מערכות בקרה מתקדמות –
הגנת סייבר בסביבה תפעולית

Gabriel Mazooz
Israel Electric Corporation

Gabriel Mazooz (please call me Gabi)

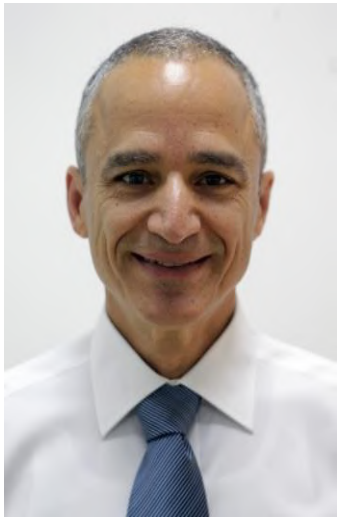
Title: Head of the Cyber Management Unit at IEC,
(Israel Electric Company)

Israel Electric - 28 years

- The last 15 years, I have been devoted to critical infrastructure cyber defense as the Computer & Cyber Department Manager.
- Engineering Planning, 6 years
- Generation & Energy Group, 21 years
- Computer Group – Cyber Headquarter

Academic Education:

- Bsc. & Msc. - Mechanical Engineering
- MBA - Haifa University
- Bsc. - Electrical Engineering



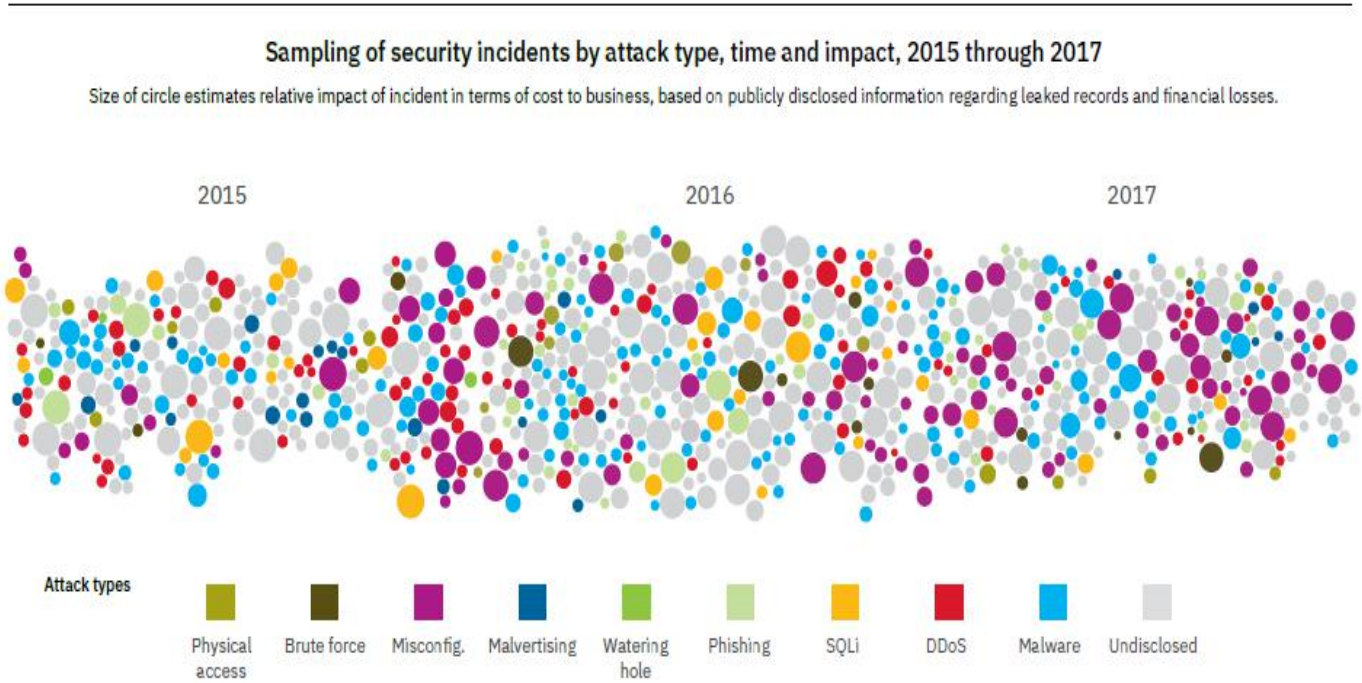
Global Cyber Attack (Reality or Fiction)

Do you think that a global cyber attack is a reality or is it fiction ?

IBM X-Force Threat Intelligence Index 2018

Incidents of Attacks by type

- More than 75% of attacks use vulnerabilities created by misconfiguration and poor integration of the system and cyber defense tools.
- IEC has developed deep expertise in the architecture of the domain, and of its cyber protection shield, to fill in the integration and configuration gaps.



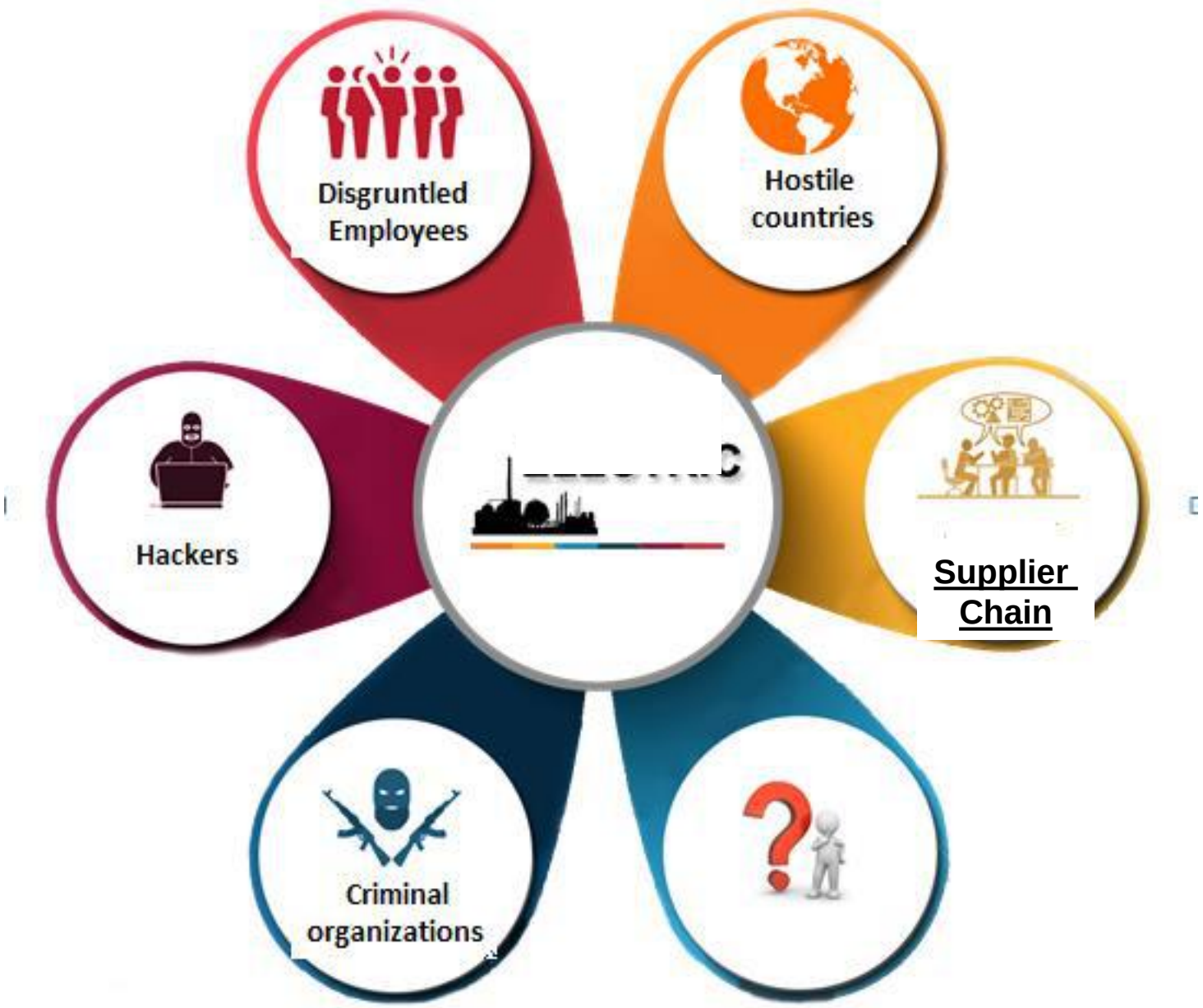
Cover Image: Sampling of security incidents by attack type, time and impact, 2015 through 2017.

