Security Convergence
What You Need to Know

Ron Woerner, CISSP

Warren Phillips

August 22, 2008

NEbraska CERT Conference 2008

Computer Security
and Information Assurance

Ground Rules

- This is our interpretation and summary and not necessarily the opinion of our employer.
- We want to share ideas on how people enforce, enact, or increase security in their organizations.
- Please feel free to ask questions or make comments at any time.

What does Security Convergence mean to you?

ASIS Definition[#]

The identification of security risks and interdependencies between business functions and processes within the enterprise and the development of managed business process solutions to address those risks and interdependencies.

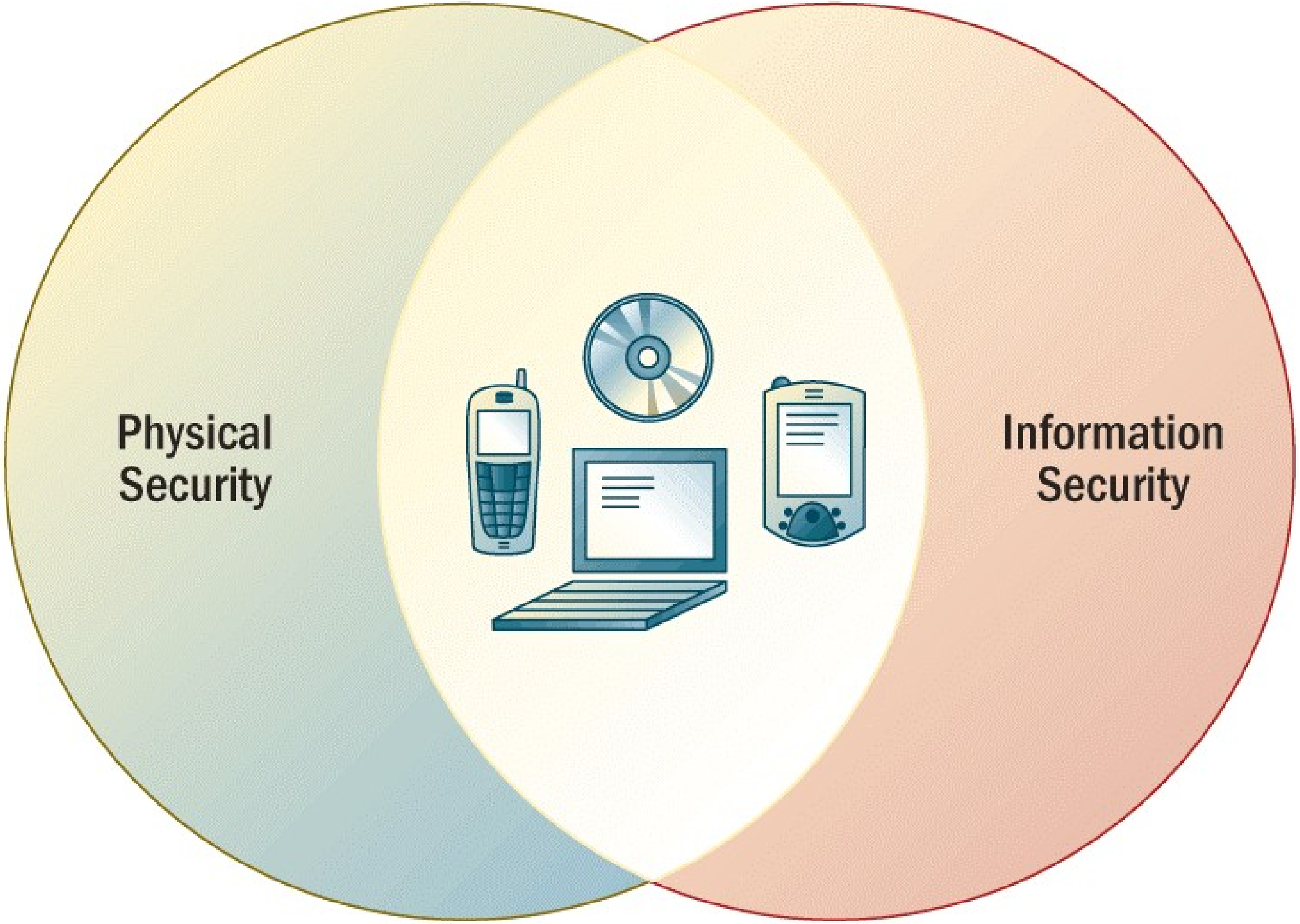
http://www.asisonline.org/

What it really is

Formal cooperation between previously disjointed security functions:

