Endpoint Physical Security

A Major Loophole for Insider Threats

Presented by:

Robert M. Bauman
President/CEO
Trusted Systems, Inc.

The Problem:
Loophole Enables Insider Threat

- Cybersecurity protects from the “Inside Out”
- Physical Security stops at the wall
- Network equipment left vulnerable
- No policy covers from wall to the desktop
- Major loophole enables Insider Threats
- I give you Manning and Snowden

Insider Threat Risk

- Likelihood – explosion of access points
- Consequence – each access point exposes entire network
- Added exposure with increased database
- Insider threat risk increases exponentially
- Intelligence used against itself
- Response? Increased scrutiny, tighter CCRIs

Why the Problem?
Opposing Cultures

Information Technology	Physical Security
C4I	G3D
dynamic	static
technology driven	facility driven
speed of light	speed of a glacier
virtual	tangible
on-line	off-line
expands access	limits access

Cyber vs Physical Security

- Cybersecurity works through the network
- Physical security works around the network
- Cybersecurity is reactive – “CyberChess”
- Physical security is proactive
- Must work together to be effective

Heart of the Problem: the Human Element

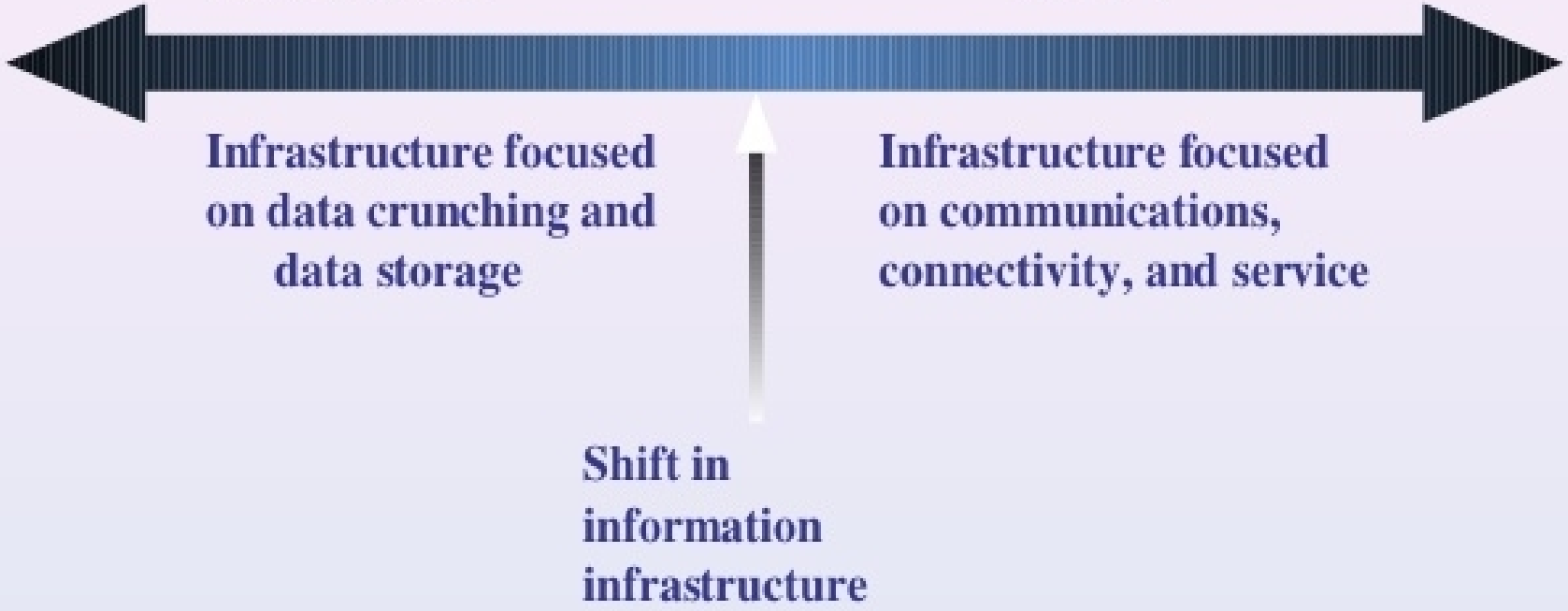
Security is always a **People Problem**

Endpoint User Interface is most vulnerable

Requires **Proactive** access control

To counter threats from the **Outside In**

The Information Age Timeline



Since 1990 – The Security World Changed

- Internet changed everything
- SCIF's became NETWORK PORTALS
- Distributed networks pushed security to endpoint
- Endpoint vulnerability grew as networks grew
- Policy unchanged, desktop the same
- Except adding VOSIP & VTC devices