The Human Factor in Cyber Security

Human Factor - Chain of Cyber Defence

You become the major vulnerability

Threat Actors



- Subway fare gates, were locked in an open position, and could not be electronically closed, during all day on Saturday

Payment Screens

Control Room Print Screen

"you are hacked.
All information is encrypted.
Make contact to get the release code"

Management Dilemma

- We are here a group of managers
- We are facing a management decision.
- On the one hand – any minute our business is losing a lot of money, and may be brought to collapse.
- On the other hand - we pay the ransom, save our company, but we support the cyber-terror

In situation like this how would you act ?

Cyber Protection Concept – Main Challenges

1. To create fully secured environments against attack vectors
2. Minimum disruption to operations
3. Minimum costs

Cyber Protection Concept – Multi-Layered Approach

The best defense against targeted attacks is a multi-layered approach, combining:

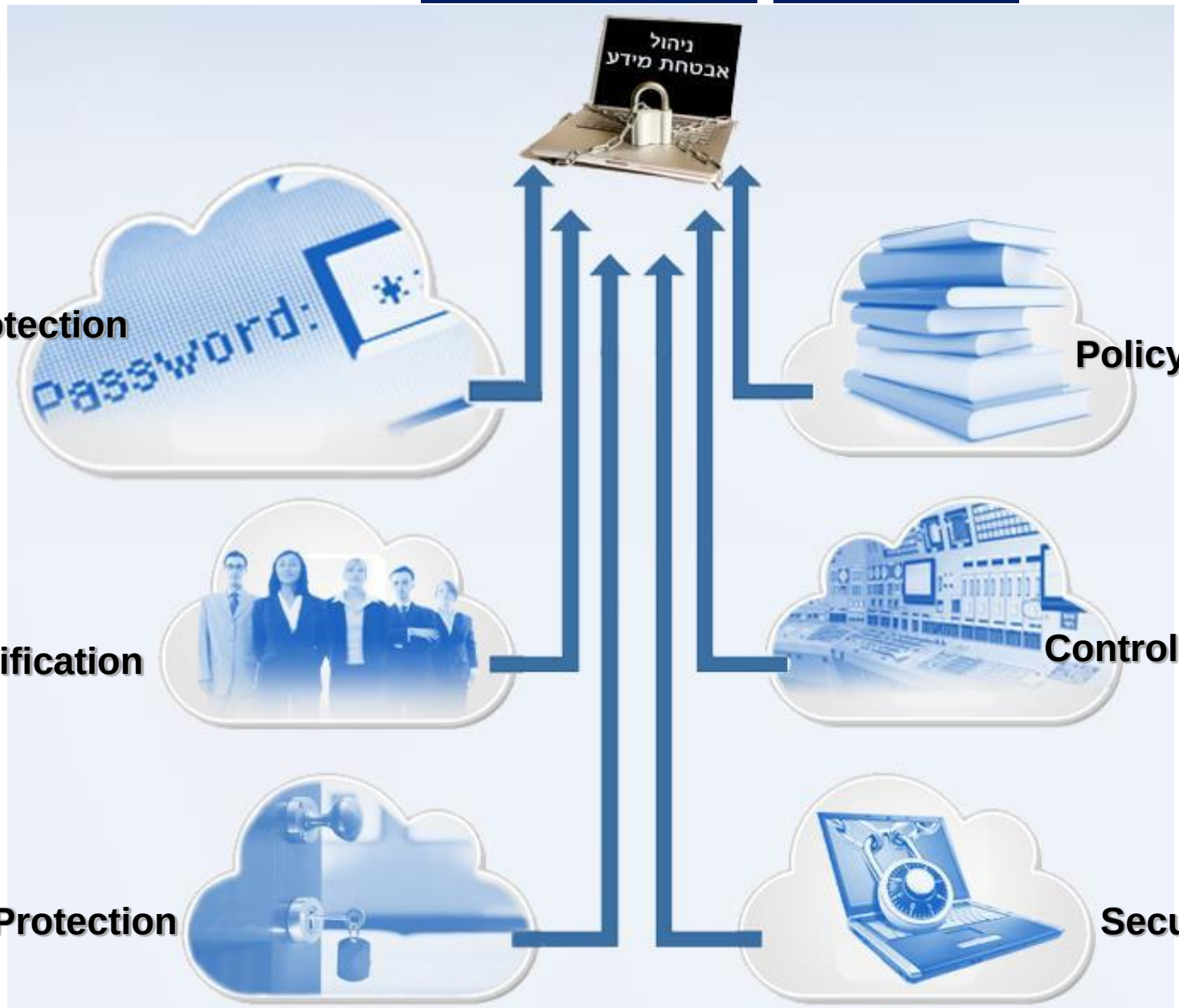
1. **Traditional - build a "wall" that hackers can't penetrate: FW, anti-virus, patch management, intrusion detection, whitelisting strategy, etc.**
2. **Proactive – don't wait for an attack, go out and find it outside your organization.**
3. **Holistic Management**

Cyber Protection Concept – The Traditional Layered

1. **Total Monitoring and Control of:**
   - **Critical systems, Ancillary, Auxiliary**
   - **Users-administrative and operational systems……**
2. **Analysis of all suspicious attempts**
3. **Procedures and Contingency Plans for Routine and Emergency Situations**
4. **Recruitment and Qualifications of skilled teams**
5. **Research and Renovation**

Cybersecurity must now be part of doing business

Cyber Protection Concept – The Traditional Layered



Logical protection

Policy & Procedure

Classification

Control & Supervision

Physical Protection

Security Incidents

Integration of these components via SOC

Security Operations Center (SOC)

- Our innovative model of cyber-security protection services, is operated from a sophisticated Security Operating Center (SOC).