- Physical
- Information / Logical

What it really is



Problem

“Security doesn't exist in a vacuum; our role is to allow our organizations to take as much risk as they want to take in the safest way possible. We don't just need to learn "their" language and methods – we need to translate our needs to their needs, and vice versa.”

Rich Mogul, Dark Reading Blog, Jan 30, 2007,

http://www.darkreading.com/document.asp?doc_id=144600&WT.svl=column1_1

Security Convergence Benefits

- Common concepts
  - Protection
  - Risk Management
- Alignment of goals
  - Security
  - Business
- Single Focal Point
- Information sharing

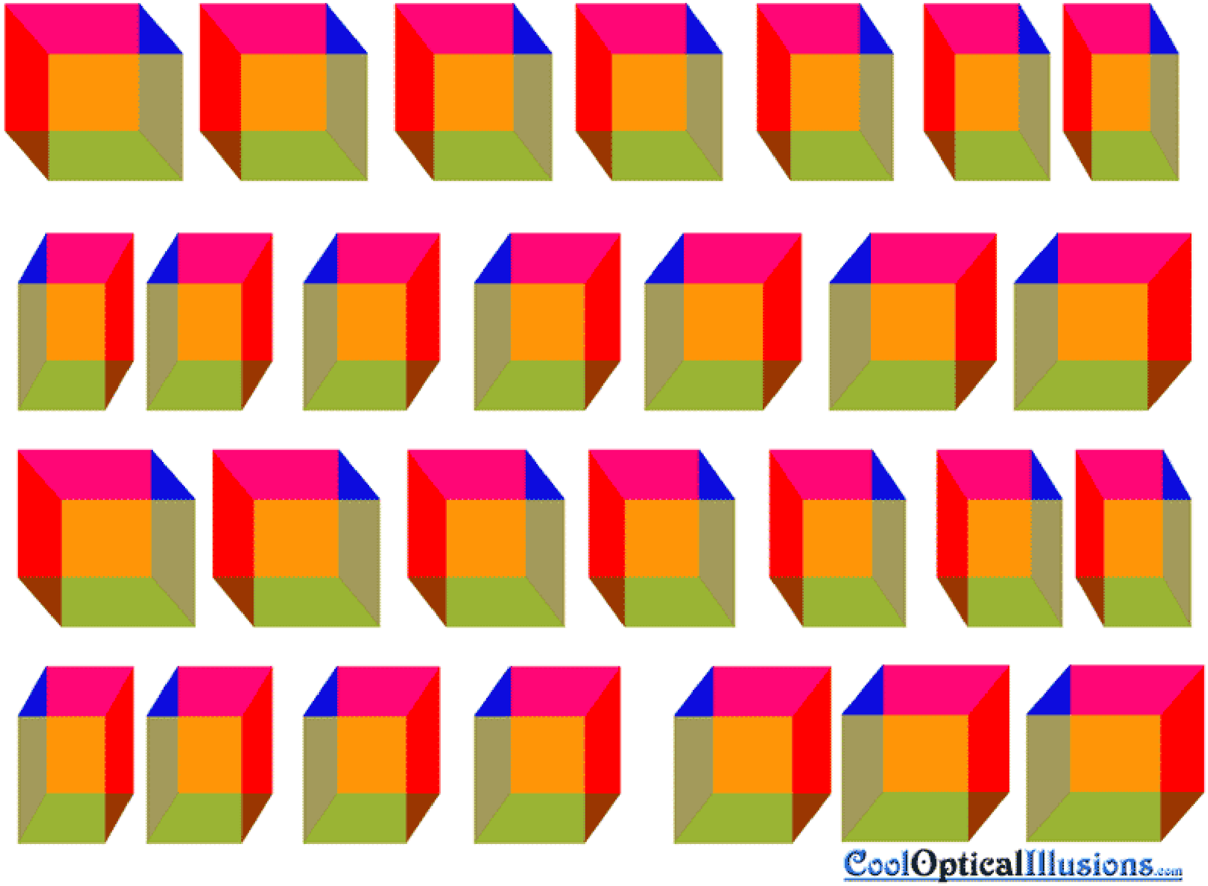
More Benefits

- Incident response and investigations
- Employee on-boarding / off-boarding
- Versatile security staff
- Technology convergence
- Save $$$

Challenges

- Cultural & background differences
- Lack of knowledge / experience
- Complicated infrastructure
- Lack of seen ROI (ROSI)
- Pay differences
- Education differences
- Turf battles and politics

Problem with Perspective



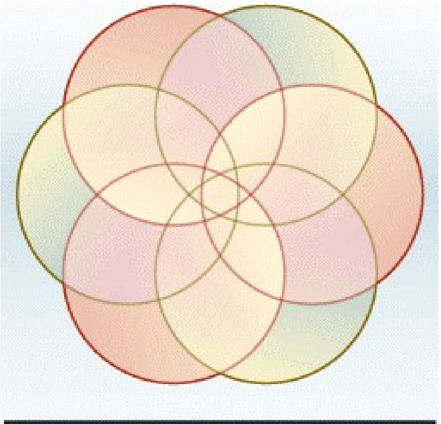
Complete Asset Protection

- Complete picture on risks to assets
- Protection throughout its lifecycle
- Peel the onion

Creating a Converged Security Program

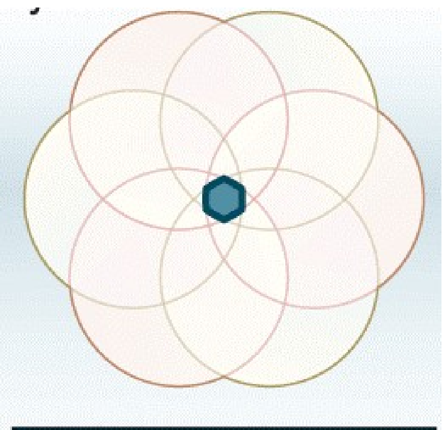
- Have your champion
- Plant the seeds and continually water them
  - Security
  - Business
- Learn and coach
- Collaborate
- Start doing it

Effect of Convergence



FROM

Multiple Functional Risk disciplines within a financial institution met individually with Business Units (BU) leaders, with redundant question sets and performing similar analysis using dissimilar methodologies.



TO: CONVERGENCE

A corporate risk group leader identified the overlap and worked together with the BUs and functional groups to rationalize the question sets, and develop a standardized approach and sequence for their visits.

As quoted in the December 2005 Information Security magazine article Thinking Ahead,

"*Security is now about risk management… This cannot be accomplished by a technician, but by a business leader with the proper authority to see that appropriate business decisions are made*."

Enterprise Risk Management (ERM)

“Enterprise risk management is a process, effected by an entity’s board of directors, management and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risk to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives.”

Source: COSO *Enterprise Risk Management – Integrated Framework*, 2004

Why ERM is Important

ERM supports value creation by enabling management to :

- Deal effectively with potential future events that create uncertainty.
- Respond in a manner that reduces the likelihood of downside outcomes and increases the upside.
- Prioritize risks.
- Ensure risks are identified and mitigated appropriately with NO SURPRISES.

