



The Demand for Data

Driving the Need for OT/IT Integration and Cybersecurity Protections

Campus Energy 2019

By
Scott Smith

Data Driven Value

Predictive Analytics

Data Aggregation

Condition Based Maintenance

Situational Awareness

Fault Detection and Diagnostics

Energy Management

Point in Time Analysis

Energy Use Reporting



Are We Ready

Demand for Data



In recent survey of Facility Managers that believe that there will be increase in the demand for data.

80%

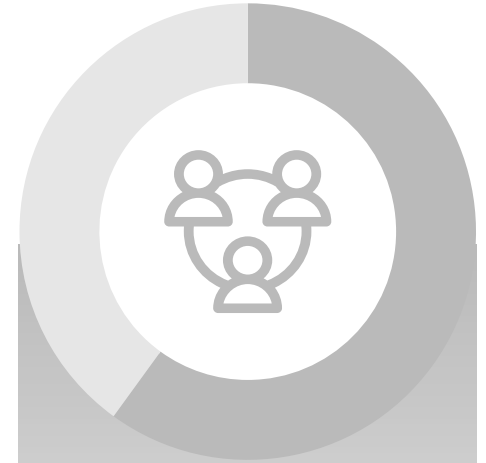
Cybersecurity



Facility Managers that have never completed a complete assessment of cybersecurity vulnerabilities.

57%

Use of Data Today



Facility Managers analyze the real time data greater than a year, never or only when there is an issue.

58%

65%

Have remote access to the controls systems to allow for outsourced support

33%

Have no plan to mitigate risk to control systems

22%

Have no documentation of configuration and code of control system

50%

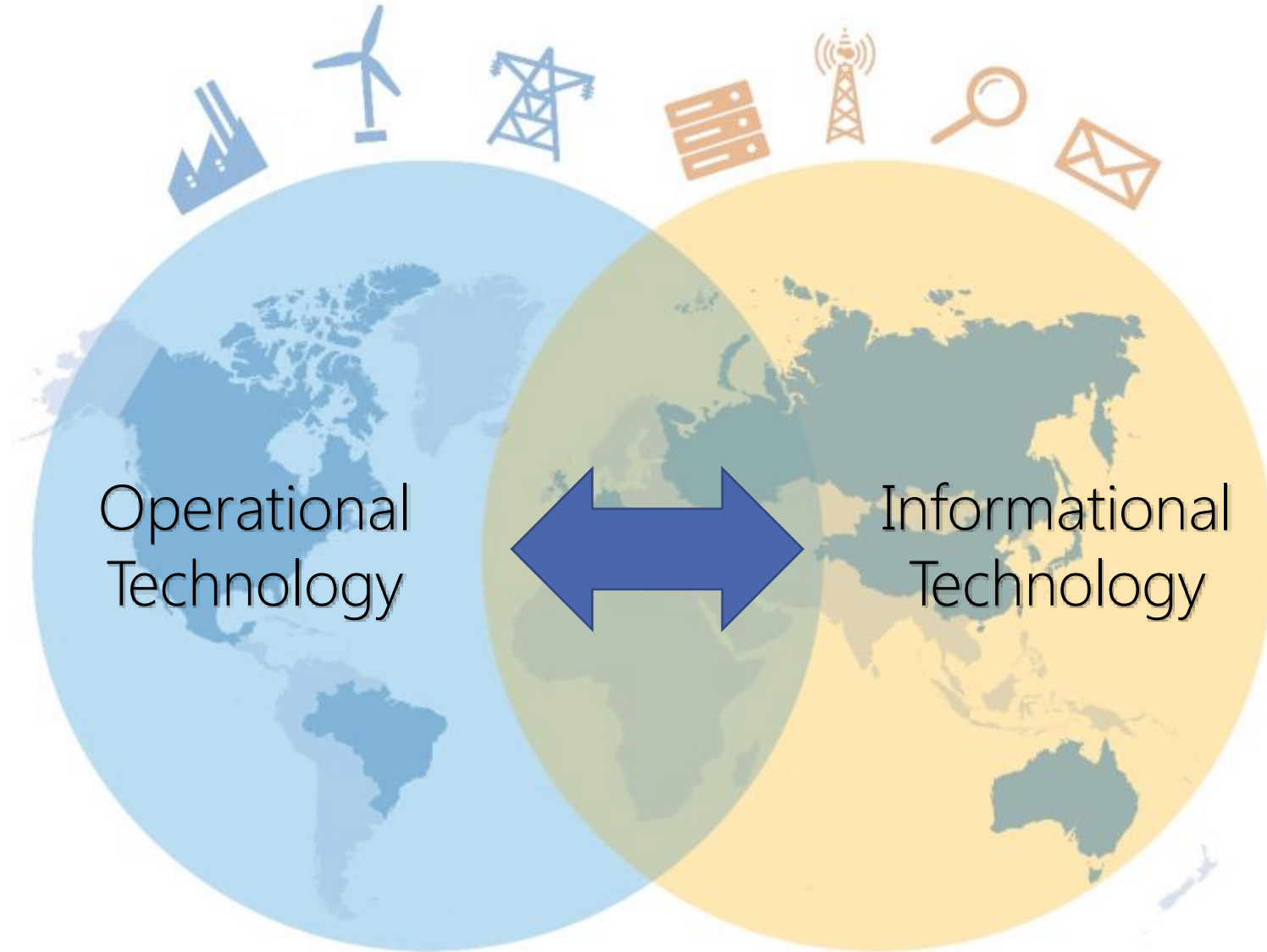
Analyze system logs less frequently than monthly and 6% never analyze them

