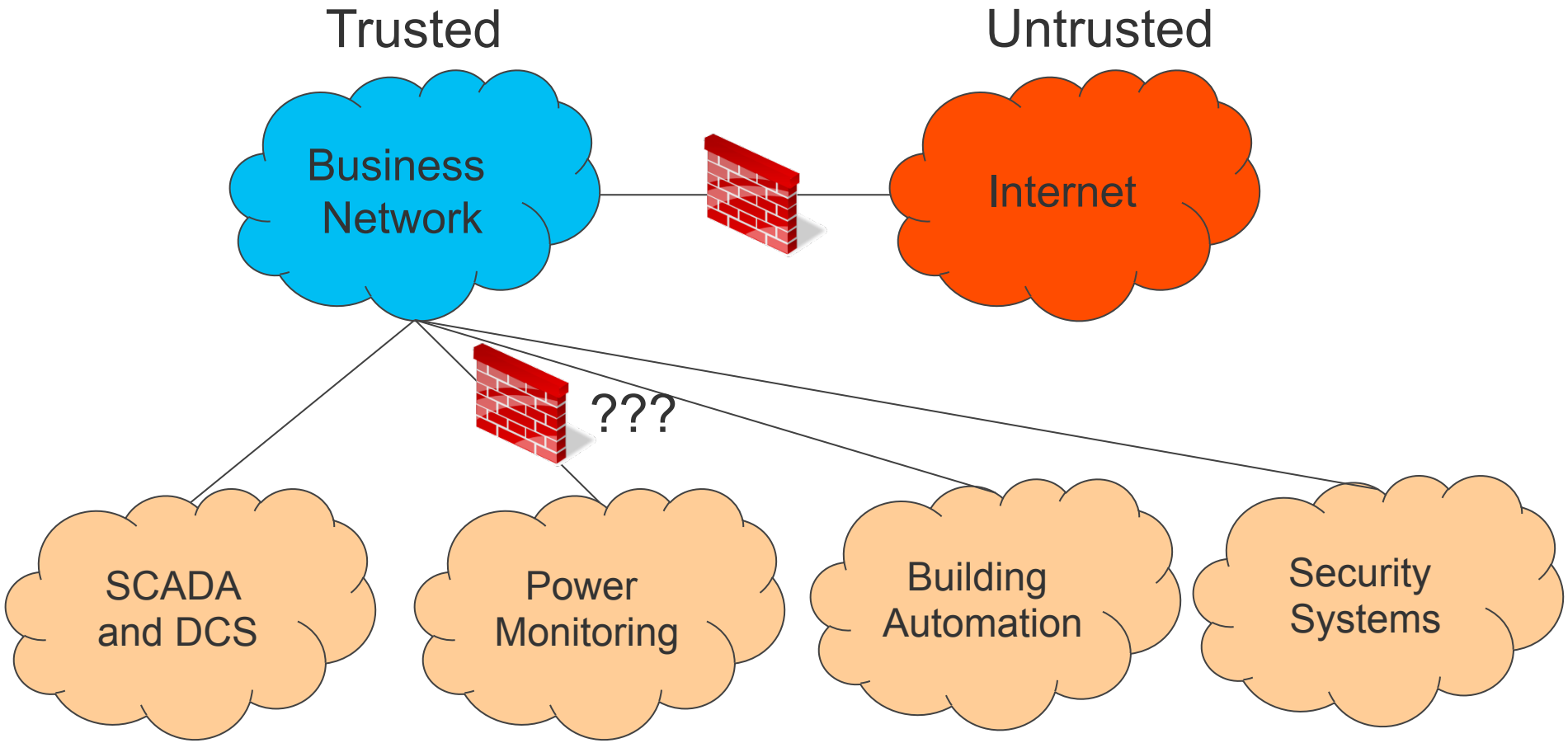
EAST BAY MUNICIPAL UTILITY DISTRICT

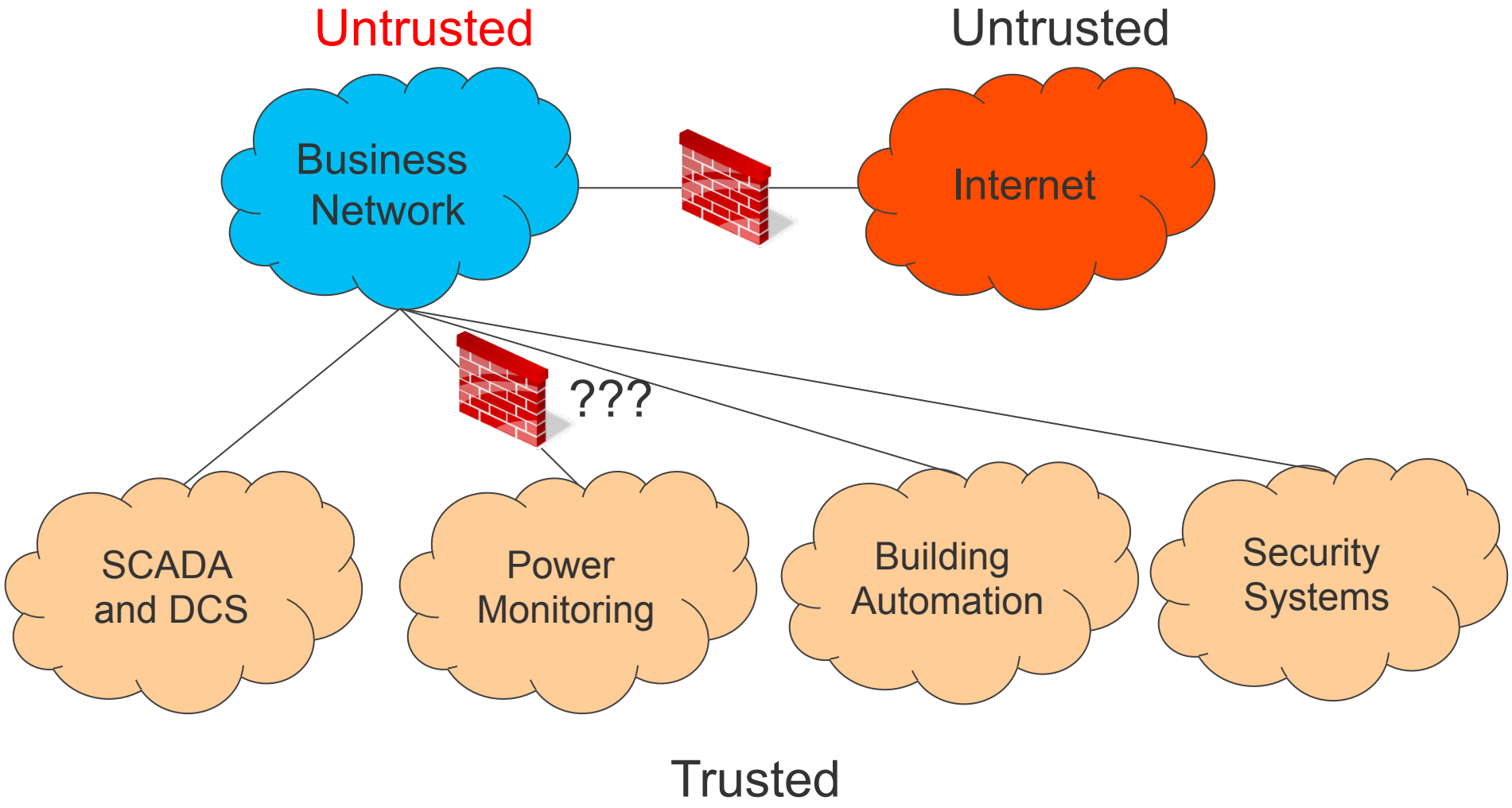
Implementing the NIST Framework and Cybersecurity Best Practices

October 2015

Business vs ICS Networks



Business vs ICS Networks



ICS Spear-Phishing Example

- Three pipeline companies participated
- Only the company name provided to researchers
- Goal: Compromise computers with remote access to the control system

