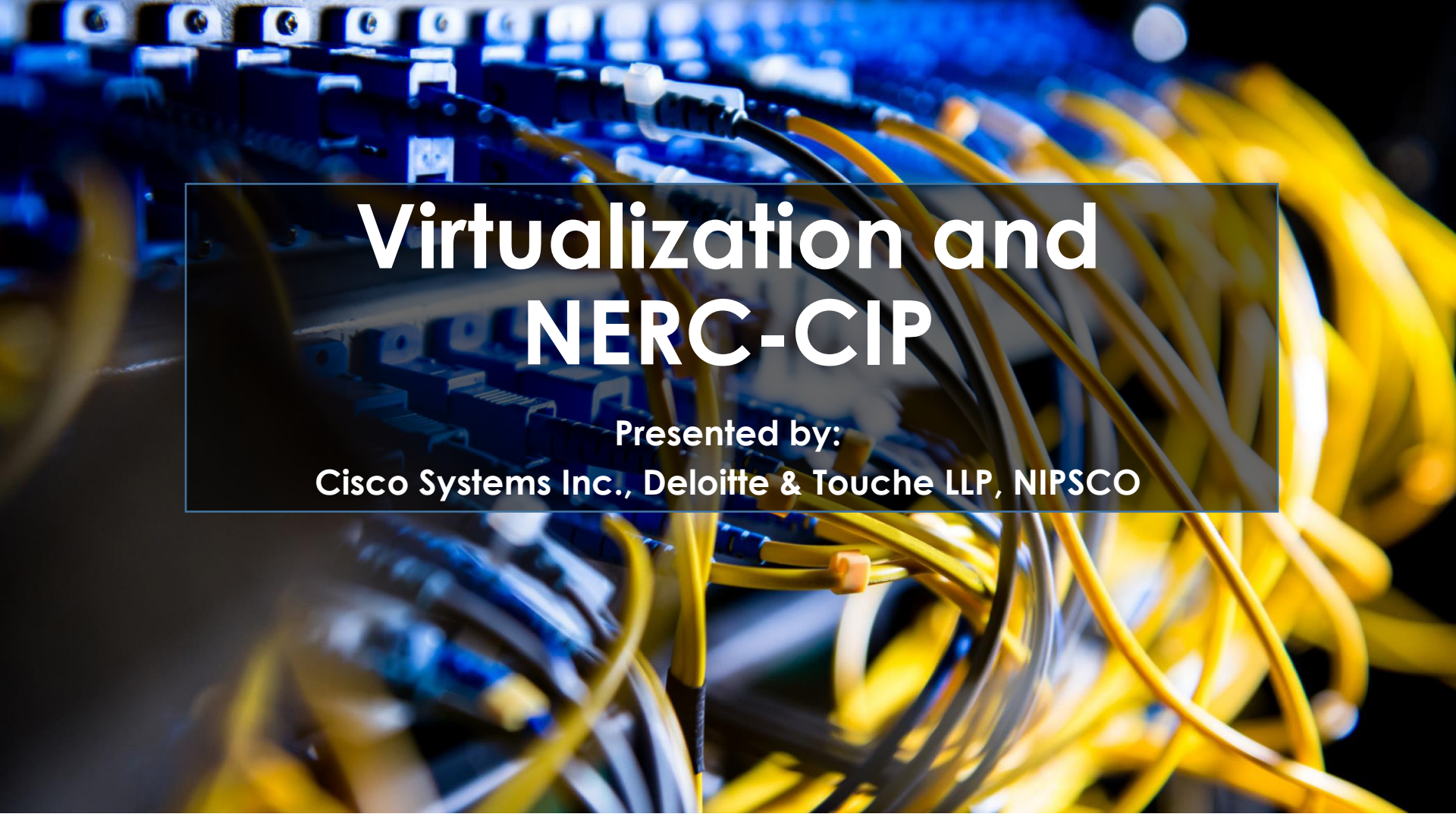


Virtualization and NERC-CIP

Presented by:

Cisco Systems Inc., Deloitte & Touche LLP, NIPSCO

UTC is a **global trade association** dedicated to **serving critical infrastructure providers**, such as electric, gas and water utilities. Through **advocacy, education and collaboration**, UTC **creates a favorable business, regulatory and technology environment** for our members who own or operate Information and Communication Technology (ICT) systems in support of their core business.