Enterprise Risk Management

=

Security Convergence

=

Total Asset Protection

Traditional Physical Systems

- Badging / Physical Access
- Video Surveillance

Physical Access Control

Operating Fundamentals

Physical Access Control

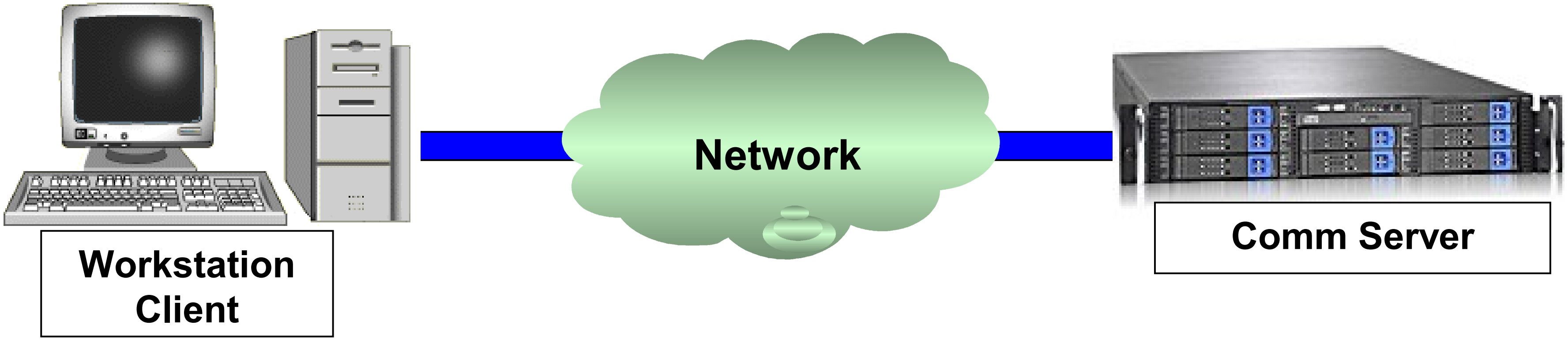
The basic components for a Physical Access Control system are the Control Panels (Nodes), the Database Communications Server and the various Workstation Client PCs

Control Panel

Database Communications Server

Workstation Client

1. Using the workstation client, you can now communicate back and forth with the server and create the application system in the database.
2. The database includes functions to allow for system activity and access card activity processes. Reader Access lists will also be contained here.
3. You can have a local hardwired system operating in one building or program network connections to accommodate remote locations as well.
4. The input for database changes are accomplished from the Workstation Client



Workstation Client

Network

Comm Server

Access Control Panel/Node

2. The access control panel maintains a local database to process events and alarms. The database is downloaded from the server and on a continuing basis, database changes are also downloaded. This database will also contain lists of authorized access to individual card readers.

3. Events and alarms are processed and archived in the comm server. At the same time they can be displayed on event screens at the Workstation PC to provide real time monitoring.

