Questions to Ask & Monitoring Your Cyber Posture

MEARIE 2016 Conference

Doug Westlund

VP, Strategic Planning & Implementation Services

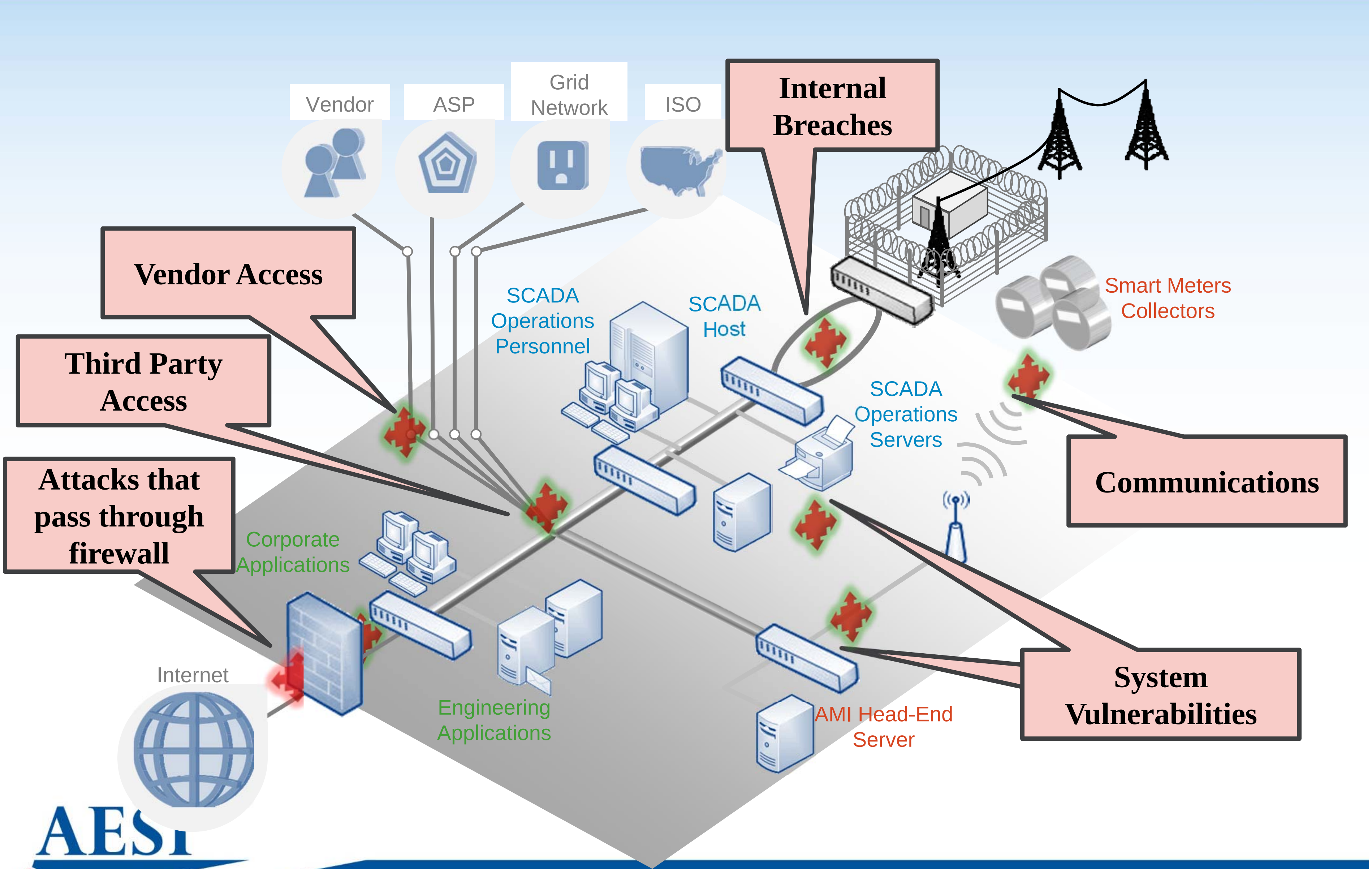
AESI Inc.