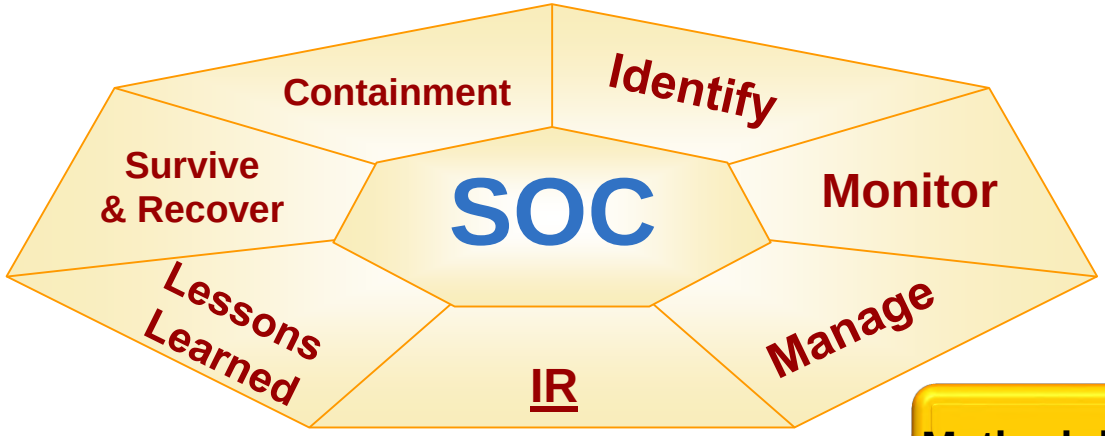
- It is manned by security experts, analysts and architects 24/7, ready to respond to any threat.

- The SOC utilizes advanced tools to detect cyber-attacks, including alert mechanisms, detection tools and comprehensive reports, providing the team of security experts an up-to-date status and allowing rapid response to threats.

Cyber Protection Concept – The Proactive Layered

1. Looking at Web resources/reports for indicators of suspicious/malicious attacks
2. Gathering Threat Intelligence from Social media and “hacktivism” campaigns
3. Utilizing the Common Vulnerabilities and Exposures (CVE)

Multi-Layered Approach - Holistic Management



Hardware

Servers:

Whitening
Anti-Virus
Admin

Software

Whitelist
Antivirus

Security Tools

One-way
SIEM
FireWall
IPS

Cyber Package

ABB
Siemens
Metso
Emerson
GE

Methodology

Policy
Procedures
Operational orders
Drills
PT

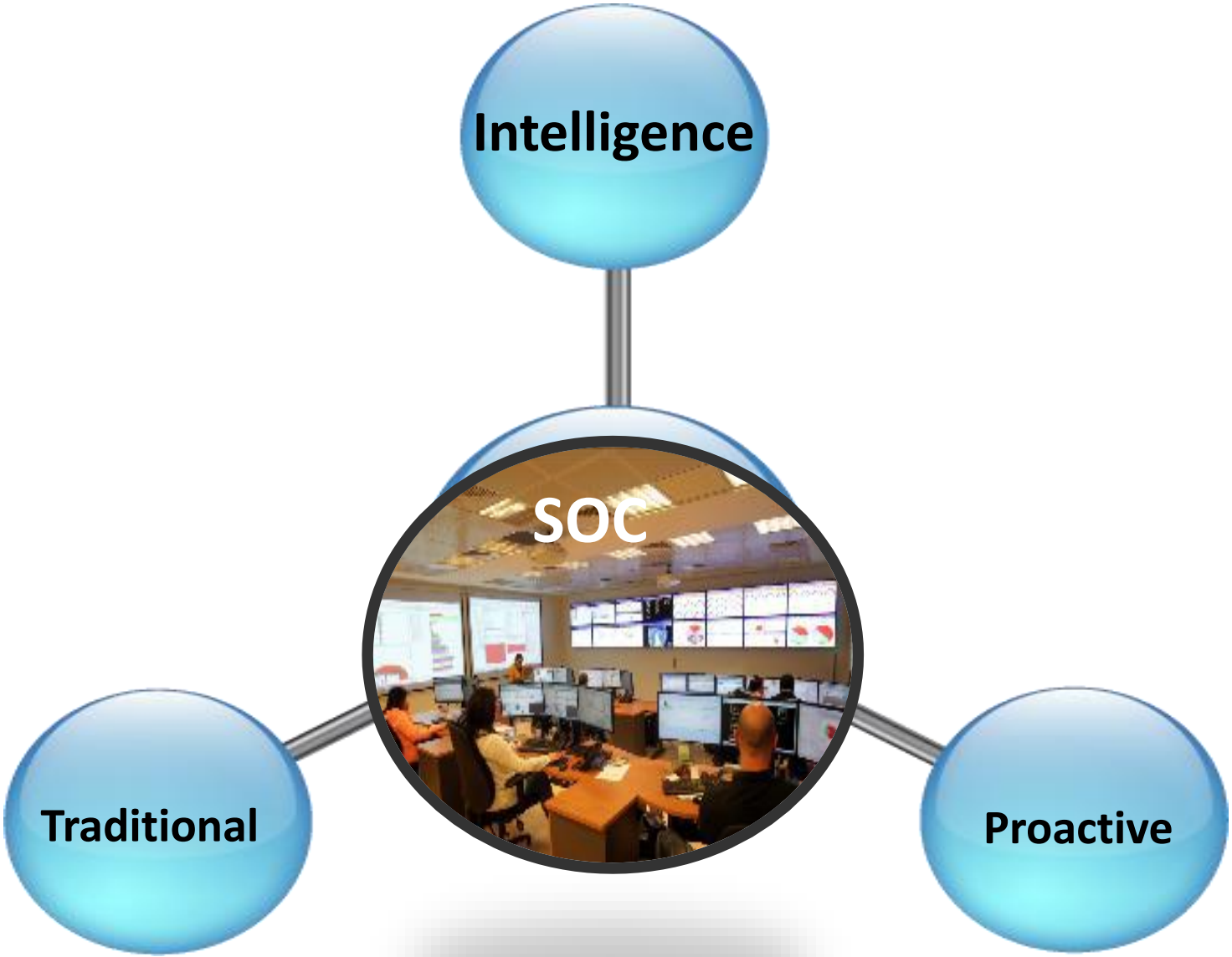
Human Resources

Organization
Training
Assignment
IR

Cyber Referent / Administrator

1. Responsible for Cyber - one at each IEC site
2. Operates and maintains on-site Cyber tools
3. Develops local controls and scripts
4. Local Point of Contact for all Cyber related issues
5. Reports to and participates in organization forum