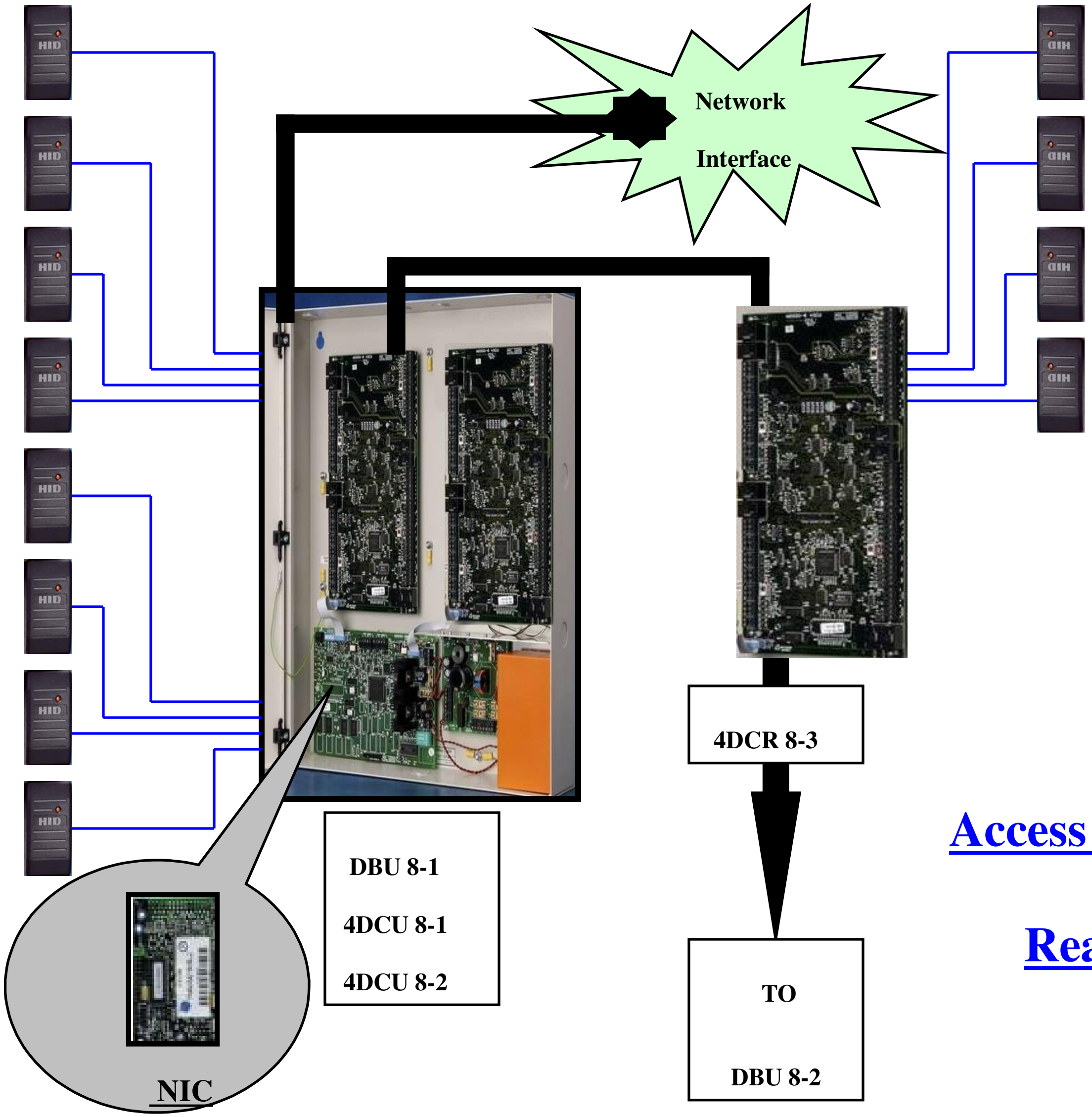
4. When the local database is created and residing on the panel itself, it can operate independently from the server within it's own building.