Presentation Topics

- **Cyber Risks for LDCs**
- **What Questions to Ask**
- **Security Blueprint – Governance Tool**
- **Security Dashboard – Risk Management Tool**
- **Q & A**

AESI

Cyber Risks for LDCs



Internal Breaches

Vendor Access

Third Party Access

Attacks that pass through firewall

Communications

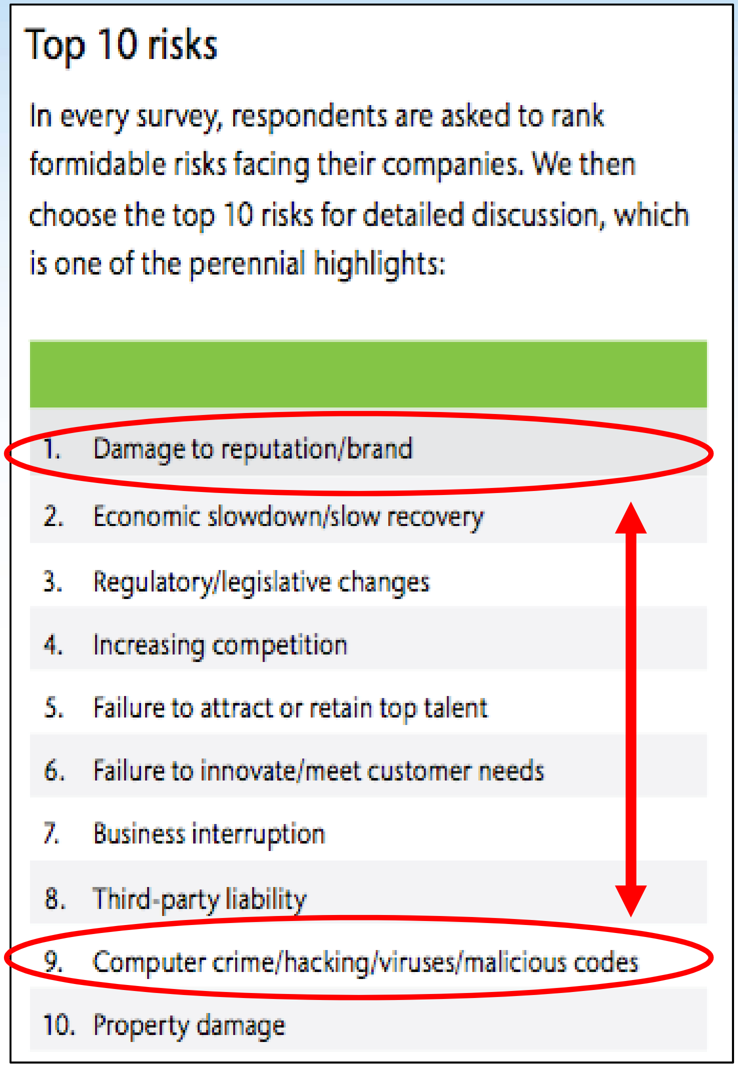
System Vulnerabilities

Key Cyber Security Principles for Utilities

- It's a continuous risk management process
- Internal capabilities and external risks and threat levels need to be gauged
- A holistic perspective is required including IT, OT, physical security and governance
- Unlike beer there is no silver bullet …

AESI

AON 2015 Risk Management Report



Top 10 risks

In every survey, respondents are asked to rank formidable risks facing their companies. We then choose the top 10 risks for detailed discussion, which is one of the perennial highlights:

1. Damage to reputation/brand
2. Economic slowdown/slow recovery
3. Regulatory/legislative changes
4. Increasing competition
5. Failure to attract or retain top talent
6. Failure to innovate/meet customer needs
7. Business interruption
8. Third-party liability
9. Computer crime/hacking/viruses/malicious codes
10. Property damage

“Computer crimes/ hacking have emerged for the first time as a top-10 risk”

“Cyber risk is fast moving, impossible to predict, and difficult to understand, but the damage can be immense”

The Board’s Role

“If a cybersecurity breach were to bring down a major portion of our power grid, we could not pump water or fuel, could not access our financial records, and our communications networks would be silent.

Electric utilities and their boards of directors need to be proactive in dealing with this threat.”

Source: A New Responsibility for Utility Boards of Directors: Cybersecurity, ElectricityPolicy.com, October 2015

What Questions to Ask ?

1) **Do we have an adequate cyber & privacy training program for the LDC and the Board ?**

Mgt Team / Board:

Cyber Risk Training

Annually, or as required

All Employees:

Awareness Training

Every Quarter

Critical Systems Users:

Detailed Training

Annually, or as required

What Questions to Ask ?

2) Who has responsibility for cyber security on the Board ?

Audit Committee ?

