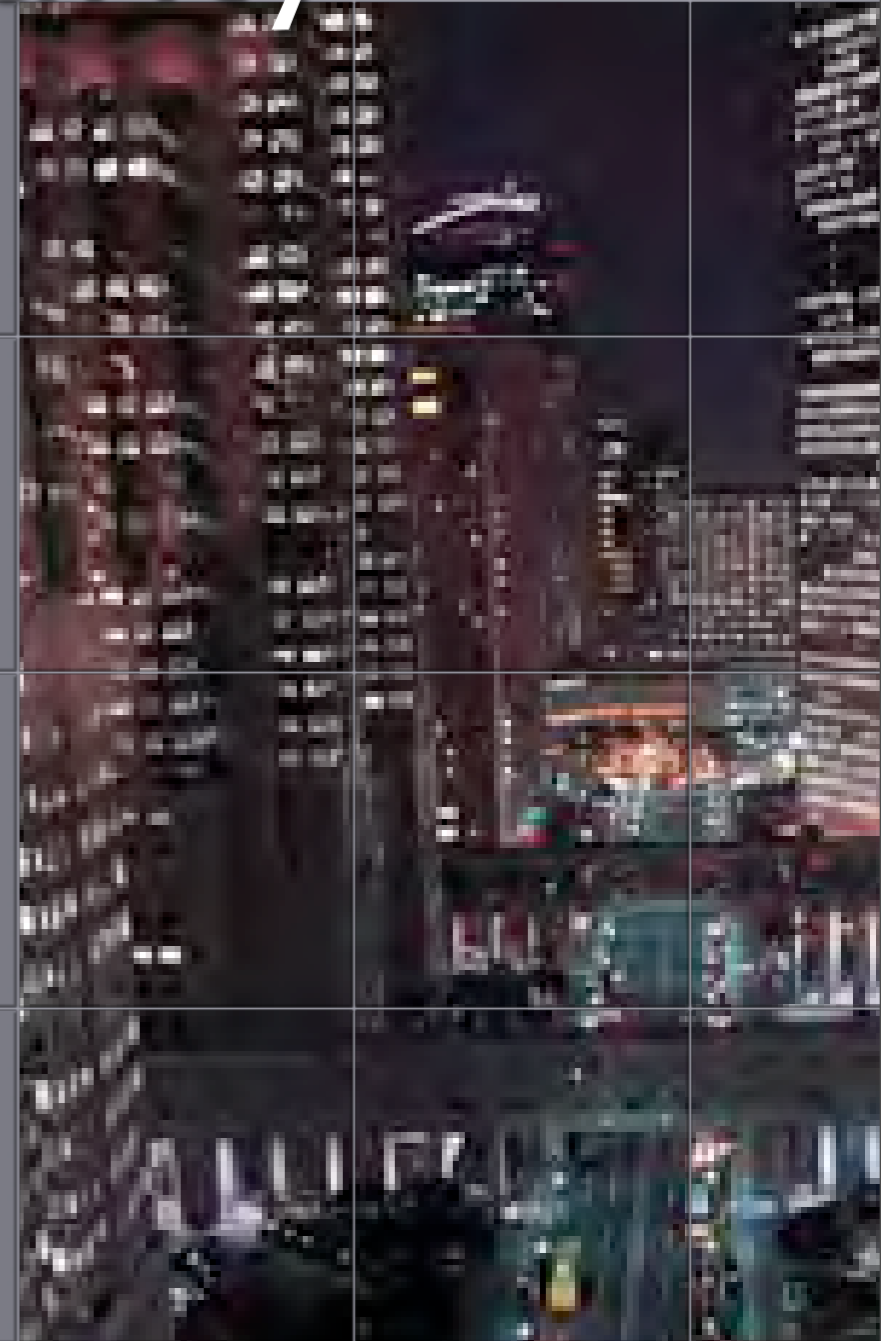


Differences between Physical and Logical Security

- Higher risk for perpetrator at physical level

However:

- Successful physical access drops the bar on technical capability
- Successful physical access creates a whole different level of attack
- Physical Security more advanced in a lot of ways (Lots more time to get it right!)
 - Safe vs. Firewall



Physical Security

(From the Eyes of a Logical Security Guy)

Physical Security:

- Environment
- Access Control
- Intrusion Detection
- Monitor and Manage

Ultimate Goal Is..... ?