Control Panel

Badge

Readers /

Doors



Network

Interface

DBU 8-1

4DCU 8-1

4DCU 8-2

4DCR 8-3

TO

DBU 8-2

NIC

Access Control Panel

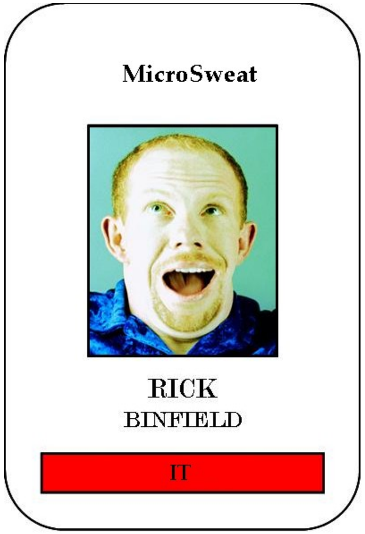
Readers/Devices

Access Control

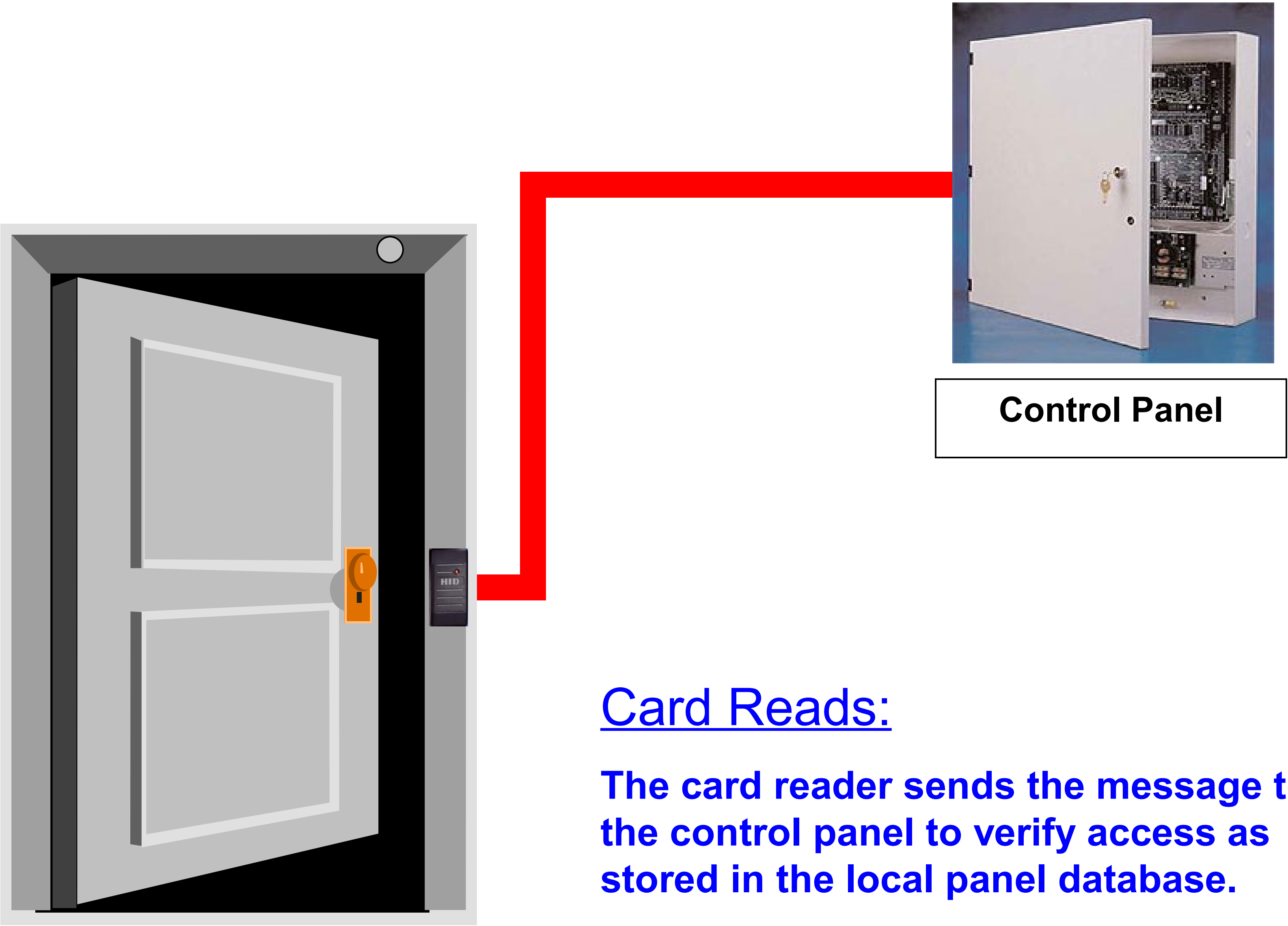
Alarms & Events Communications

A Typical Access Door would have a type of door monitor contact and a card reader attached to control access and system door monitoring

In a system using proximity type cards, pass your access card (or similar credential) by the card reader. There are also various ways to allow exiting doors.