Technology Committee ?

Other ?

Risk Management Committee ?

What Questions to Ask ?

3) Does the Board and the LDC have the necessary skills to manage our cyber risk ?

Hiring

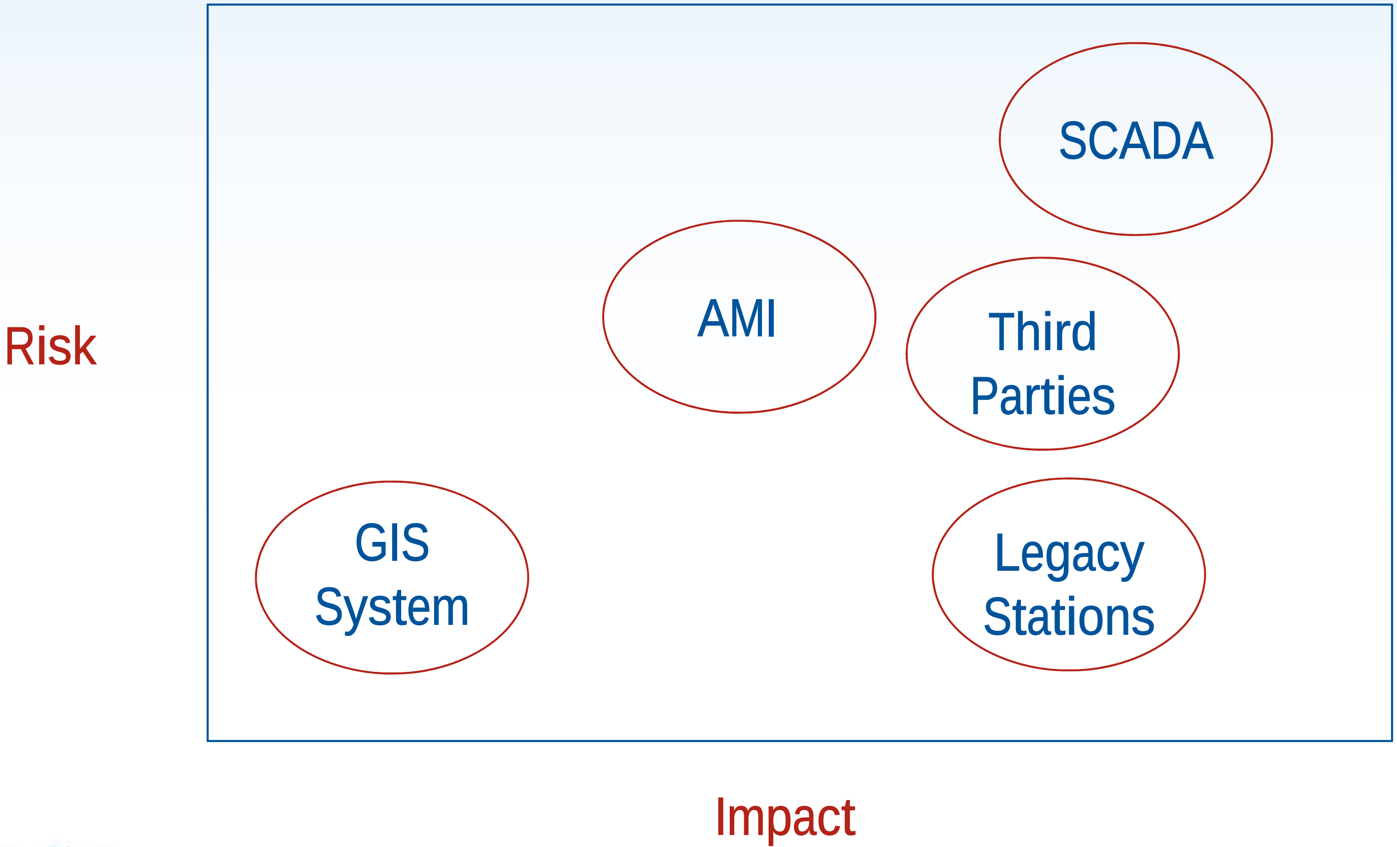
Training

Assistance from Vendors

Collaboration with other LDCs and industry groups !

What Questions to Ask ?

4) What is our cyber risk tolerance ?