Company	Online Employees Identified	ICS Related Employees Identified
A	346	23
B	206	49

ICS Spear-Phishing Example

I found this article today on Rockwell's site and was thinking it would be a good idea for all control system staff to take a look at it. Particularly those who work with FactoryTalk and Allen Bradley.

http://www.ab.com/en/pub/catalog/12762/2181376/1239781/2147816/print.html

Company	Online Employees Identified	ICS Related Employees Identified	Spear-Phish Success Rate
A	346	23	7 of 22
B	206	49	11 of 48

26% fell victim to spear-phishing attempts

Insecure By Design

"The pro's don't bother with vulnerabilities when attacking ICS. They use documented features of protocols and products."

Ralph Langner (of Stuxnet Fame)

- Worst vulnerabilities in ICS are not bugs, they are features
- Stuxnet took advantage of legitimate product features

Common Problems

- Hard-coded passwords
- Interfaces intentionally left in devices for future vendor access
- Client side security
  - Security works if you use their software
  - Can connect directly to device (e.g., Ethernet port)
- Communication between devices has no authentication
- Hard to physically secure geographically dispersed and unmanned systems

Operating System End of Life

Operating System	End of Mainstream Support	End of Extended Support
Windows XP	April 14, 2009	April 8, 2014
Windows 7	January 13, 2015	January 14, 2020
Windows 8	January 9, 2018	January 10, 2023
Windows 10	October 13, 2020	October 14, 2025
Windows 2000	June 30, 2005	July 13, 2010
Windows 2003	July 13, 2010	July 14, 2015
Windows 2008	January 13, 2015	January 14, 2020
Windows 2012	January 9, 2018	January 10, 2023

Microsoft Windows

Impact of a Compromise

- Simple: Take a component or system down or cause random changes
- Moderate: “Brick” the system requiring hardware replacement
- Advanced: Modify process in a high impact manner
- Ultra-advanced: Modify the process in a high impact manner that disguises the fact it was a cyber attack

Traditional Tools

- **Antivirus software**: Antivirus is based on identifying and blocking known malware
- **Network segregation**: Firewalls and air gaps doesn't address those who have a legitimate reason to access the ICS
- **Security patches**: Vendors may patch operating system but it may take years for the ICS vendor to fix the issue

What's Changed

- ICS traditionally less risky because they are not connected to IT networks
- "Security through obscurity"
- Traditional maintenance steps
  - Install
  - Don't touch unless it stops working
  - Replace when you can't get parts
- More risk today because integration of ICS with IT

Executive Order 13636

- Presidential Executive Order issued February 19, 2013
- Objective to **improve cybersecurity for critical infrastructure**
- Directed the National Institute of Standards and Technology (NIST) to develop a **Cybersecurity Framework**
- NIST finalized framework in February 2014