Virtualization and NERC-CIP

Agenda

- Introduction - UTC
- Value of Virtualization – Cisco
- Virtualization and NERC-CIP – Deloitte
- Virtualization Applied – NIPSCO
- Q&A - Panel

Session Participants

Moderator

Bob Lockhart
VP, Cybersecurity, Technology, and Research
UTC

Panelists

Tom Alrich
Manager Cyber Risk Services
Deloitte & Touche, LLP

Joe Andrews
Manager Cyber Risk Services
Deloitte & Touche, LLP

John Reno
IoT Product and Solutions Marketing
Cisco Systems, Inc.

Steven Sumichrast
Lead System Engineer
NIPSCO

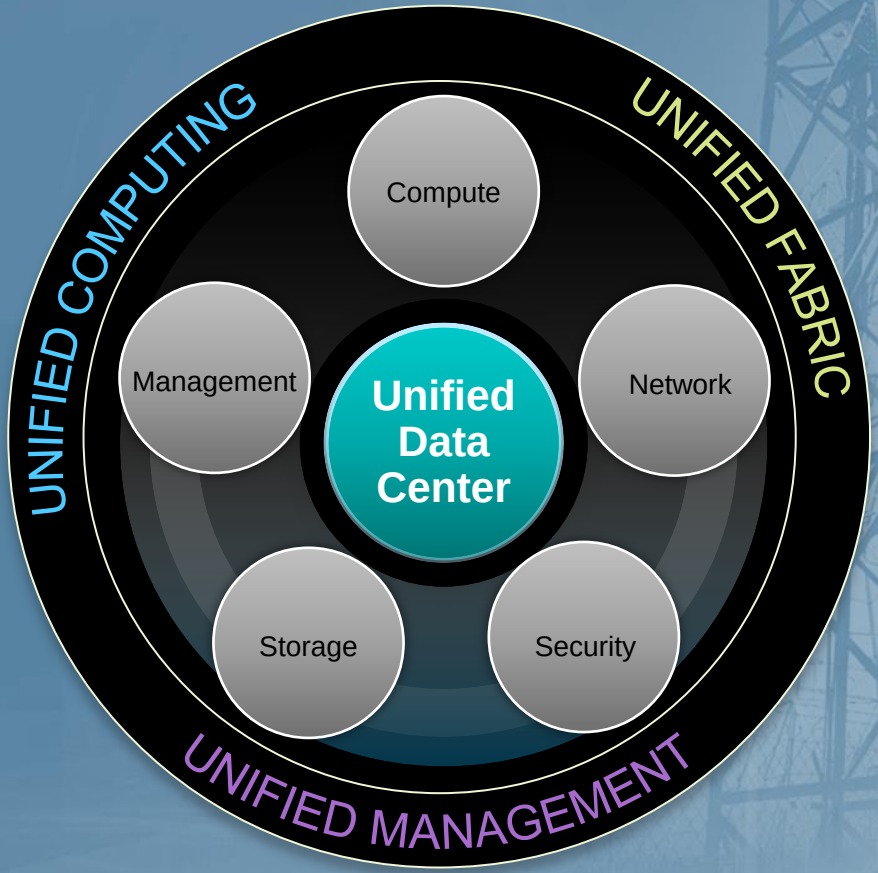
The Value of Virtualization

Virtualization Scope

Physical

Virtual

Cloud

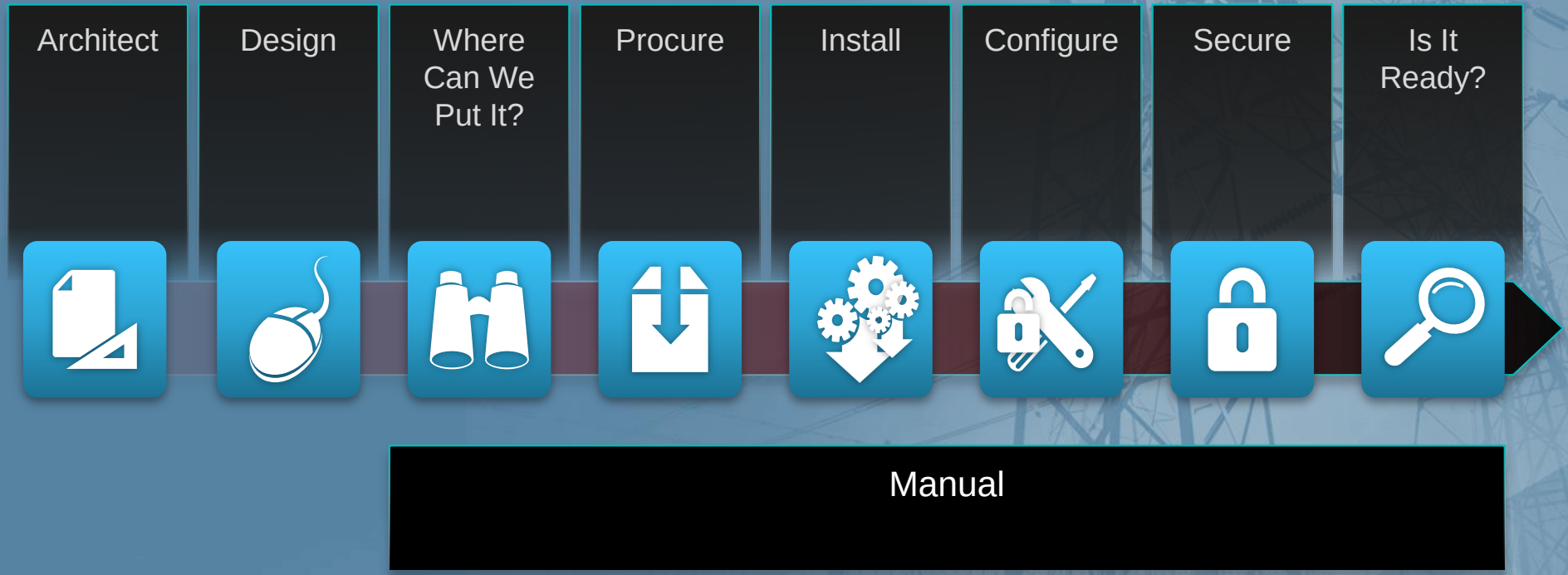


Agility

Efficiency

Simplicity

Cisco Experience – Status Quo



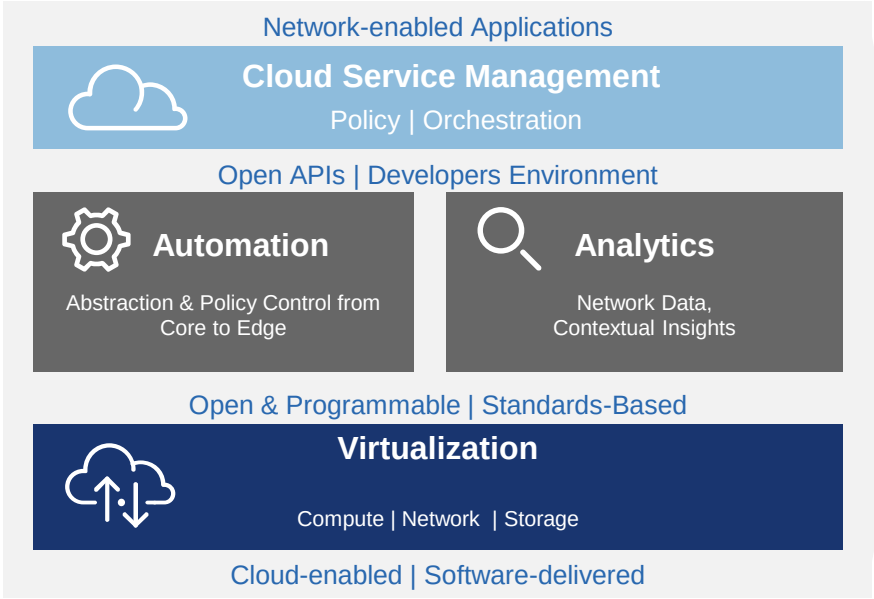
Design to Production Now: From Weeks To Minutes

