SANS

Cyber Security and the Chemical Sector

Glenn Aydell

LazyHacker Consulting

Disclaimer

The views, thoughts, and opinions expressed in this presentation belong solely to the author, and not necessarily to the author's employer, organization, committee or other group or individual.

Who is Glenn Aydell?

Background

- Numbers make me look old, so let's go with double digit years experience in programming, networking and cyber security
- Started as a CICS/DB2 programmer in the early 90's
- Past 23 years in various IT/OT security and networking roles with large chemical company where currently hold title of "senior expert" (whatever that means)
- Various working groups within the chemical industry
- Most intimidating career change occurred in 2011… the official move to engineering with a focus on ICS security (engineers are smart and they scare me)

Expected Takeaway about the Chemical Industry

Diversity

Defensibility

Dependency Management

Where does the Chemical Industry fit?

- Oil and Natural Gas?
- Utilities?
- Manufacturing?
- Mining?

Expected Takeaway about the Chemical Industry

Diversity

Defensibility

Dependency Management

Chemical Industry Diversity

- Petroleum Refining
- Rubber and Plastic Products
- Textiles
- Apparel
- Pulp and Paper
- Primary Metals
- Agriculture

Chemical Industry Product Types

Product Type	Examples
inorganic industrial	ammonia, chlorine, sodium hydroxide, sulfuric acid, nitric acid
organic industrial	acrylonitrile, phenol, ethylene oxide, urea
ceramic products	silica brick, frit
petrochemicals	ethylene, propylene, benzene, styrene
agrochemicals	fertilizers, insecticides, herbicides
polymers	polyethylene, Bakelite, polyester
elastomers	polyisoprene, neoprene, polyurethane
oleochemicals	lard, soybean oil, stearic acid
explosives	nitroglycerin, ammonium nitrate, nitrocellulose
fragrances and flavors	benzyl benzoate, coumarin, vanillin
industrial gases	nitrogen, oxygen, acetylene, nitrous oxide

Company Overview

Diverse Portfolio

- Agriculture
- Construction Chemicals
- Coatings
- Polyurethanes
- Oil & Natural Gas
- Catalysts
- Personal Care and Nutrition
- Additives and Specialty Chemicals

Diverse Sites

- Large (Verbund) Sites
- Medium (Multi BU) Sites
- Small (Single BU) Sites

Diverse Plants

- Batch
- Continuous
- Hybrid
- Utilities

What does a 'Typical' Chemical Plant look like?

It depends…

- Washing sand
- Cracking natural gas
- Dipping components in slurry
- Creating super absorbents
- Mixing paint