Risk

SCADA

AMI

Third Parties

GIS System

Legacy Stations

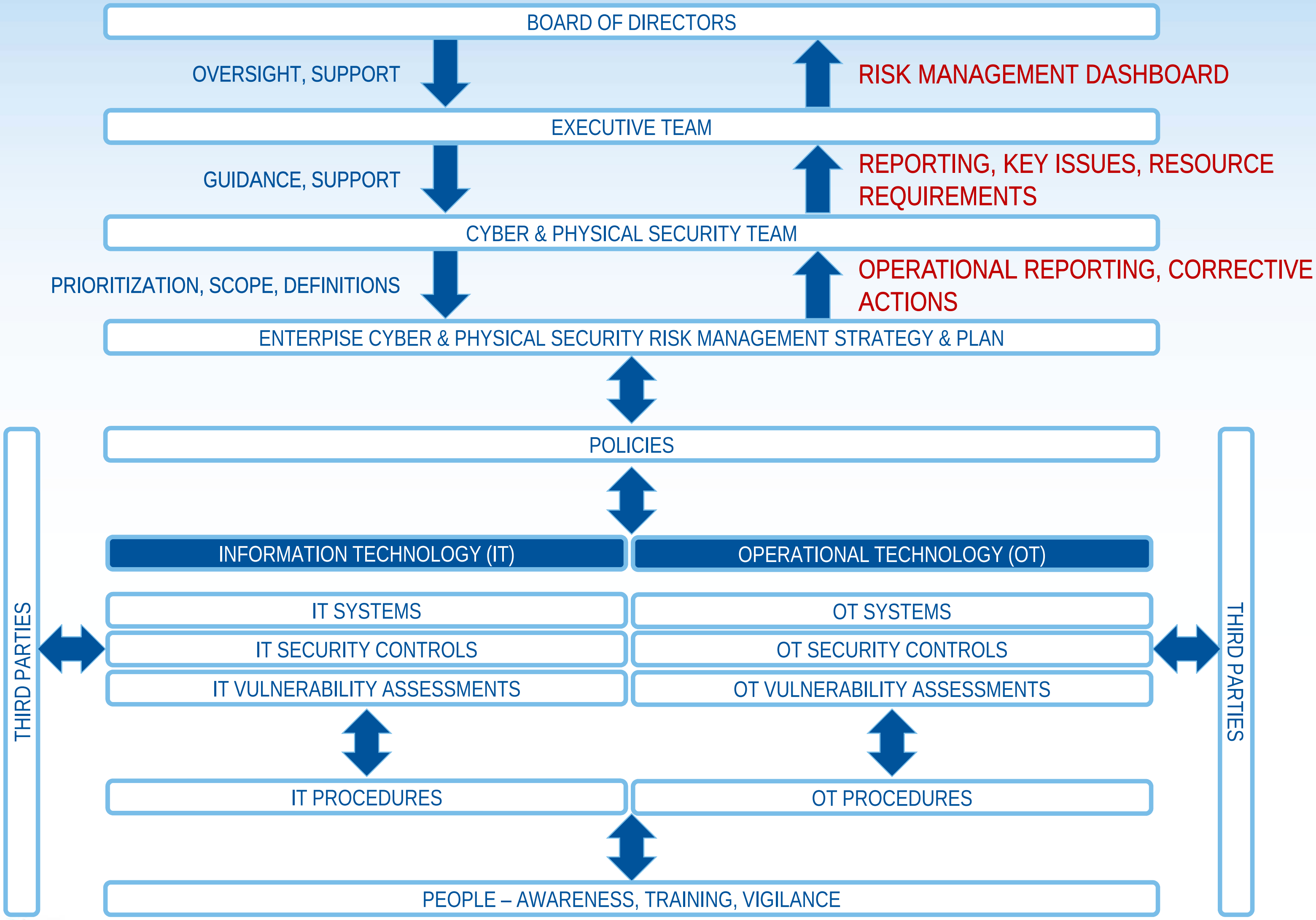
Impact

What Questions to Ask ?