Multi-Layered Approach - Holistic Management



Cyber Security Concept for

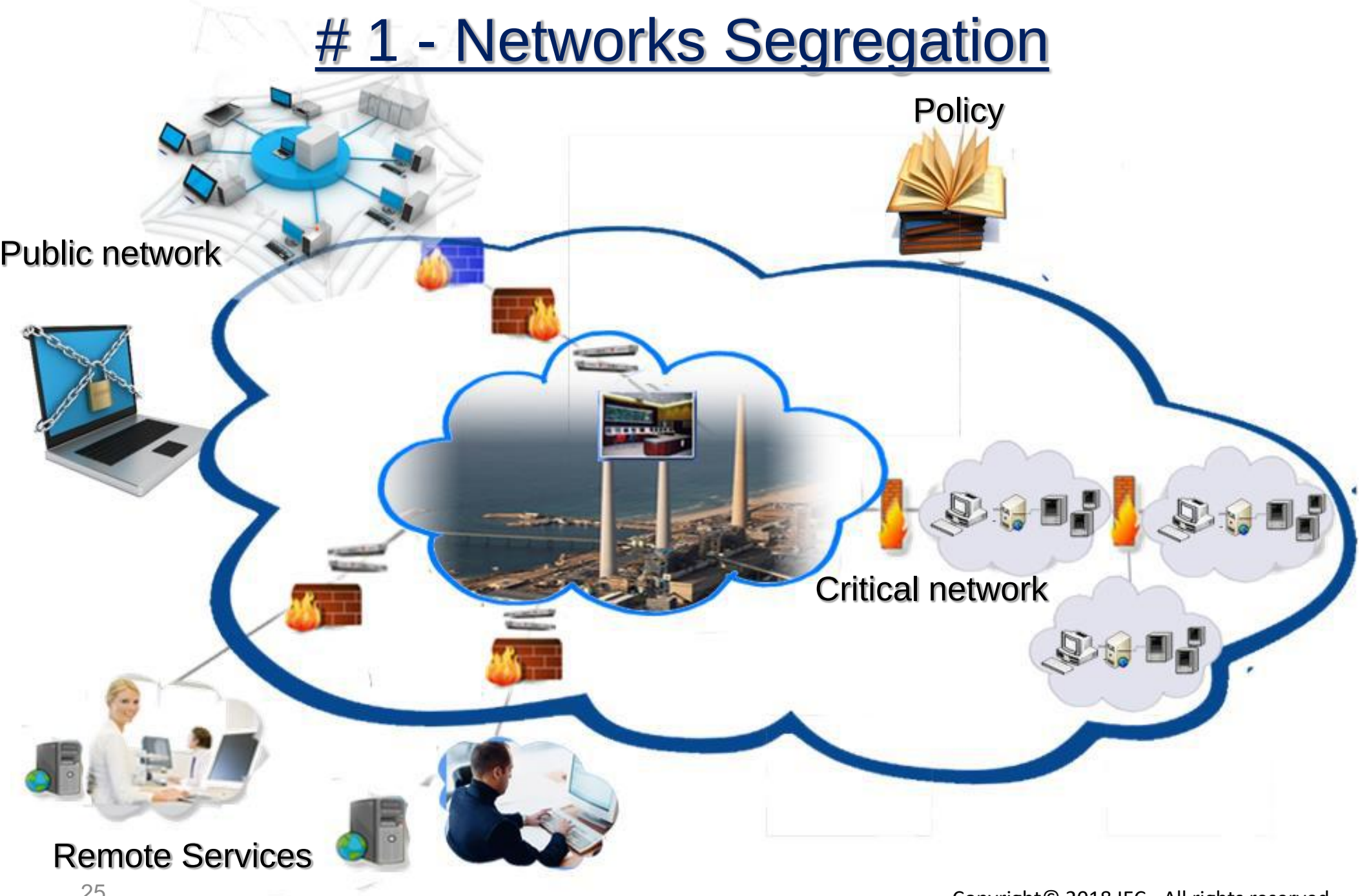
National Electrical Infrastructure Systems

