The New Resilience in Industrial Cybersecurity

CCI: XVI International Congress of experiences in Industrial Cybersecurity – September 30 2021

INTRODUCTION

- Centro de Ciberseguridad Industrial (CCI) US Coordinator
- Former utility staff (telecommunications, water & electric)
- First NERC CIP auditor in the US
- Drafter of NERC CIP standards and formal interpretations
- NERC CIP Supply Chain Working Group contributor
- Former Principal Investigator US DOE National Electric Sector Cybersecurity Organization
- EnergySec Founder, Director and President Emeritus
- Cybersecurity Advisory Team for State Solar, NARUC/NASEO
- Advisor to multiple industrial security product vendors
- GCIP, CISA, CRISC, CISSP-ISSAP, SSCP, NSA-IAM, CVI, TCP, SCP


THE OLD WAY

RESILIENCE WITH LIMITATIONS

- Something breaks – fix it
- Incidents (accidental or malicious) limited to one or a small number of systems
- Incident response and disaster recovery
  - Rarely tested
  - Few documented IR/DR plans
  - Limited root cause analysis
  - Few documented lessons learned
- Often requires highly specialized knowledge
  - Unique mix of systems and applications
  - Specific to plant/location
  - Historical knowledge of system environment
  - Sequence matters

REACTIVE AND SPECIALIZED

- Little if any situational awareness
  - Unable to see problem happening in early stages
  - Unable to stop problem from becoming worse
- Little if any environment telemetry
  - Unable to see impacts on environment
  - Unable to infer issues based on other system behavior
- Critical systems and applications difficult to restore
  - Legacy hardware and software
  - Undocumented configurations
  - May or may not have backups, build documents
  - Licensing issues and end-of-life platforms

ASSET INVENTORY

- Not everything, but at least the critical systems
- You must know what you have to protect it
- All other key control areas are based on this
- Start with simple baseline elements
  - Make/model
  - Network and/or or host address
  - OS and/or firmware
  - All other software installed
  - Listening Ports (services)
  - Patches (or patch state; vulnerability)
  - Latest configuration(s)

PHASE OUT FRAGILE SYSTEMS

- Legacy systems
- Custom systems
- Unique systems
- That one application written by 3 engineers
- Brittle and unreliable hardware
- Borrowed IT used as OT
- Applications that don’t work well with other tech
- Applications that are the hardest to update
- Standardization will lower costs/risk and improve uptime

ARCHITECT FOR DEFENSE

- MINIMUM - a firewall between IT/OT with strict rules
- Specific points for detection and visibility
  - Network boundary
  - Each network segment
  - Critical systems
  - Administrative & engineering systems
- Dependencies on outside systems
- Dependencies on outside business processes
- Intelligent islanding, shear-away networks & “turtle mode”

CONTROL CHANGE

- Best defense against both accidents and malice…
- Establish a change control/review board – at least for the critical systems
- Prepare for backing out any change
- Record all changes through baseline tracking
- Include changes into build/restore documentation
- Test changes, whenever/wherever possible

LOGGING AND MONITORING

- Log and monitor as much as you possibly can
- Network monitoring
- System monitoring
- SIEM tools
  - Tuning
  - Monitoring and alerts
  - False positives
  - Integration with other tools
- OT-specific tools exist
- Integrate with enterprise for the full picture
  - Most attacks start on the IT side of the organization

KEEP IT SIMPLE

- Don’t over-buy security technologies
- Train your staff
- Complexity is the enemy of security
- Reduce technology diversity
  - Standardize tech blueprint (software and hardware)
  - Standardize configurations; control “drift”
- Fewer places for attackers (or problems) to hide
- Reduces attack surface area
- Less expensive through volume purchase
- Easier on supply chain risk

RESPONSE AND RECOVERY

- Write down an Incident Response Plan (IRP)
- Keep it simple – something you can follow
- Practice, practice, practice then practice more
- Are you sure you can recover – even from destructive malware? Have you tried to do this?
- Is your supply chain ready?
- Which processes can go to “manual?”
- Can you continue operating through the attack?