Capacity On-Demand

Policy-Based Provisioning

Built-In Governance

Cisco Digital Network Architecture



Utility Customer Example

Operational Efficiency

Challenge

- Lower cost in operations and infrastructure, especially for remote locations
- Slow and expensive service rollout that requires service calls

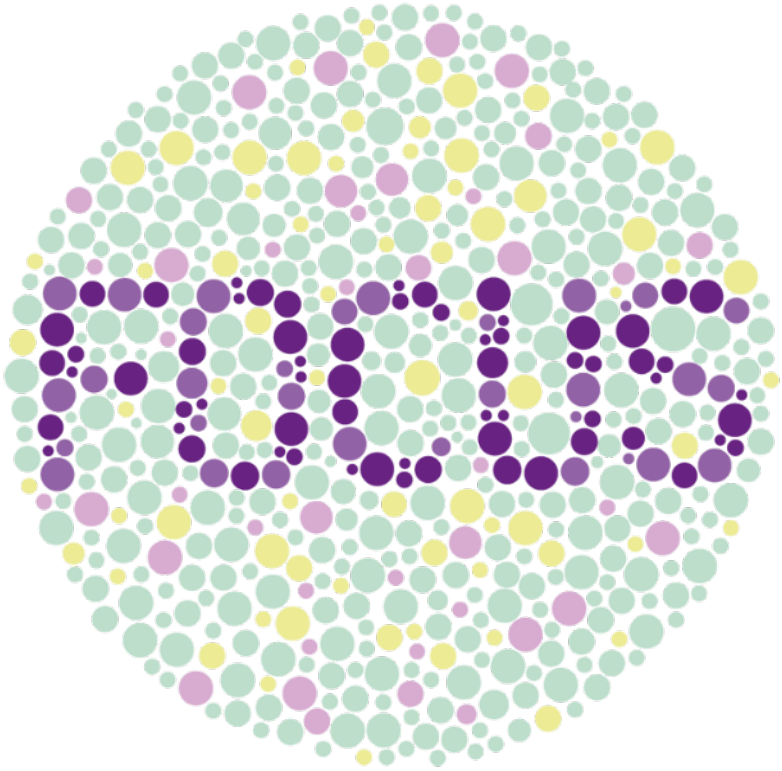
Solution

- One standard platform for all locations
- Services: Routing, Firewall, Wireless LAN Controller, WAN Optimization

Benefits

- Lower cost by utilizing x86 servers with Cisco® NFVIS
- Keep current operational standards with best-of-breed services
- Agile service deployment and monitoring with Cisco ESA

Deloitte.



Virtualization and NERC CIP

Tom Alrich and Joe Andrews
Deloitte & Touche LLP

Introduction

Virtualization provides a lot of benefits….

But CIP is silent on it. Is it allowed? Not allowed?

Can you do it at all?

If you can, can you also remain compliant?

Many NERC entities have decided not to virtualize….

But some have gone ahead anyway…..

A fundamental problem

Cyber Assets are “Programmable electronic *devices*”! VMs aren’t devices.

Can you virtualize without worrying about CIP? No….

So do you treat all VMs as BES Cyber Systems? Leads to other problems….

Then maybe we should forget about virtualization!

This solves the CIP problem, but…

What is a solution?

A solution is to rewrite CIP!

The SDT is on the case, but…

Meanwhile, back at the ranch….

How is the NERC ERO approaching virtualization? Here's…Joe!