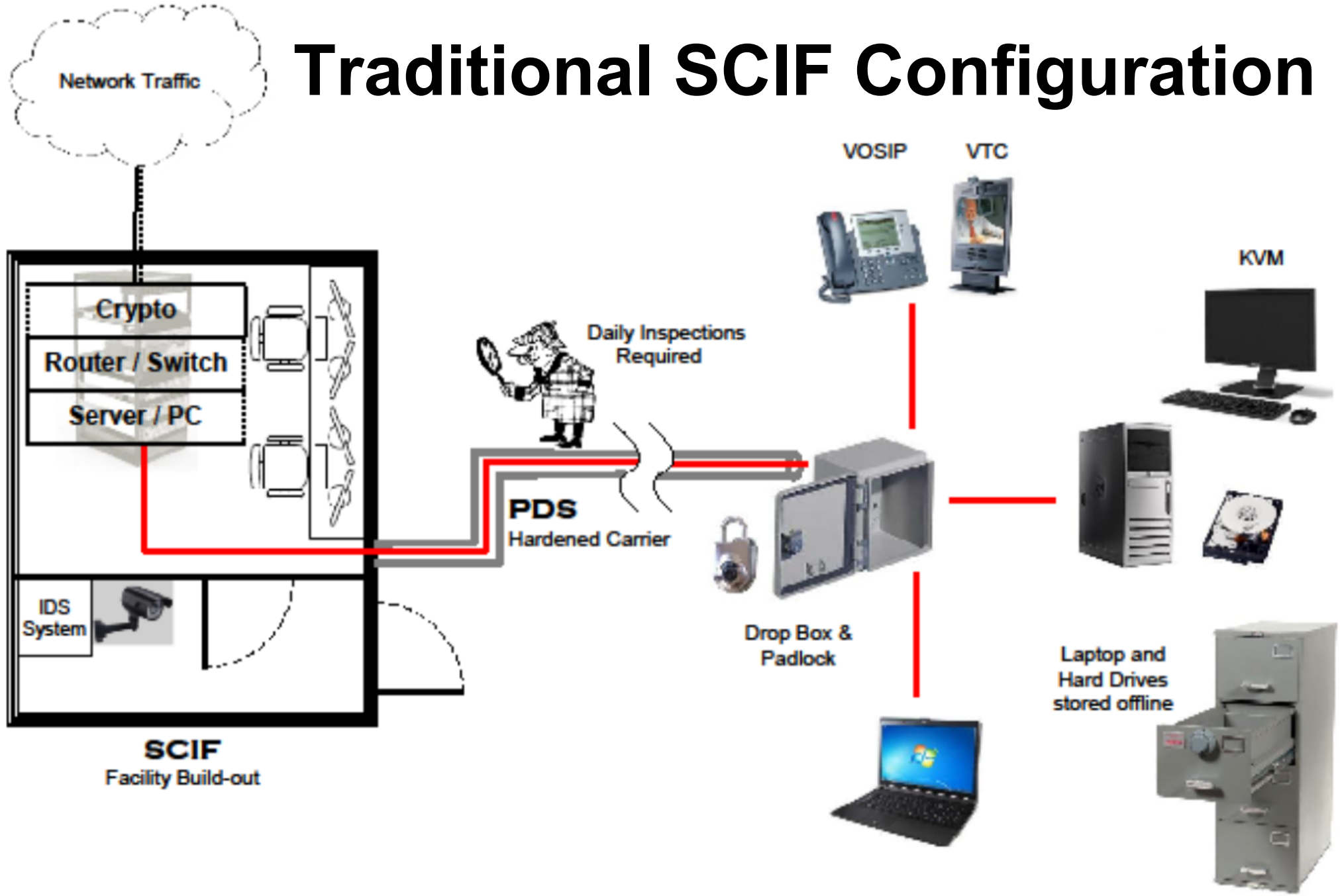
Endpoint Security Objectives

- Secure NETWORK HARDWARE, not space
- On-line operation, not off-line storage
- Tie security to network, not facility
- Seamless security to desktop, not just the wall
- Bring network to you, not you to the network

Traditional Countermeasures Fall Short

- SCIFs/CAAs/OSS – only secure space
- PDS – fixed (red) infrastructure
- GSA Storage Containers – off-line storage
- Endpoint – ignored, in disarray