Top 10 - Cyber Recommendations

Review

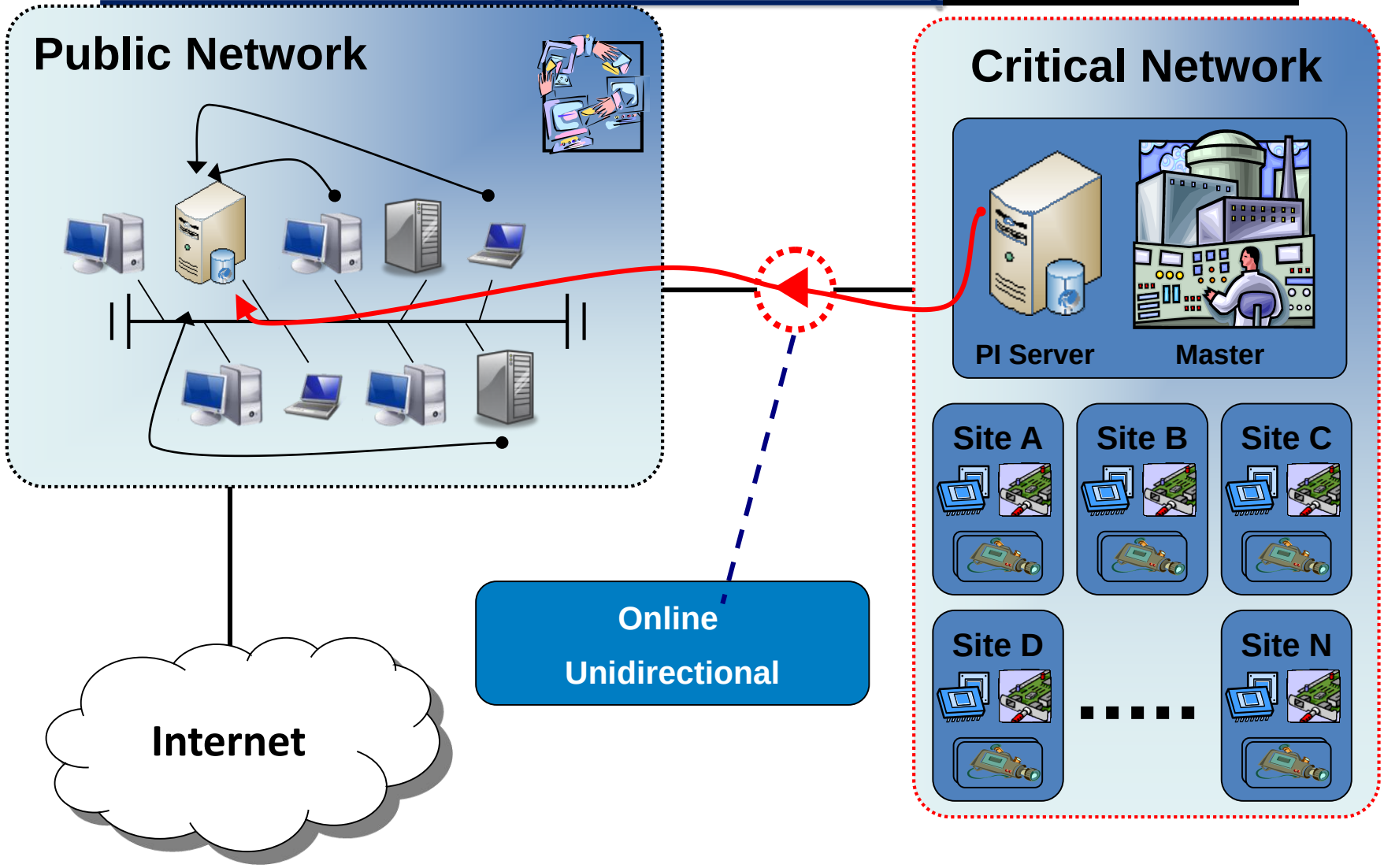
Top 10 - Cyber Recommendations

1 - Networks Segregation



Top 10 - Cyber Recommendations

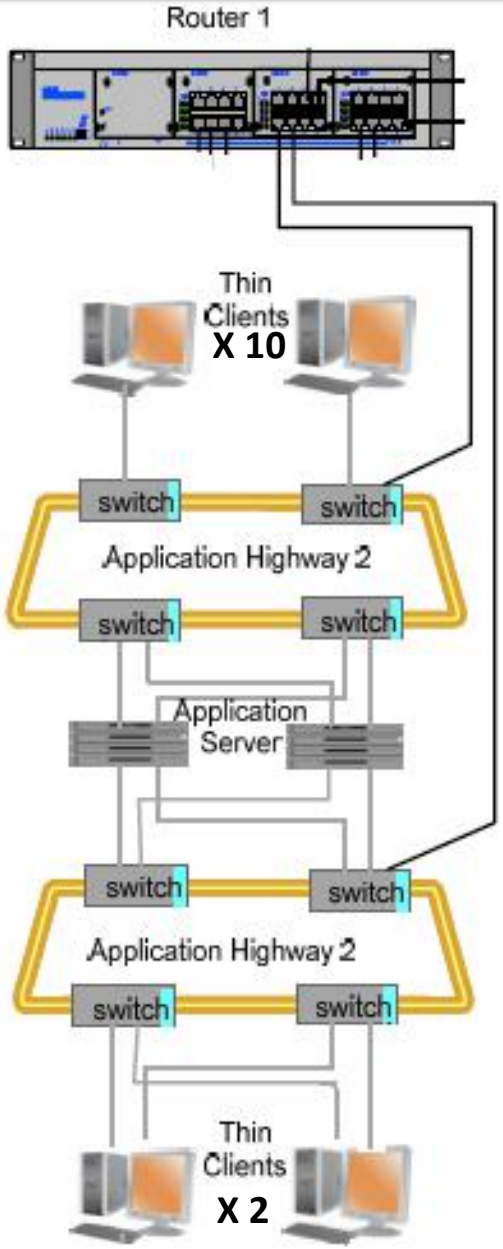
2 One-way data flow (Data Diode)



1. **Data flow from critical to less critical network is allowed only via one way device**
2. **One point of interface**