0 20 40 60 80 100



67% of Facility Managers believe they have the same level of support as IT in terms security, availability, disaster recovery and maintenance of the control systems

The Challenge is OT/IT Integration



MANY FACTORS CONTRIBUTE TO THE OT-IT DIVIDE

Resistance to change, fear of security breaches, different organizational priorities

Data Cleanliness - Machine and sensor-based data reflects real-world conditions and is, by nature, messy.

Fragmented Data Landscapes - OT systems are typically purpose built, limiting access and use of OT data for wider purposes.

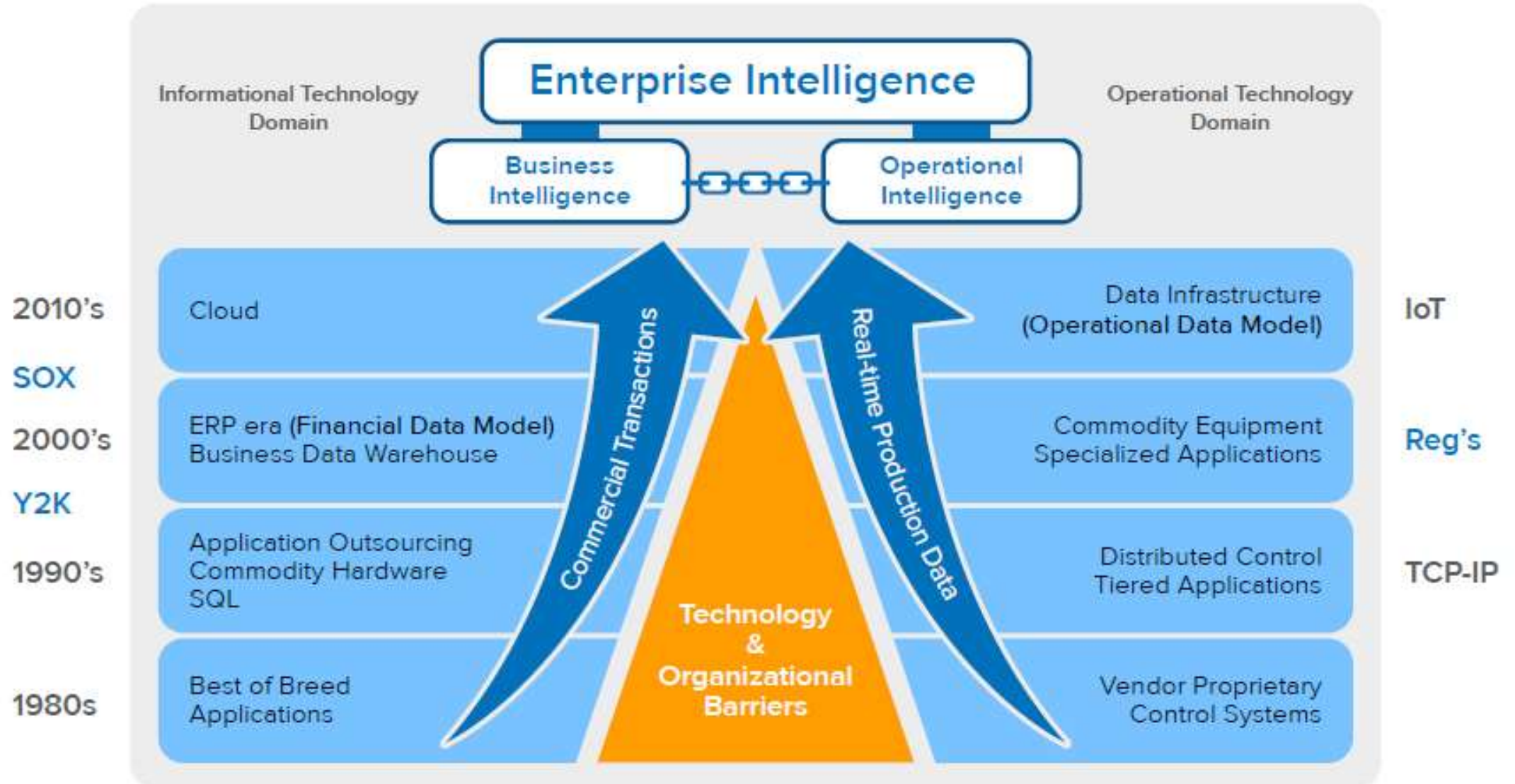
Inability to Scale - Converting sensor based data for local insight is one thing – doing it at fleet or enterprise scale is quite another.