Logical Security

Logical Security:

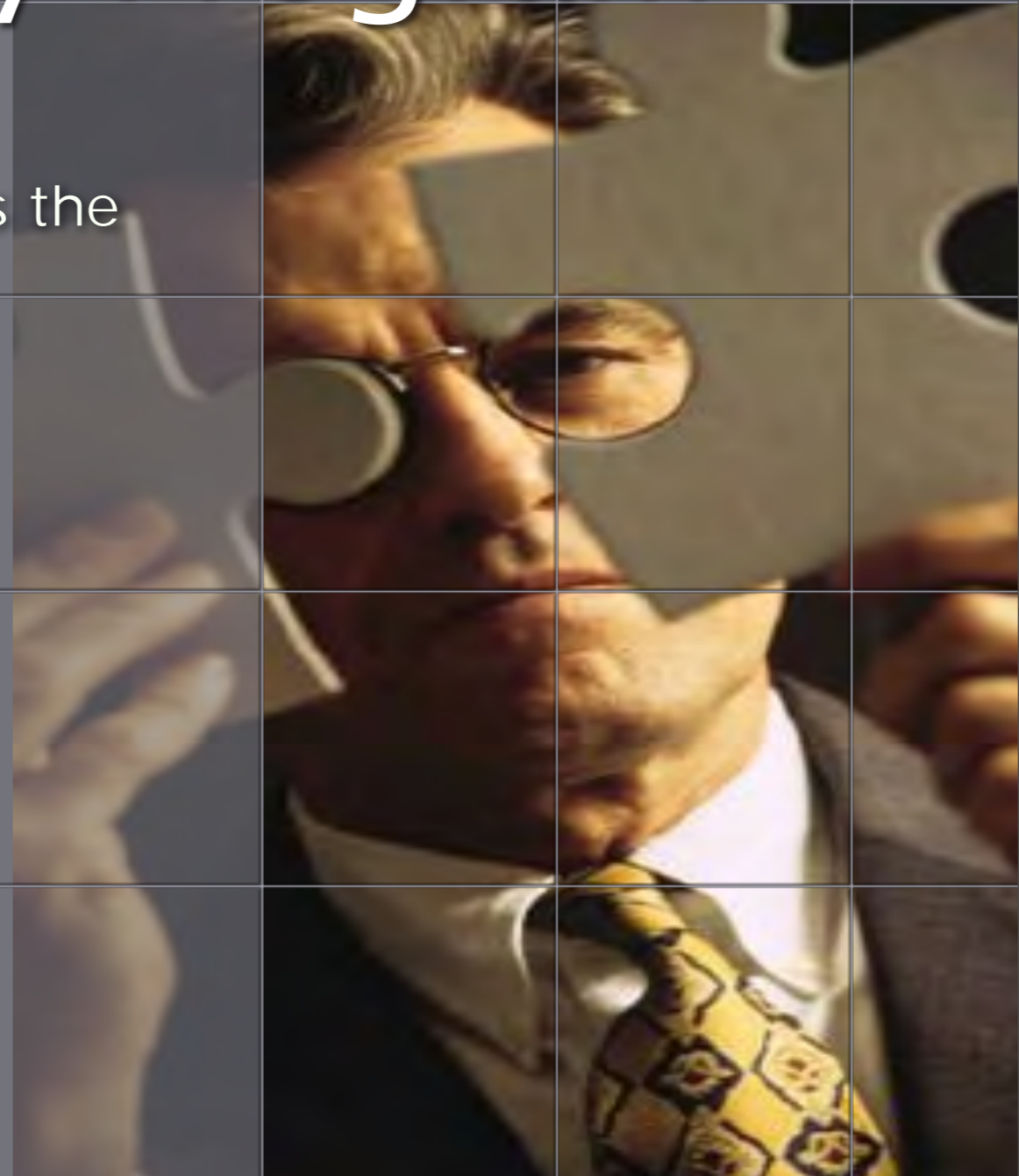
- I
- A
- C

Once a perp has physical access the game is over!

Characteristics of a Solid Logical Security Program

Each piece operates, "fits" and supports the other pieces.