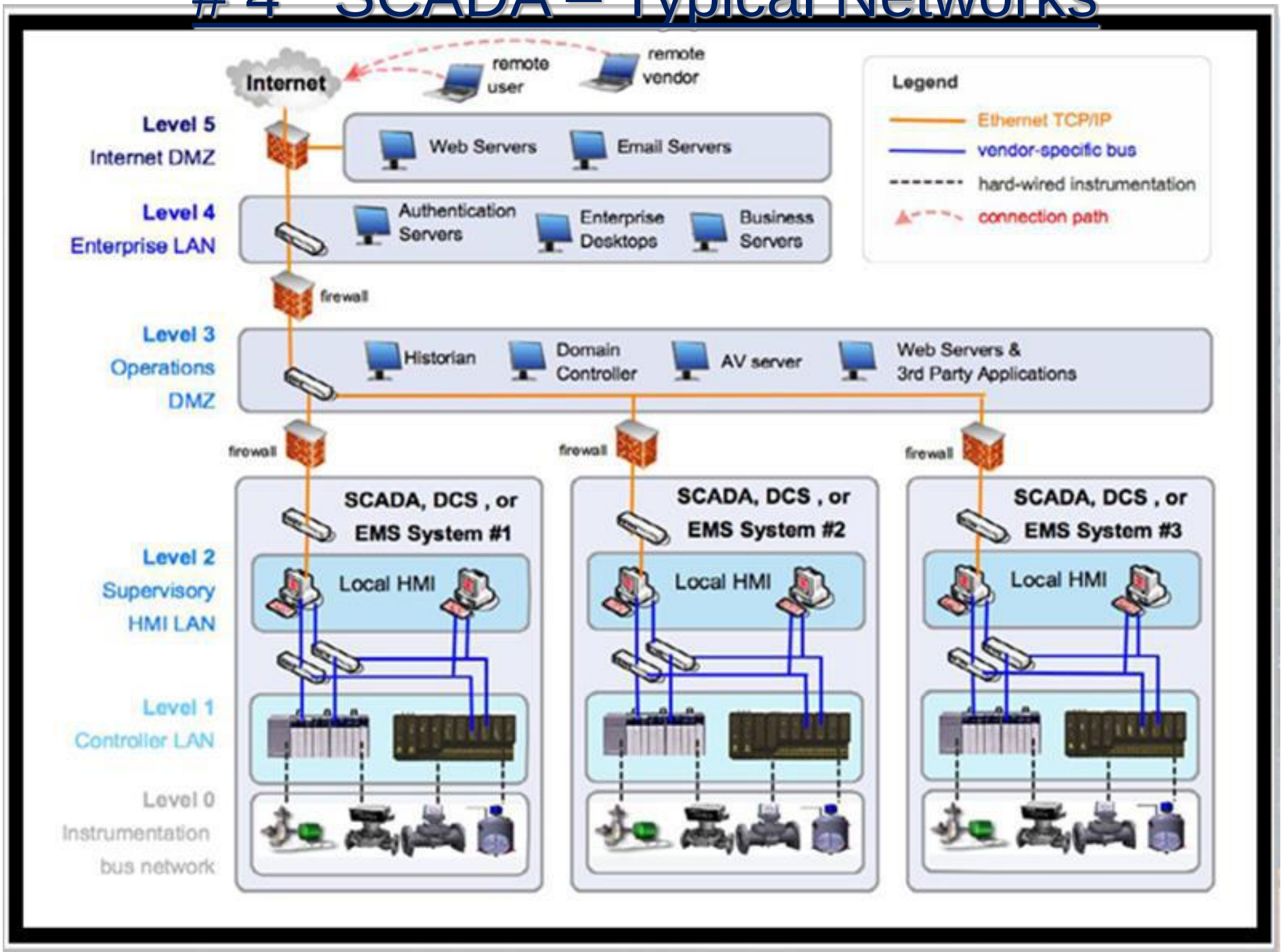
Top 10 - Cyber Recommendations

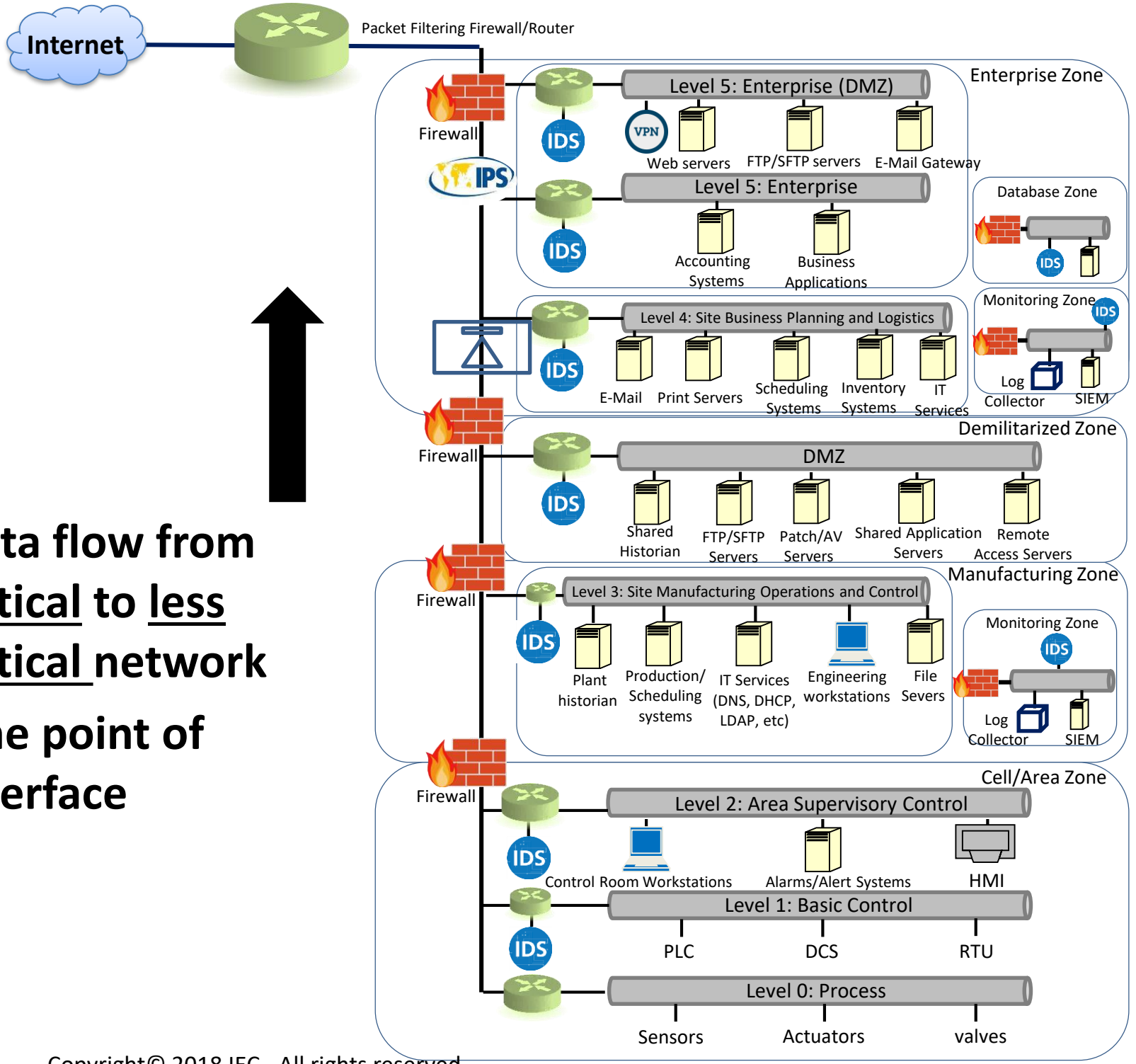
3 Redundancy



Top 10 - Cyber Recommendations

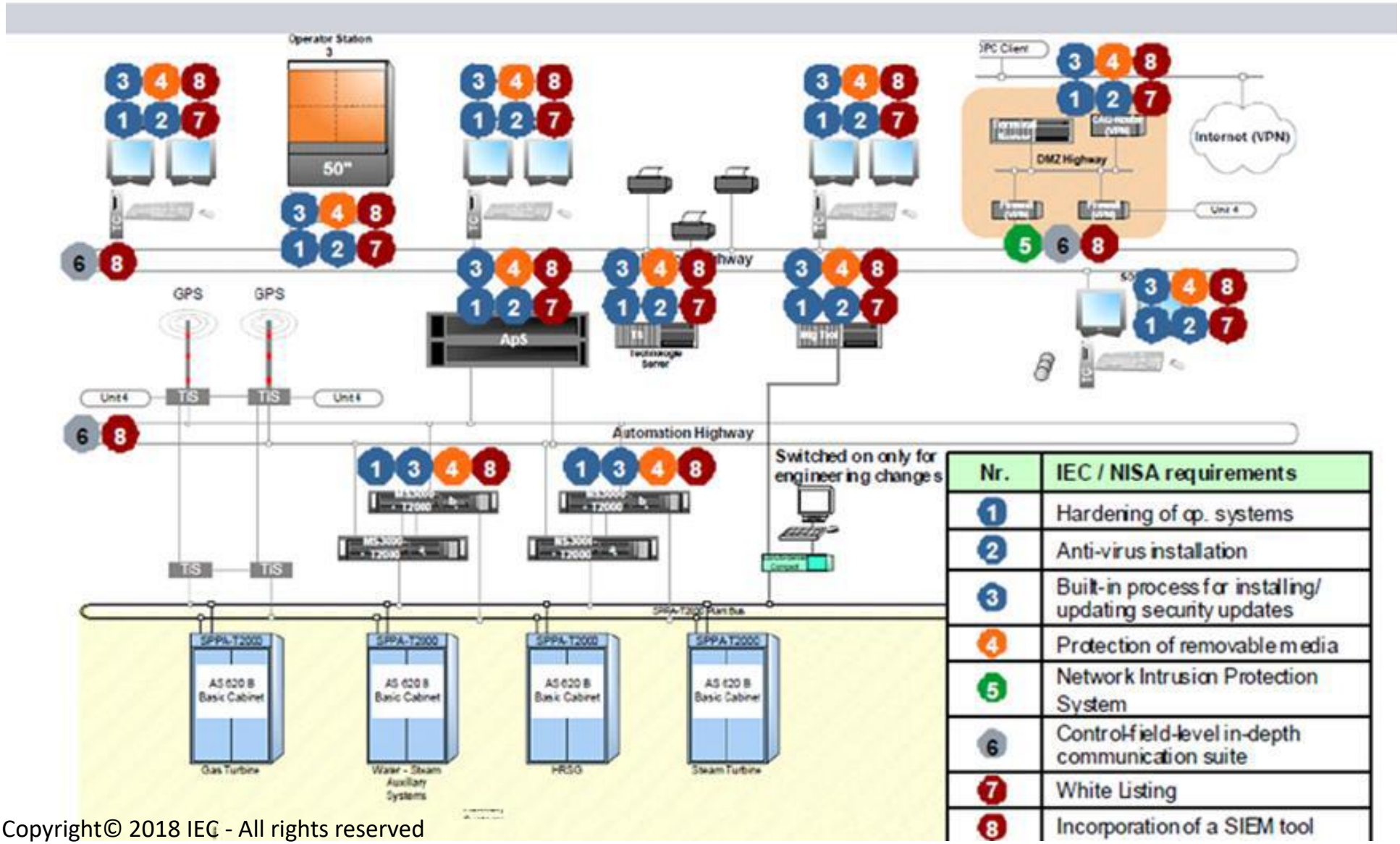
4 SCADA – Typical Networks





1. **Data flow from <u>critical</u> to <u>less critical</u> network**
2. **One point of interface**

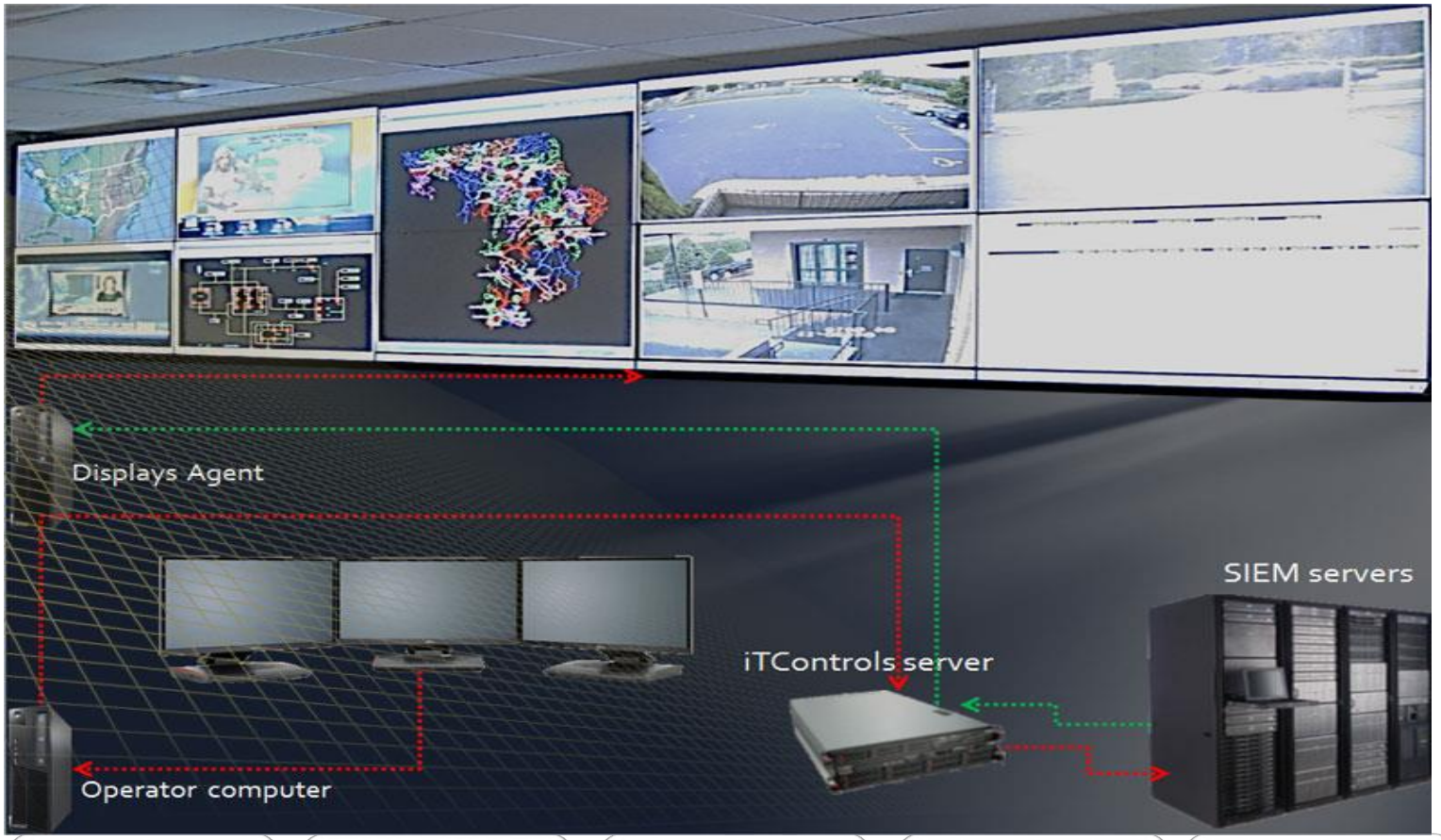
Top 10 - Cyber Recommendations
5 – Cyber Protection Package



Nr.	IEC / NISA requirements
1	Hardening of op. systems
2	Anti-virus installation
3	Built-in process for installing/ updating security updates
4	Protection of removable media
5	Network Intrusion Protection System
6	Control-field-level in-depth communication suite
7	White Listing
8	Incorporation of a SIEM tool