What do most plants have in common…

Expected Takeaway about the Chemical Industry

Diversity

Defensibility

Dependency Management

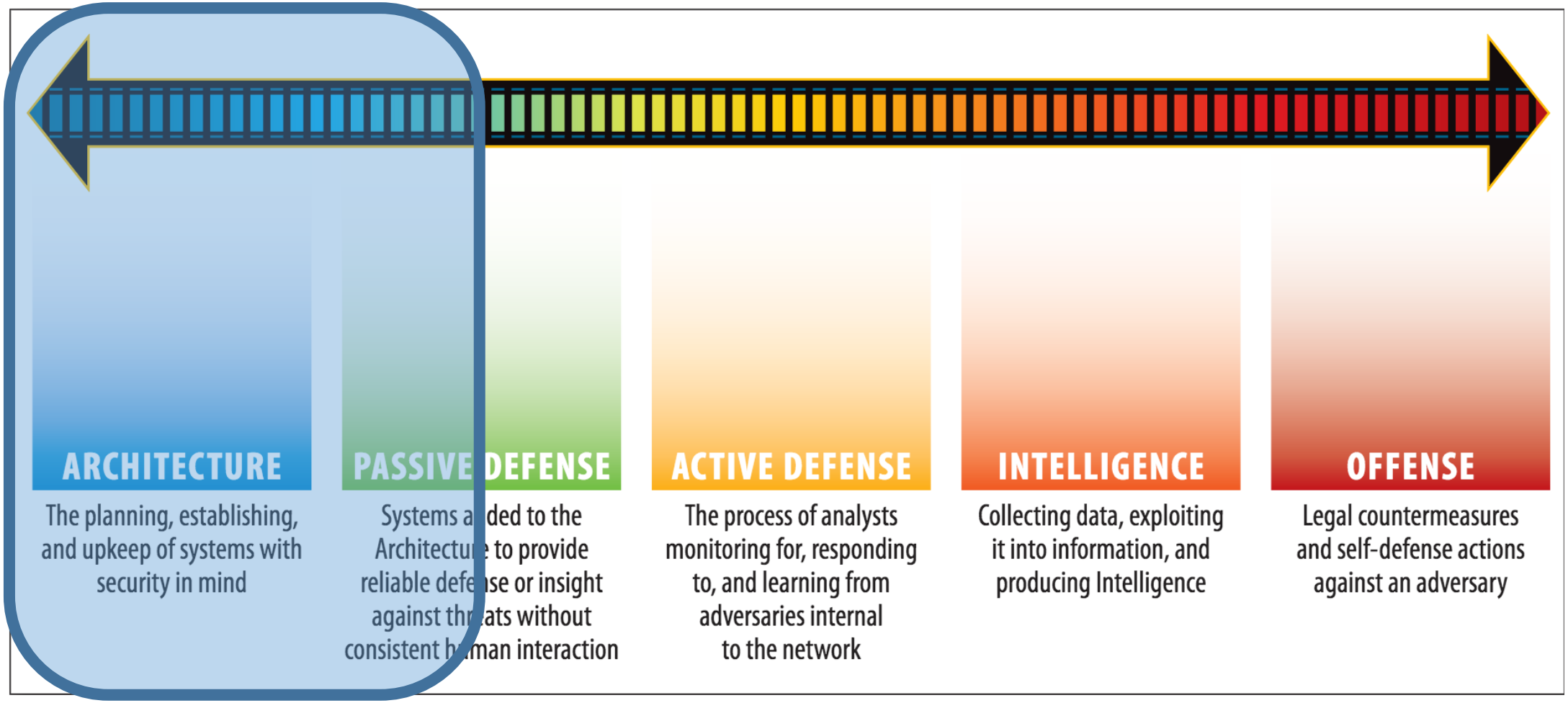
Common Among Plants

Operators onsite

Limited or NO Direct Communications Requirements

No Persistent Remote Access Requirements

Sliding Scale of Cyber Security



Expected Takeaway about the Chemical Industry

Diversity

Defensibility

Dependency Management

Incident/Near Miss

Example: Power Test

Overview:

Routine electrical test of non-critical circuits in administration building outside normal working hours triggered unexpected outages in important infrastructure components.

Impact:

- WAN router outage caused loss of access to offsite systems including ERP resulting in inability to process lab data for shipments which in turn resulted in long logistic delays and penalties
- Virtualization host outage resulted in important site servers becoming unavailable for access to online documentation for manual processes
- OT firewall outage resulted in loss of primary source of environmental data

Incident/Near Miss

Example: Feed stock pipeline

Overview:

A supplier loss of containment incident led to a request by the supplier to install a ‘read only’ wireless sensor on a single flow meter at the ingress point of the pipeline into our campus. Security review of the technology to be installed revealed the ability to calibrate the flow meter over this wireless connection.

Impact:

This was considered a “near miss” as the risks were discovered before the implementation, but the result could have been modifications (accidental or intentional) to flow meter parameters which could have led to a significant incident.

Incident/Near Miss

Example: Firewall upgrade

Overview:

Several weeks after the upgrade of a large firewall cluster a decommissioned firewall from the old cluster (which was left in the rack but powered off) was accidentally powered up.

Impact:

- Logistics – trucks and rail cars were not able to enter or leave the facility causing significant traffic delays for the entire city
- Lab – lab results were not able to be processed within ERP resulting in additional delays for processing shipments
- Fire station – onsite fire response was blind

Incident/Near Miss

Example: Backhoe

Overview:

Off site work being done by a farmer resulted in cutting a fiber bundle which contained both the primary and backup circuits for the site.