Traditional SCIF Configuration



Conflicting SIPR Requirements

- Tighter CCRI criteria with DISA STIGs
- Reduce PDS reliance, inspection shortfalls
- Push encryption to the endpoint
- Restrict user access to network devices
- Growing need for instant SIPR access
- Update antiviral patches in hours, not days

Current Policy and Practices

- No policy from the wall to the desktop
  - ICD-705 covers SCIF perimeter, not the interior
  - CNSSI-7003 covers PDS ending at a drop box
  - AA-C-2786 covers the IPS Container envelope
- Policies & practices remain “stove piped”
- Local accountability for CCRI compliance
- With limited guidance, open to interpretation

Limited Endpoint Security Guidance

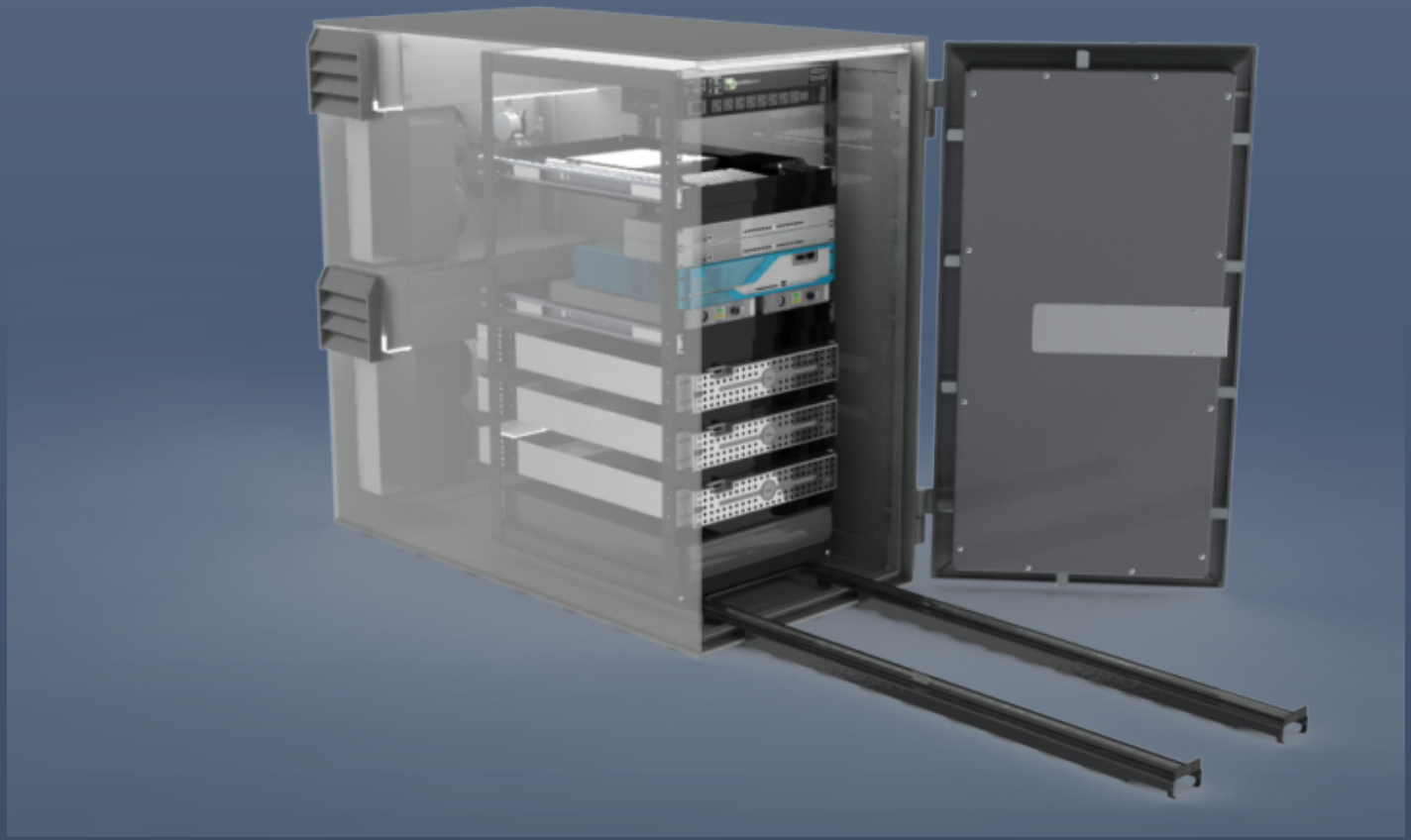
DISA STIG ID: V31132 Title: Information Assurance – Network Connections – Physical Protection of SIPRNet Network Devices:
CHECK 1 (a): IPS Containers equivalent to CAA
CHECK 2: Network Administrators and other (authorized) personnel are **only** persons with unimpeded access to the network connections