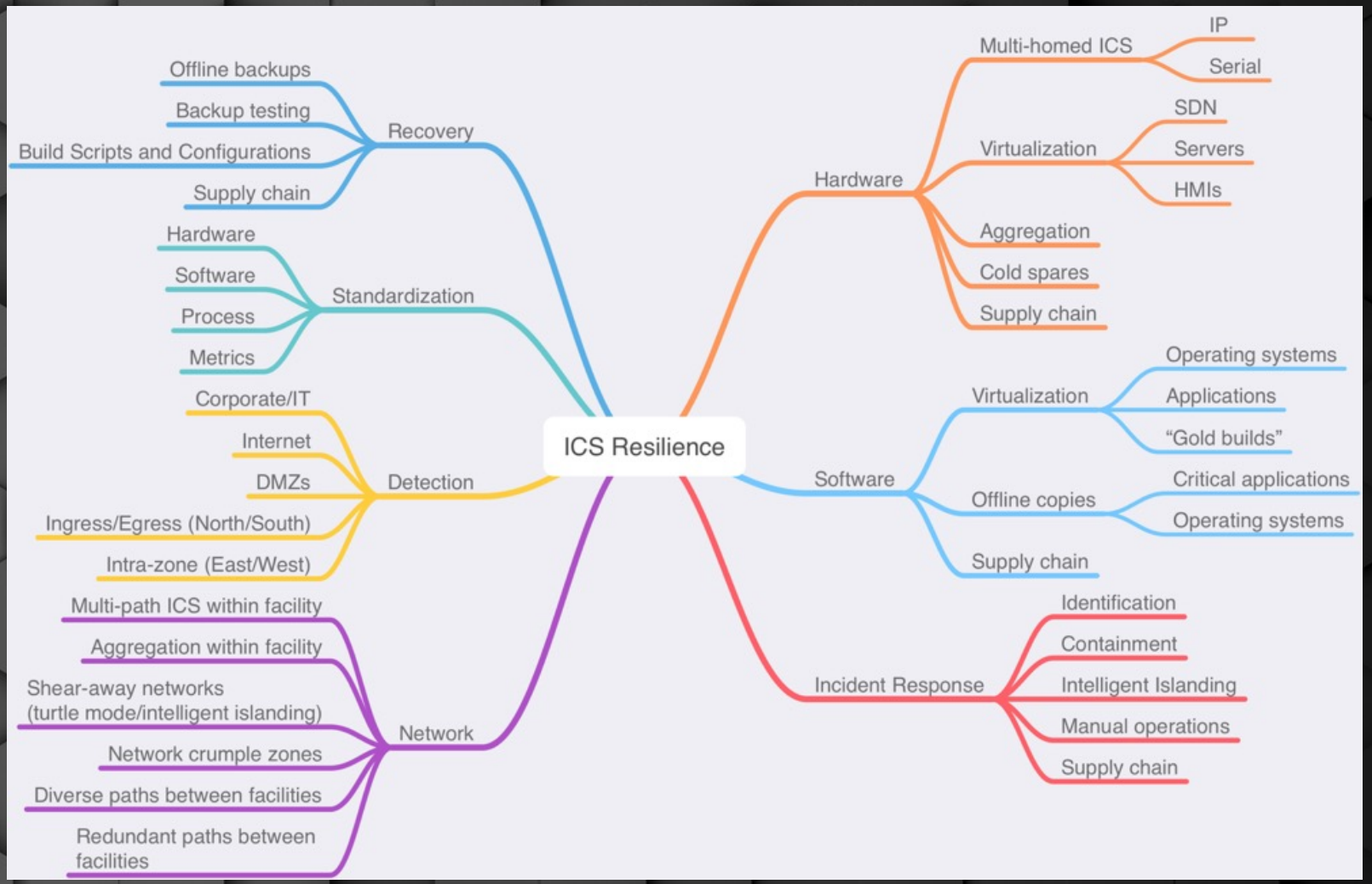
FRAMEWORKS AND METRICS

- Where do you start? Is there a playbook?
- Pick one, apply it, and measure to it
- Start with a gap assessment (good, but not required)
- IEC 62443; NIST-800-53 and 800-82
  - Map to other standards as needed
  - ”High water mark” for multi-standard environments
  - Understand one-way “mapping” limitations
- KEY: consistent measurement to demonstrate progress


THE NEW WAY

THE NEW OT RESILIENCE

- Know what you have and how to protect it
- Modernize, standardize and simplify
- Build a network you can see and defend
- Change control and configuration management
- Monitor as much as possible
- Practice response and recovery like it's "game day"
  - Prepare for catastrophic scale events
- Anticipate and predict the problem before it happens
- Training and tools for staff to succeed
- Be able to continue operating through the attack
- CCI methodologies – RECIN and ESCIM


ICS Resilience
Recovery
Offline backups
Backup testing
Build Scripts and Configurations
Supply chain
Standardization
Hardware
Software
Process
Metrics
Detection
Corporate/IT
Internet
DMZs
Ingress/Egress (North/South)
Intra-zone (East/West)
Network
Multi-path ICS within facility
Aggregation within facility
Shear-away networks
(turtle mode/intelligent islanding)
Network crumple zones
Diverse paths between facilities
Redundant paths between
facilities
Hardware
Multi-homed ICS
IP
Serial
Virtualization
SDN
Servers
HMIs
Aggregation
Cold spares
Supply chain
Software
Virtualization
Operating systems
Applications
"Gold builds"
Offline copies
Critical applications
Operating systems
Supply chain
Incident Response
Identification
Containment
Intelligent Islanding
Manual operations
Supply chain

CONTACT ME


@PATRICKCMILLER


LINKEDIN.COM/IN/MILLERPATRICKC


PMILLER@AMPERESEC.COM


WWW.AMPERESEC.COM


+15032721414