Top 10 - Cyber Recommendations

6 - Security Operations Center (SOC)



Presentation manager | Computer configuration management | Dashboards management | Monitoring set management | Monitoring set example

1. **Real time alerts**
2. **Working in SOC requires a lot of skills and expertise.**
3. **The operator can benefit from a “graphical representation”**

Top 10 - Cyber Recommendations
7 - Incidence Response

1. Preparation
- Planning is everything
- Management support
- Policy review
- Law enforcement interaction
- Tracking
- Identify team
- Use information from users
- Checklists, procedures, other tools

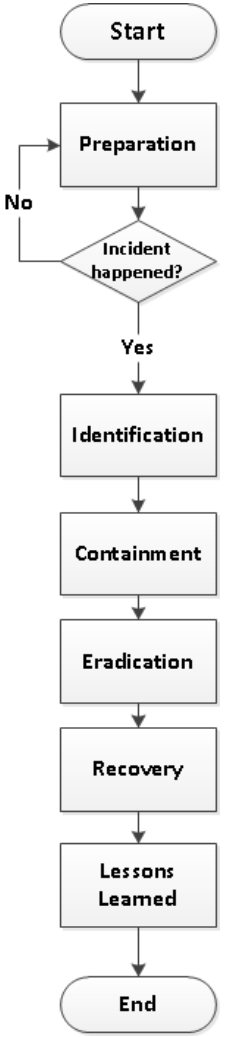
2. Identification
- Alert
- Analyzers
- Minimize false positives
- Source of alert
- Primary Handler
- Checklists for first responders
  - Date, time, description
  - first sign, patterns

3. Containment
- Isolating the issue
- Document what is or will be done
- Making Backups
- Do not make things worse

4. Eradication
- Fix before putting back online
- Identify attack vector
- Potential for repeat compromise
- Perform cleanups
  - IP changes
  - Scans, integrity checks..

5. Recovery
- Do not restore compromised code
- Validate
- System owner makes the call on full operation
- Monitor

6. Lessons Learned
- Gather all related info and facts
- Have on site handler submit draft executive summary
- Outside, non-technical points of view



Incidence Response team has to be prepare for any event

Top 10 - Cyber Recommendations

8 - Awareness – Training & Drills

Training

Attackers premises

Defender premises

Supervisory

Drills

SCADA

- **Lack of awareness in one part of the organization constitutes a threat to all**

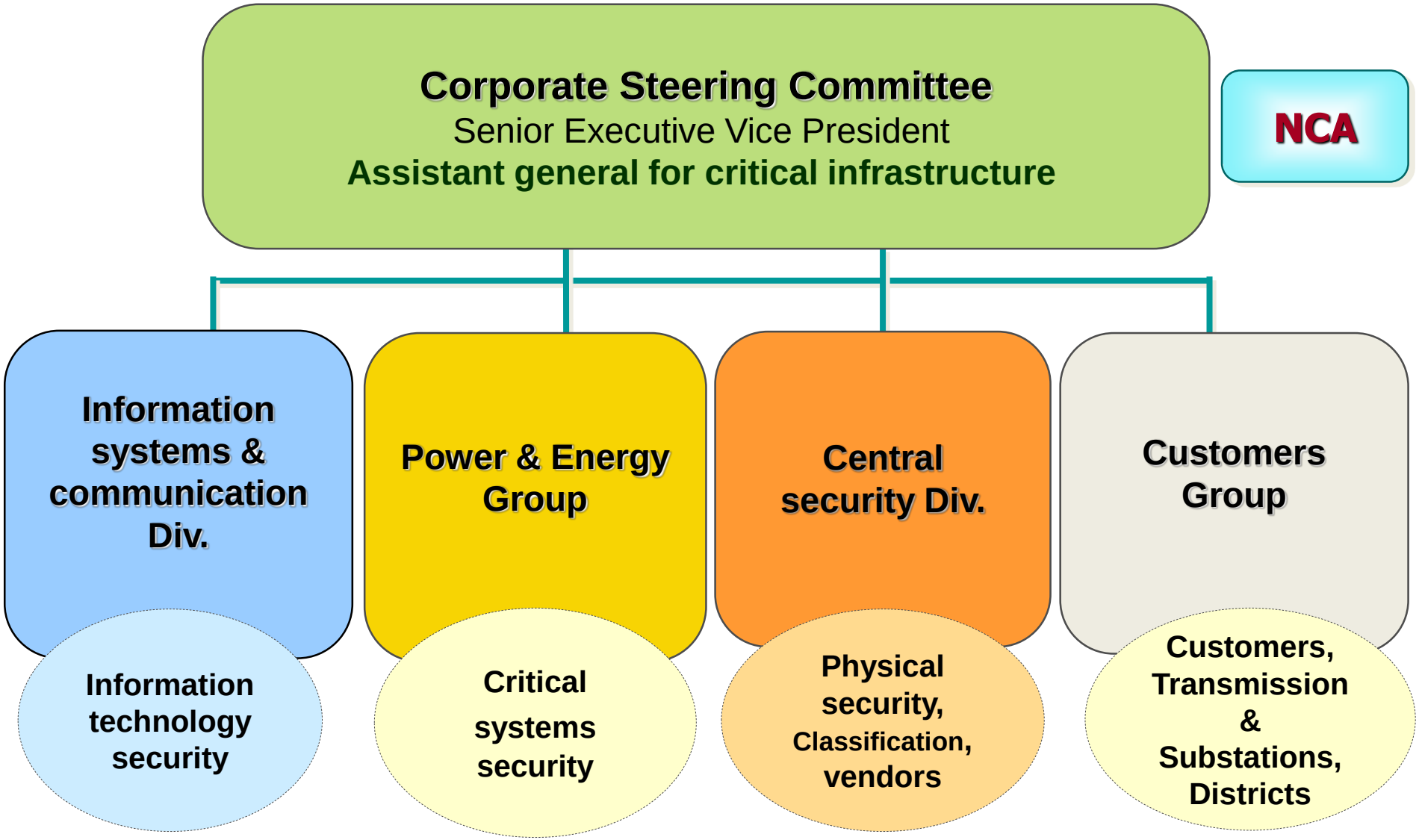
Top 10 - Cyber Recommendations

8 - Awareness – Training & Drills


CYB
ER
GYM

Top 10 - Cyber Recommendations

9 - Defense Strategy- Steering Committees



Top 10 - Cyber Recommendations

10 - Intelligence

1. **Web resources/reports for indicators of suspicious/malicious attacks**
2. **Threat Intelligence Provider - Social media monitoring, “hacktivism” campaigns**
3. **CVE - Common Vulnerabilities and Exposures**

Conclusions

Adapt or become extinct !


Thank you