Impact:

- WAN outage resulting in loss of access to offsite data and ERP
- Phone outage resulting in inability to phones even for onsite calls
- Manual processing of shipments resulting in delays, traffic issues and penalties

Incident/Near Miss

Example: OT Switch reboot

Overview:

Troubleshooting the loss of communications to a redundant controller pair led to the reboot of a pair of redundant OT switches. The saved switch configurations were not current and the loop detection protocol settings did not align with the rest of the infrastructure resulting in an unexplained flooding. The misconfiguration was not known or detected as troubleshooting continued down a different path.

Impact:

Loss of view for DCS operators for over 8 hours. The process was run off the SIS while troubleshooting continued.

Lessons Learned

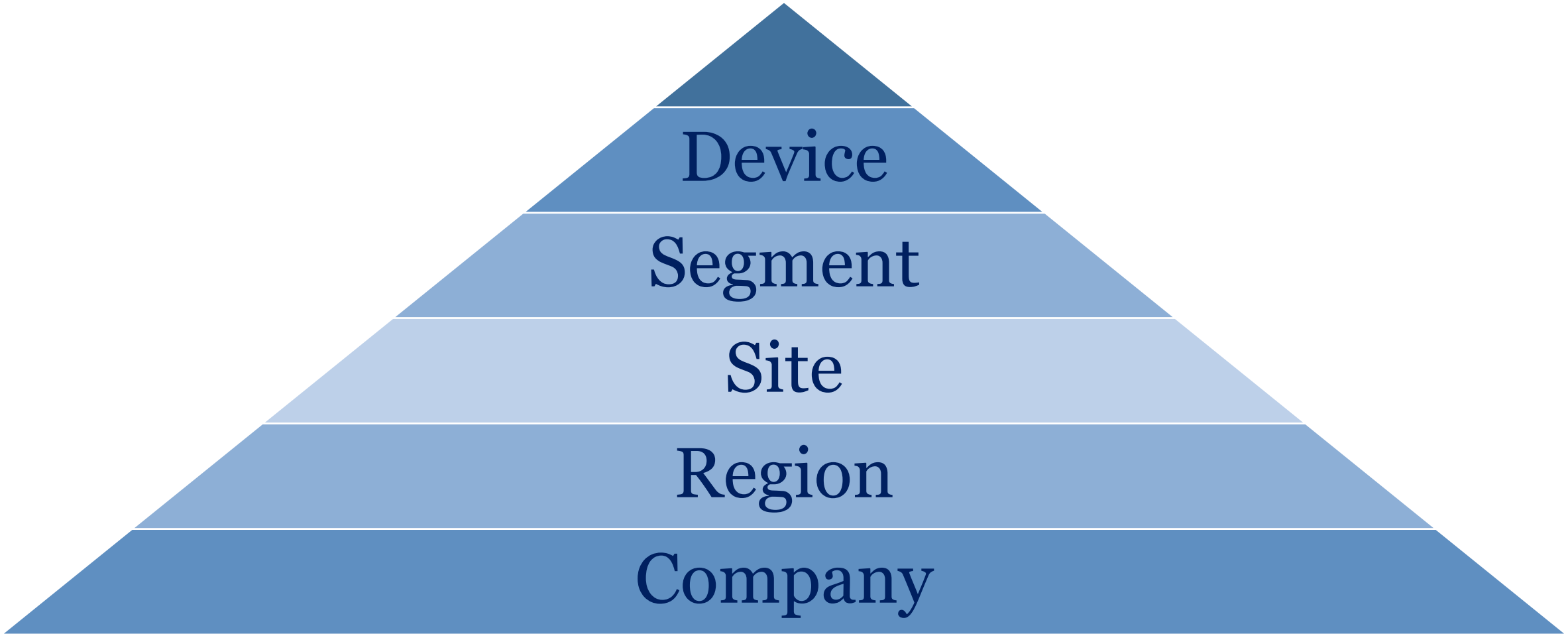
Dependency Management:

- How do projects handle dependencies?
- What about Business Continuity Planning?
- Why don't we do a better job managing dependencies after project delivery?

How does this relate to ICS Cyber Security?

Cyber Incident Containment Plan

Cyber Security Incident Containment



Takeaway about the Chemical Industry

Diversity

Defensibility

Dependency Management

Questions