5) **Do we have visibility / line of sight to our cyber security posture on a continuous basis ?**

AESI

Security Blueprint – A Governance Tool



BOARD OF DIRECTORS

OVERSIGHT, SUPPORT

RISK MANAGEMENT DASHBOARD

EXECUTIVE TEAM

GUIDANCE, SUPPORT

REPORTING, KEY ISSUES, RESOURCE REQUIREMENTS

CYBER & PHYSICAL SECURITY TEAM

PRIORITIZATION, SCOPE, DEFINITIONS

OPERATIONAL REPORTING, CORRECTIVE ACTIONS

ENTERPISE CYBER & PHYSICAL SECURITY RISK MANAGEMENT STRATEGY & PLAN

POLICIES

THIRD PARTIES

INFORMATION TECHNOLOGY (IT)

IT SYSTEMS

IT SECURITY CONTROLS

IT VULNERABILITY ASSESSMENTS

IT PROCEDURES

OPERATIONAL TECHNOLOGY (OT)

OT SYSTEMS

OT SECURITY CONTROLS

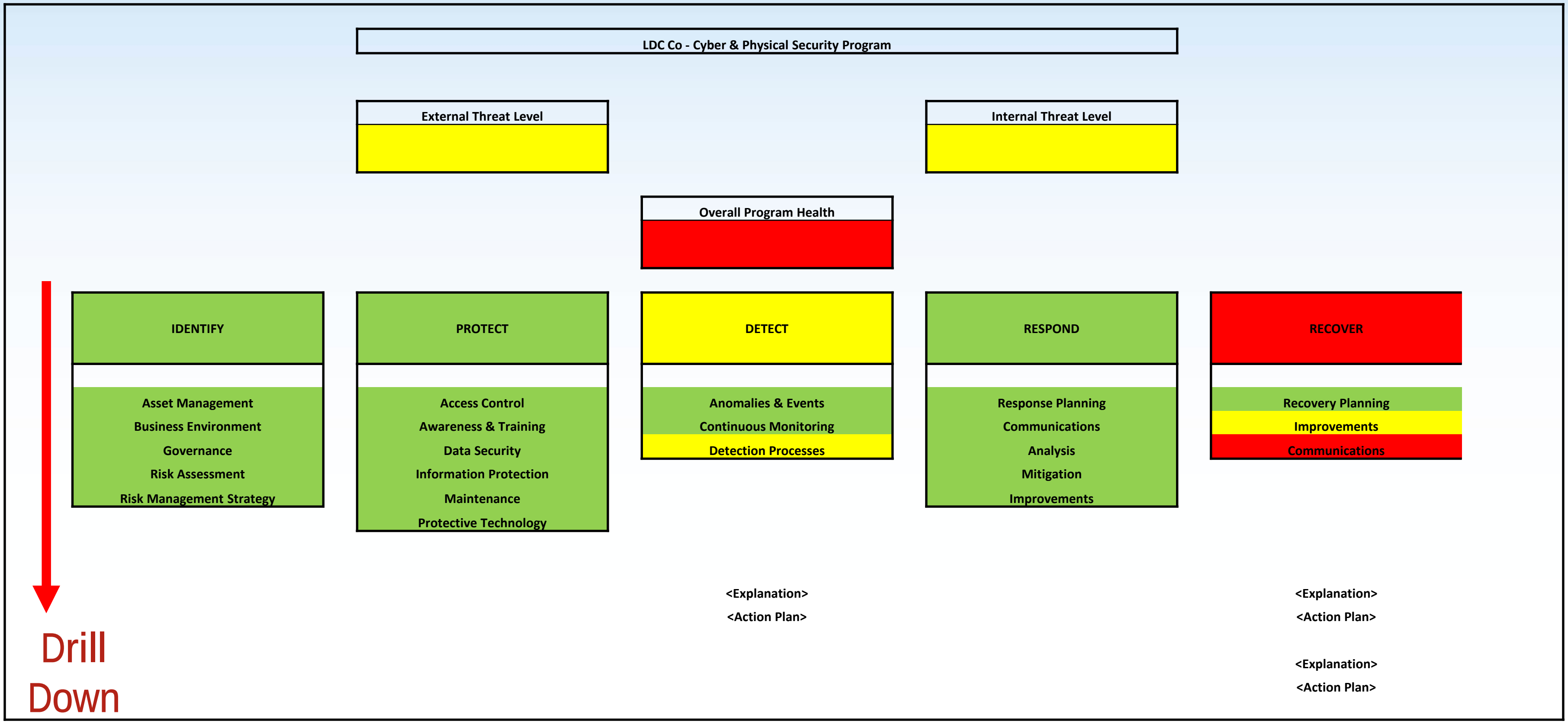
OT VULNERABILITY ASSESSMENTS

OT PROCEDURES

THIRD PARTIES

PEOPLE – AWARENESS, TRAINING, VIGILANCE

Dashboards – Operational View



LDC Co - Cyber & Physical Security Program

External Threat Level 🟨

Internal Threat Level 🟨

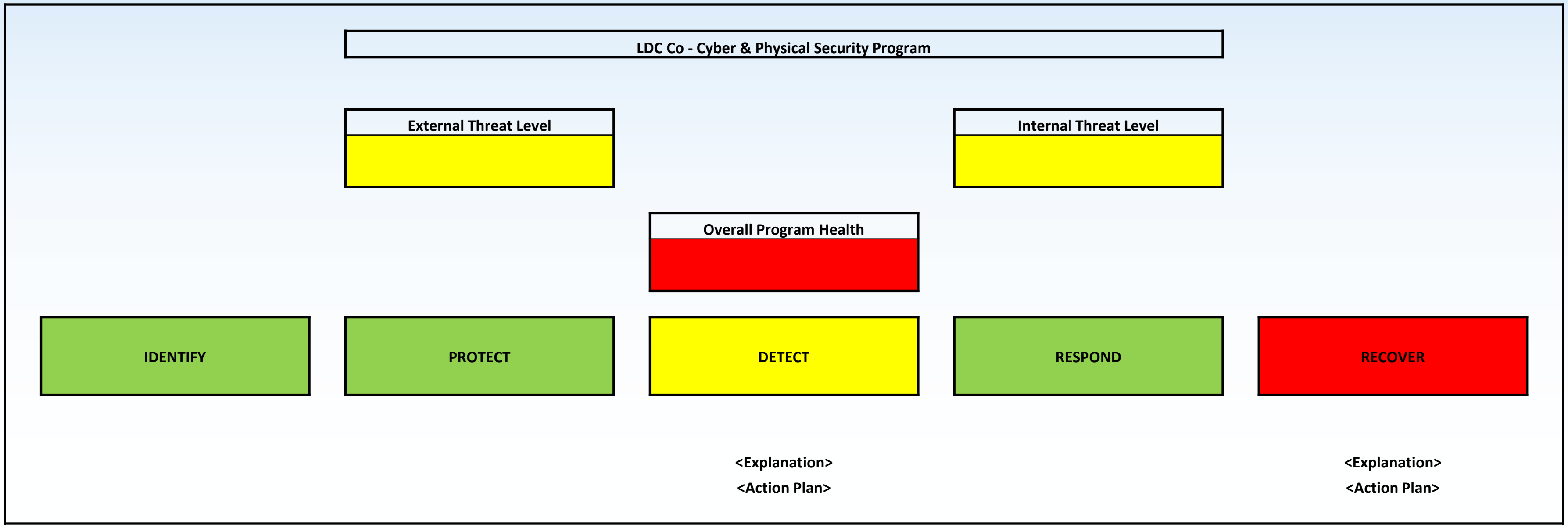
Overall Program Health 🟥

🟩 IDENTIFY	🟩 PROTECT	🟨 DETECT	🟩 RESPOND	🟥 RECOVER
🟩 Asset Management	🟩 Access Control	🟩 Anomalies & Events	🟩 Response Planning	🟩 Recovery Planning