NERC ERO initial concerns & discussions

- **Mixed trust environments**
  - Managing VM Cyber Assets (disparate trust levels)
  - Mixed trust authentication

- **For layered virtual architectures**
  - Applicable Standards (i.e., CIP-002, 005, 007, 010, & CIP-011)
  - Enforcement of logging?
  - Enforcement of monitoring?
  - Enforcement of access controls?
  - Baseline snapshots (previous state VM instances)

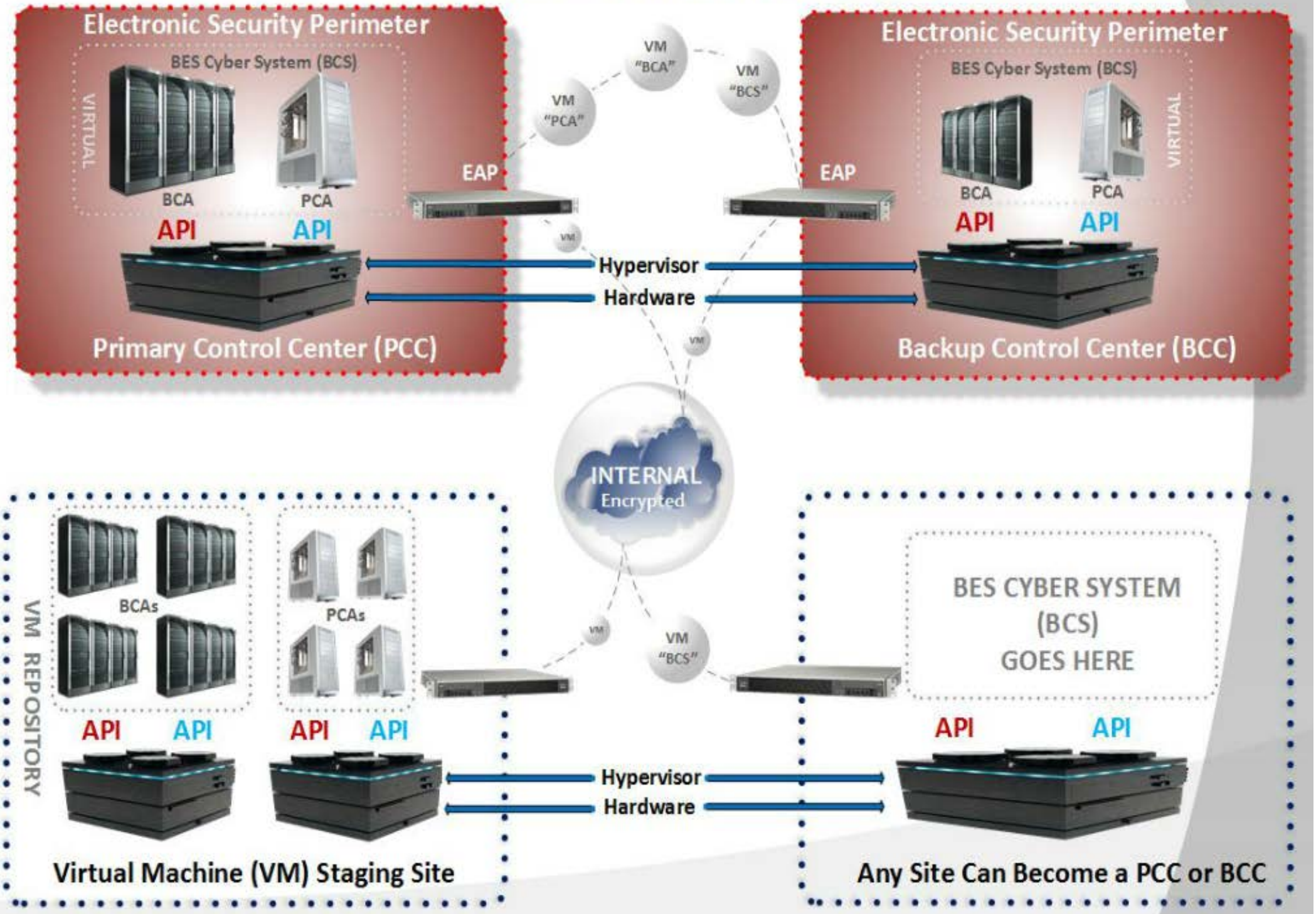
Audit approach regarding virtualization

- **Virtualization is allowed (*with important caveats!*)**
  - No mixed-trust environments
    - Medium & High BES Cyber Assets cannot coexist
  - High watermark concept enforced
    - Lowest impact rated Cyber Asset inherits highest rating
  - Host (hypervisor) and VM Cyber Assets protection
  - All VMs, including Host (hypervisor) should be inventoried