Context and Governance - Experts estimate that 80% of data is “dark” – underutilized, unavailable or forgotten.

Corporate Organization - Traditional cultural and functional boundaries remain.

Safety and Security - Many organizations create a demilitarized zone around OT systems that includes firewalls, data diodes and one-way networking systems as well as razor wire and personnel access control.

Technology Barriers Have Fallen



Remember the Human Dynamic



- Cultural and Functional Boundaries
 - Language Differences
 - Priorities
 - Risks

Steps Towards A Strategy

Liberate Human Capital

- Focus on analysis and solution and less on data collection
- Spend less time in spreadsheets
- Allow time to focus on strategic solutions

Leverage Resources Already in Place

- Solutions come from the control room not the boardroom
- Asset or Process Centric Knowledge Sharing

Reduce Risk and Complexity

- Focus on use cases not on “Big Data” projects
- Separate data from control
- Define Objectives, Governance, Accountability

Don't Cross the Security Barrier

WannaCry Ransomware Should Have Raised to Alarm



57%

Facility Managers have not completed a full cybersecurity assessment



65%

Facilities with remote access for 3rd parties



22%

Have no documentation of configuration and code of control system



38%

Lack situational awareness of the real-time operations across the enterprise

DoD estimates it could cost more than a quarter of a billion dollars to identify, register and implement current vulnerabilities over the next four years in facilities control systems.



A 3D illustration of a level tool, tilted diagonally. It has a white body with a red rectangular bubble level in the center. The level is shown from a perspective that makes it look like it's floating or resting on a surface.

Cybersecurity Challenge

Have you solved growing data demands by separating data from control?

Have you completed a compressive security assessments from a facility operations point of view.

Do you have real-time awareness from generation through consumption including all mission critical KPI?

Do you secondary access security with active approval and logs of all changes?

Do you maintain configuration management, change control, and auditing of systems and logs



The Risk is Real

An attack on US retailer Target, in which millions of customers' credit card information was stolen, was traced back to the heating and ventilation

Remote Access

"How a fish tank helped hack a casino"

IoT Device

Tomorrow's Buildings:
Help! My building has been hacked
In 2013, Google - one of the world's pre-eminent tech companies - was hacked.

Generic Password

IBM ran a penetration test for a facility management company with more than 20 buildings...gained access to the BAS and could have taken control of the systems

Maintenance

The risk does not have to be malicious it could be the execution of poorly trained or inappropriate resources




Internet Accessible

TOTAL RESULTS	
7,931	
TOP COUNTRIES	
	
United States	5,507
Canada	1,176
United Kingdom	175
Australia	95
France	82
TOP SERVICES	
BACnet	7,854
8081	19
Qconn	7
HTTP	7
50695	2
TOP ORGANIZATIONS	
Comcast Business	822
AT&T Internet Services	497
Verizon Wireless	352
Time Warner Cable	313
Frontier Communications	77
TOP OPERATING SYSTEMS	
Unix	2
TOP PRODUCTS	
NiagaraAX Station	1,463
Niagara4 Station	547
DSM_RTR	340
eBMGR	273
DSC_1616E	157

In less than 5 minutes from query to log in screen

Quick Search:

1. US University
2. Military Base
3. US Hospital
4. Electric Utility



SKF_JCISation

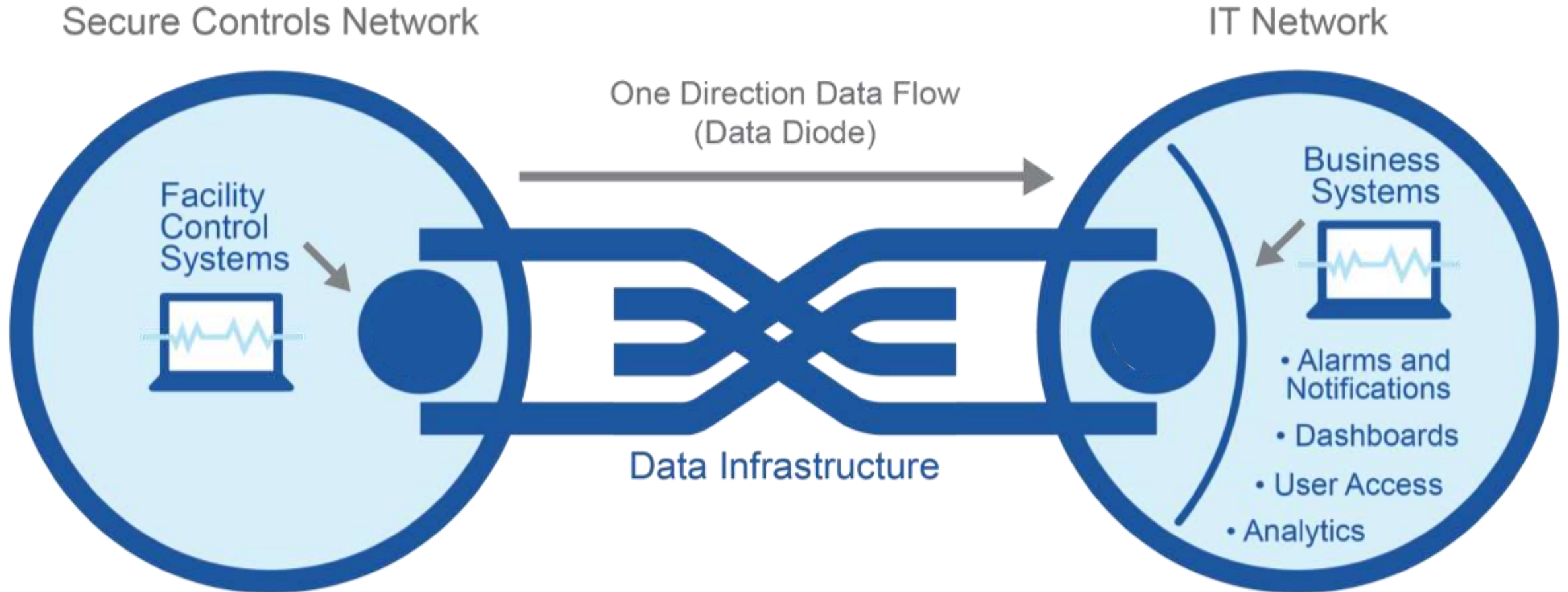
Username:

Login

Use of this software is subject to the [End User License Agreement](#) and other [Third Party Licenses](#)

To connect using Java Web Start [click here](#)

Separate Data from Control



1. Understand future needs and value of data
2. Increase access to data while separating control
3. Use the situational awareness of data to evolve security posture

Steps Towards A Strategy

Situational Awareness is a Security Solution

- Similar to Physical Security Awareness Provides Context
- Facility Awareness Supports Health and Safety
- Monitor Change from Expectations

IT Experience can be Leveraged

- IT Security (Network, Passwords, Account Management, CERT)
- Move Data to the IT Network to Limit Control Access
- Maintenance

Assessments and Audits

- Assessments are Annual not Point in Time
- Audit Log Files
- Vulnerability Tests

Survey

- Do your facility systems provide environmental conditions that are critical to health and safety (examples: housing, food service, medical services, or research)
- Do you believe the demand for data of facility systems will grow?
- Do you have demands in your environment for more data?
- Have you created a data infrastructure to provide access to the data and at the same time restricted access to control?
- Do you regularly complete cybersecurity assessments and vulnerability tests?

Questions



Scott Smith

ssmith@osisoft.com

Industry Principal

OSIsoft, LLC



THANK YOU