CNSSI No. 7003 – September 2015
SECTION VIII - GENERAL PDS INSTALLATION GUIDANCE
22. “terminal equipment must be safeguarded to prevent tampering” (i.e. tamper evident)

Endpoint Solution Criteria

- Functional Simplicity
- Configuration Flexibility
- Self-contained Modularity
- Built-in Reliability
- Real time Availability
- Cost effective Affordability

GSA Class 5 IPS Security Container

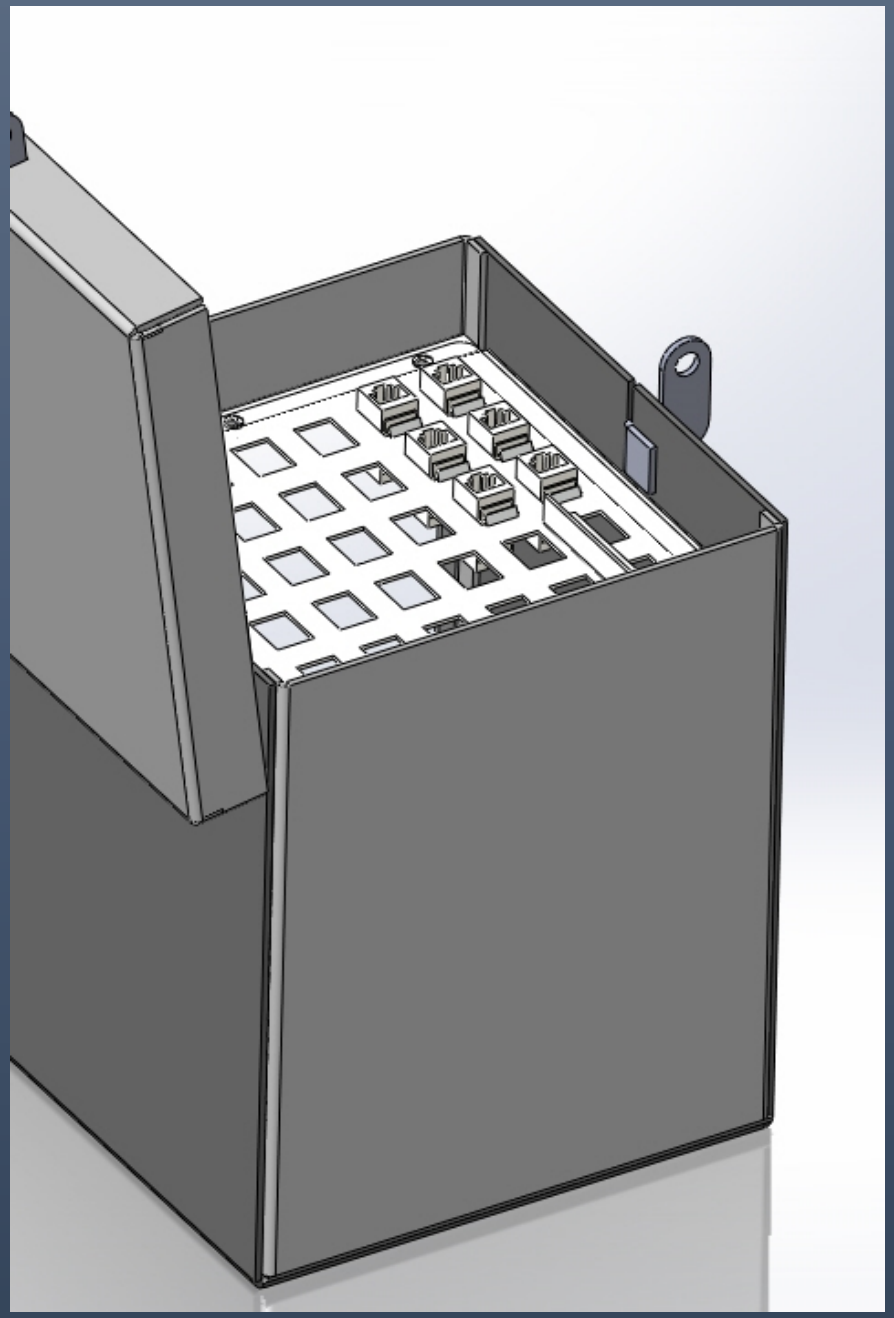


Storage Container into an Armored Computer Cabinet
Cooling, Rack Mounting, Secured Cable Portal