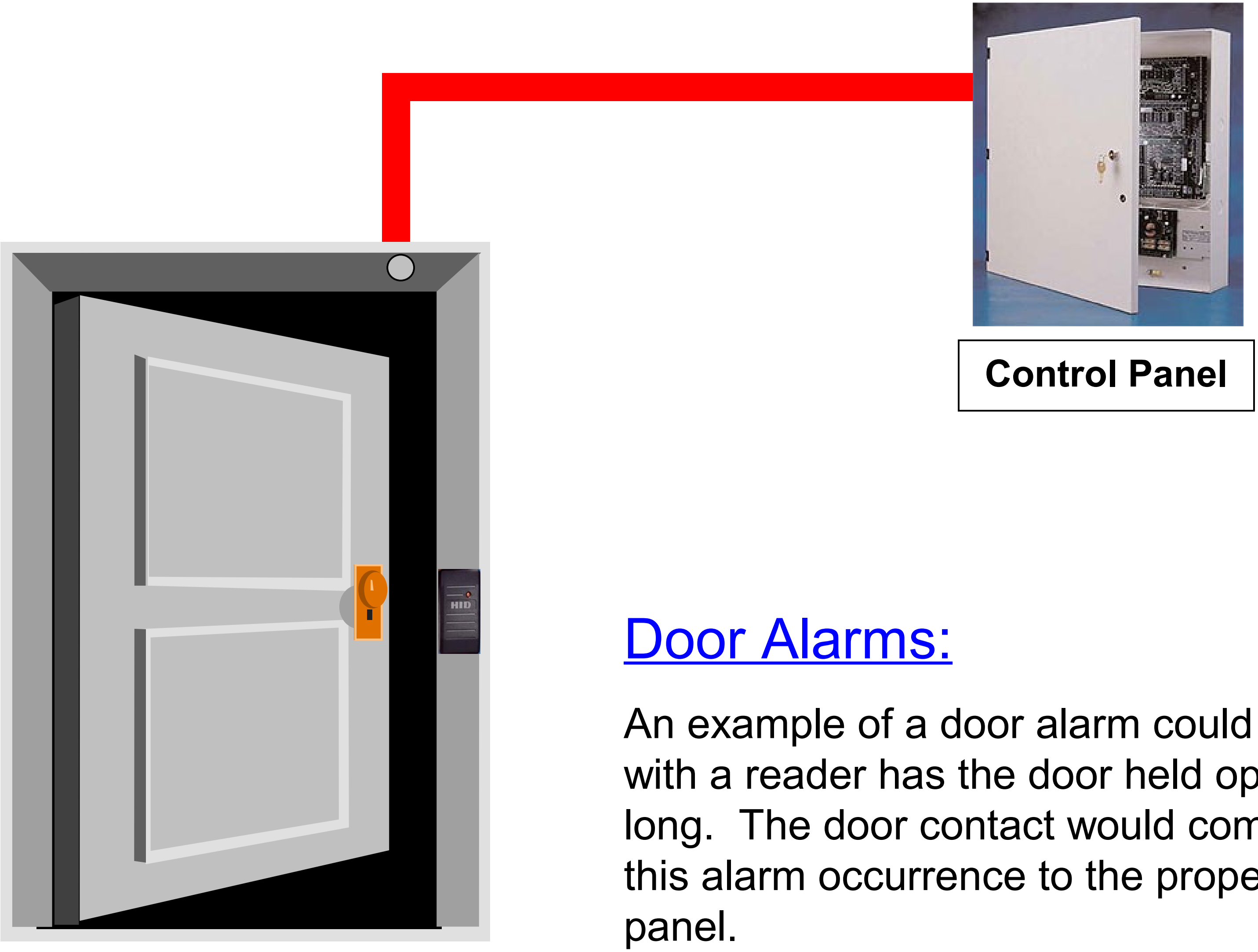


Control Panel



Card Reads:

The card reader sends the message to the control panel to verify access as stored in the local panel database.



Control Panel

Door Alarms:

An example of a door alarm could be a door with a reader has the door held open for too long. The door contact would communicate this alarm occurrence to the proper control panel.