- Perimeter
- DMZ Technology
- Early Detection Monitoring
- Response Capability
- Policy and Procedure
 - The "Big 5" P & P
- User Education



Avoiding The Money Pit: Policy and Procedure

"The Big 5" of Effective Security Program:

- Acceptable Usage Policy
 - Must agree (not "understand") monitoring takes place.
 - Should state implicitly "no reasonable expectation of privacy".
- Remote Access
 - Whose equipment is used to access main network? How is the equipment certified/maintained?
- Data Encryption
 - Data at rest and in transit.
- Response
 - "The Bad Date Rule"
- Business Continuity
 - Data replication AND function replication

Assessment and Audit: Attack Vector Analysis

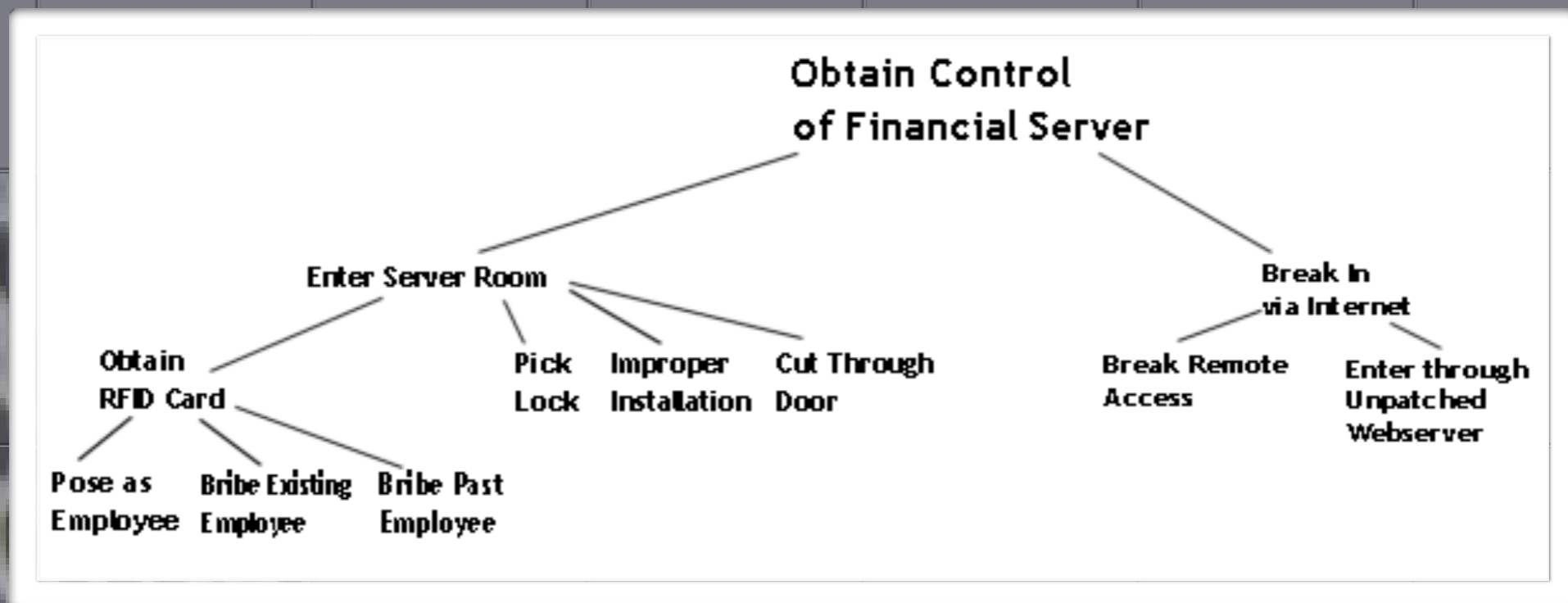
(Threat Modeling/ Attack Trees)

Where is the attack most likely to come from?

Provides planning for various attack scenarios, typically:

- Difficulty of attack
- Cost to attack
- Likely detection of attack
- Cost to the organization of a successful attack
- Cost to the organization to mitigate an attack path

Threat Modeling Example



Real World Examples

Examples of Physical Considerations:

- Environment:
 - RJ45 jack placement
- Access Control
 - Security Guard Habits
 - Server Room Locks
- Information leakage
 - Sensitive Document Handling (Military Base)

Valuable Resources

Action Plan:

- Valuable Reading:
 - www.sans.org/reading_room/
 - Logical Security Policy and Procedure Examples
 - Email me: HughesA@IACSecureTech.com
 - Threat Modeling
 - Attack Trees (Bruce Schneier):
 - <http://www.schneier.com/paper-attacktrees-ddj-ft.html>
 - Threat Modeling Software
 - Microsoft (if problems finding it contact me)
 - Book: Frank Swiderski
 - *ME! - Contact anytime.*

"Security is a process, not an event"

Infosec: What the Physical Security Practitioner Should Know

Aaron Hughes, CISSP
President/CEO
IAC SecureTech
www.iacsecuretech.com

281-705-9714
hughesa@IACSecureTech.com