🟩 Business Environment	🟩 Awareness & Training	🟩 Continuous Monitoring	🟩 Communications	🟨 Improvements
🟩 Governance	🟩 Data Security	🟨 Detection Processes	🟩 Analysis	🟥 Communications
🟩 Risk Assessment	🟩 Information Protection		🟩 Mitigation	
🟩 Risk Management Strategy	🟩 Maintenance		🟩 Improvements	
	🟩 Protective Technology			
		<Explanation> <Action Plan>		<Explanation> <Action Plan> <Explanation> <Action Plan>

Drill Down

Framework for Improving Critical Infrastructure Cybersecurity, Version 1.0, NIST

Dashboards – Board / Executive View



LDC Co - Cyber & Physical Security Program

External Threat Level 🟨

Internal Threat Level 🟨

Overall Program Health 🟥

IDENTIFY	PROTECT	DETECT	RESPOND	RECOVER
🟩	🟩	🟨	🟩	🟥
		<Explanation> <Action Plan>		<Explanation> <Action Plan>

Framework for Improving Critical Infrastructure Cybersecurity, Version 1.0, NIST

Recap

Addressing the 5 Questions

+

Governance

+

Risk Management

=

Improved Cyber Security Posture and

Evidence of Due Diligence

AESI

Q & A

Thank You !

Doug Westlund

VP Strategic Planning & Implementation Services

AESI Inc.

dougw@aesi-inc.com

905-875-2075 ext 278