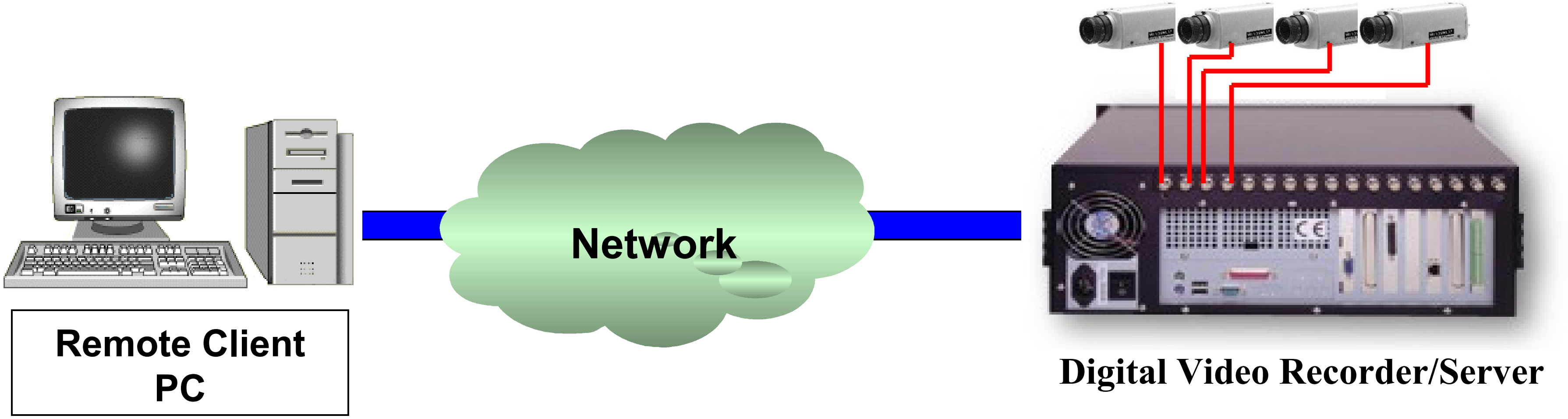
Video Surveillance

Operating Fundamentals

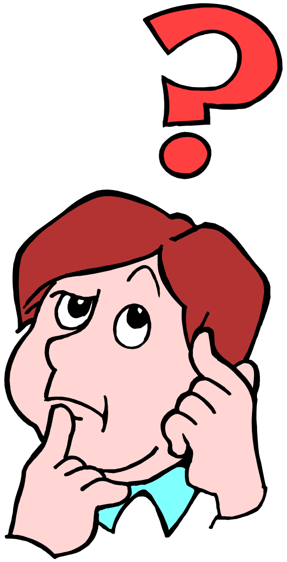
Video Surveillance

2. Video surveillance in the Physical Security arena sometimes uses a digital video recorder which is also a self contained DVR/server.

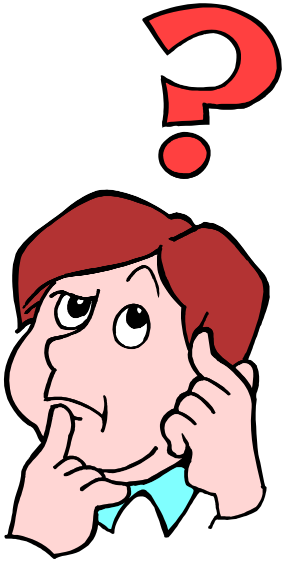
3. Software can be installed in Desk Top PCs to remotely operate and view the camera systems over networks. It also allows retrieval of incident video clips.



Questions



Are you Converging your Security Program? Why not?



References

- Booz, Allen, Hamilton, *Convergence of Enterprise Security Organizations*, Nov 8, 2005, http://www.asisonline.org/newsroom/alliance.pdf
- Kroll, Karen, *IT & Security Convergence Means That Departments Need to Cooperate*, http://www.facilitiesnet.com/bom/article.asp?id=4995
- CSO Fundamentals: ABCs of Physical and IT Security Convergence, Dec 5, 2005, http://www.csoonline.com/fundamentals/abc_convergence.html

Ron Woerner, CISSP

Ron[dot]Woerner[at]tdameritrade[dot]com

Warren Phillips