Successful virtualization adoption recommendations

- **Don’t be deterred**
- **ERO actually supports innovation**
- **Work closely with virtualization vendor support**
  - Communicate compliance concerns and requirements
  - Ensure your compliance staff are involved
  - Incorporate best practice virtualization security controls
- **Inform the ERO ahead of time**

POTENTIAL VIRTUALIZATION BENEFITS (CONCEPTUALLY)



Contact Us

Steve Livingston

Principal, Cyber Risk Services

Deloitte & Touche LLP

+1 206 716 7539

slivingston@deloitte.com

Tom Alrich

Manager, Cyber Risk Services

Deloitte & Touche LLP

+1 312 515 8996

talrich@deloitte.com

Joe Andrews

Manager, Cyber Risk Services

Deloitte & Touche LLP

+1 248 231 5926

joeandrews@deloitte.com

Deloitte.


NIPSCO

Planning, Planning, Planning

- Virtualization team may not be same team operating BU applications.
- Work with BU to understand the applications.
- Design requirements for CIP clusters may not fit the normal virtualization mold.
  - Primary driving factor is operational and security benefits.
  - Consolidation great; not the primary driver, though.
- Consider operational cost efficiencies.
  - Backup, Change Control, security controls for CIP-005/CIP-007.

Know Your Environment

- Baseline the performance of the environments.
- Baseline the configuration of the environments.
- Diagrams are key for discussion points.
  - Single line diagrams for logical network topologies.
  - Component diagrams for physical topologies.
- Involve Network & Security teams.
  - They need to know what to expect from hypervisor traffic (storage, virtual machine migrations, etc).

NIPSCO

Consider everything

- Management consoles must be at least considered for CIP-002 inclusion.
  - Often provide interactive remote access that cannot be restricted by IP Address sources.
  - Two factor considerations for management consoles listed as EACMS w/ Interactive Remote Access.
- Follow vendor best practices.
  - Individualized Access.
  - Log *Everything* centrally.
  - Use Hardware monitoring to control unauthorized changes (TPMs).

Secure it!

- Follow vendor best practices.
  - Isolate all hypervisor management ports. VM escape technologies all rely on exploitation of hypervisor.
  - Minimize keys to the kingdom – Only let key personnel have access to hypervisors. Least privilege is key, not only for CIP but for your security sanity! Not everyone needs access to the Hypervisor.
  - Use Layer 2 VLANs to protect networks for the infrastructure; don't be tempted to add that SVI – keep the networks islanded within your ESP infrastructure.
  - Use automation tools to help with CIP-010.
    - Scripted tasks to snapshot; increase or decrease capacity; block changes to network or hosts settings.

Test it!

- SCADA applications are old; they do not always get along with the new kid on the block.
- Make sure technologies in use do not cause operational issues.
  - Live migrations (e.g. VMware vMotion) often introduce VM “stun” operations.
  - Stuns may cause clocks to jump forward.
- Be mean to the environment.
  - Pull cables; Introduce disk latency; introduce network latency; do things you’d never do in production.
  - Know what’s going to happen before it hits production floor.

NIPSCO

Defend it!

- Be prepared for ERO to ask for evidence showing where the VMs live.
  - Strongly advise mapping VMs to Clusters, and Clusters to Hosts.
  - Develop scripts that generate audit-ready evidence for the audit team to prove your High Impact VMs are stuck on High Impact hypervisors.
- Use vendor-provided tools to check the configuration of hosts frequently.
- Log everything – including the management console events.
- Know your virtualization technology inside and out.
  - Knowing your version numbers or where configuration is in the GUI is great; know how that vendor is controlling module loading, what traffic to expect, how does that live migration technology actually work.
  - Confidence portrayed in knowing not only your system but the technology is incredibly important.

Questions?