IPS Container Based Solutions

- Self-contained CAA
- Closed door on line operation
- Flexible sizing to suit each application
- Adaptable to legacy PDS networks
- Integrated office suite cabinetry
- TEMPEST & EMP hardening

GSA Class 5 IPS Containers



Integrated Drop Box with Patch Panel

Secured Integrated Office Suite

TEMPEST and EMP Hardened Enclosures

SCIF vs IPS Container Comparison

SCIF/CAA Buildouts

- Fixed, permanent
- Protects space
- Expensive
- Unmovable, obsolete
- Lengthy build cycles
- Attached to facility, PDS
- Manpower intensive
- Users inside

IPS Container

- Self contained
- Protects equipment
- Cost effective
- Movable, non-obsolescent
- Modular construction
- Attached to network, crypto
- Minimal human intervention
- Users outside

IPS Container By Itself Not Enough

A physical security platform

upon which you build

An integrated security solution

Requires access control enhancements:

- User interface
- Network interface

Seamless protection - User to the Cloud

Desktop User Access Control

- LOCAL controlled two factor authentication
  - Toggles desktop peripherals on and off
  - Supplements SIPR token login
  - Motion sensor cutoff if user leaves workstation
- Network devices remain on line inside safe
  - Instant SIPR access
  - Locked “air-gapped” isolation
- User has access to network, NOT equipment

UserGuard™ Desktop Access Control

"We take the leak out of Wiki"

Network Hardware Monitor & Control

- Remote IP addressable via smart PDU
- Separate from network traffic
- Monitors IPS lock/door & environment
- Alerts guards & network operators upon alarm
- Uses SNMP trap protocol & email/text
- Enables immediate remote power shutdown

Network Hardware Remote Monitor & Control System

Monitor 24/7

Door Position
Lock Status
Dial Rotation
Temperature & Power

Alarm Output

Shutdown

Email/Text

SNMP Trap

Guard Force/First Responder

Network Operations Center

Bottom Line

- IPS Containers meet CCRI criteria
- Secures network hardware, not the room
- On line unattended operation, no off line storage
- Security tied to the network, not the facility
- User network access with no hardware exposure
- Remote monitor & control of power to hardware

Conclusion

For integrated network physical security
Against insiders, outsiders and human errors
Consider using IPS Containers
With built-in access controls
In conjunction with Cybersecurity
For Seamless Network Endpoint Security
User-to-the-Cloud

Robert M. Bauman

President/CEO, Trusted Systems, Inc.

Mr. Bauman's career spans 50 years in the computer industry. He earned a BS in Mechanical Engineering from Wisconsin in 1969 and started with GE as a programmer and sales engineer in process computers, eventually specializing in telecommunications and teleprinters.

In 1973 he joined Hazeltine, a pioneer in video display terminals. After 8 years in Silicon Valley as their top salesman and regional manager, he left to start a rep and systems integration firm in Phoenix. His business expanded into distributed networks becoming a VAR for Sun Microsystems.

In 1986 while at Los Alamos National Labs, Mr. Bauman invented the "computer safe" to protect electronic devices while operating on line. He founded Trusted Systems, and in 1992 received the first GSA approval for an Information Processing System (IPS) Security Container.

Since then, continuous innovation and several patents later enabled expansion to six sizes, including a TEMPEST model, for applications from single users to data centers. To enhance the user interface, a family of secured executive workstations in furniture was created with desktop access control and continuous equipment monitoring and control.

Throughout his long career, Mr. Bauman has been intertwined with one common thread: the ENDPOINT, the Man-Machine Interface.

No matter the technology or network architecture, the endpoint user interface and its vulnerabilities remain the same. From the beginning the most critical element has been its SECURITY. It is Mr. Bauman's intimate knowledge and witness to the evolution of the computer industry and its protection that provides his unique perspective on the subject.

Contact:
Bob Bauman
Trusted Systems, Inc.
2920 Dede Road, Suite A
Finksburg, MD 21048 USA
(bob@trustedsys.com)
(703) 624-9236