FEDERAL REGISTER

The President

Executive Order 13636—Improving Critical Infrastructure Cybersecurity

NIST Cybersecurity Framework

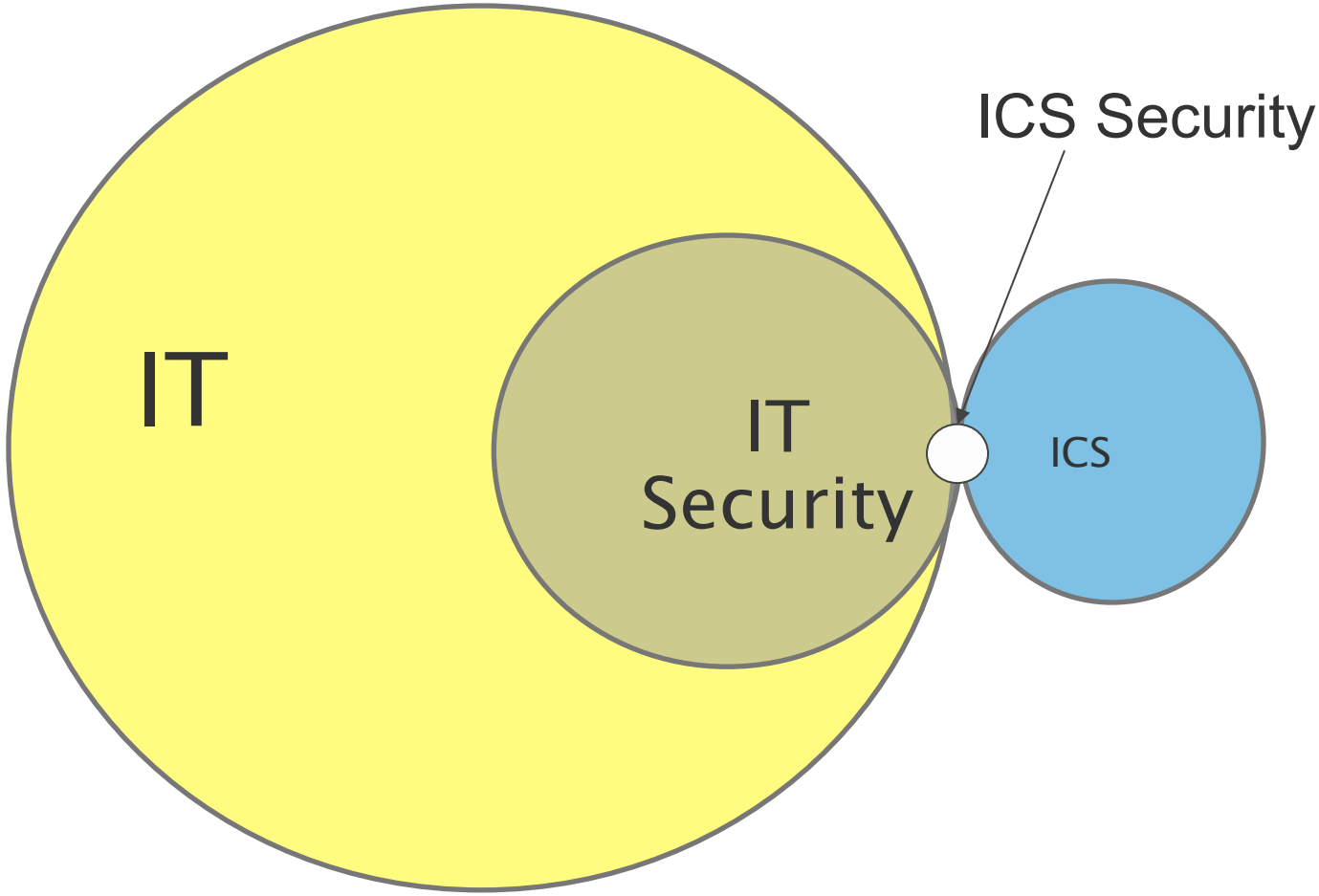
- Risk-based approach
- Three parts
  - Implementation tiers
  - Core: Industry standards, guidelines and practices
  - Profile

National Institute of Standards and Technology
U.S. Department of Commerce

Implementing Cybersecurity Framework

- How we implemented the NIST Framework
- Starts with selecting a vendor

ICS Security Expertise



How to Find a Vendor

- Consult ICS vendor for suggestions. Ideally, don't hire the vendor to perform the assessment.
- Identify firms based on their experience with ICS rather that typical IT cybersecurity
- Firms should have ICS network experience
- Ask for resumes of staff who will perform the assessment
- Don't disclose sensitive information in the RFP before having vendors sign an non-disclosure agreement
- Send the RFP to pre-selected vendors
- Informed vs uninformed assessment

Vulnerability Assessment

- Involve all stakeholders: Operations, Maintenance, Engineering and IT
- Form a Steering Committee
  - Provide policy direction
  - Establish reliability and recovery objectives
- Vulnerability Assessment starts with
  - Interview
  - ICS architecture review
  - Document and configuration review
  - Online testing
- Short-term (0 to 6 months) and medium-term (6 to 18 months) recommendations

Implementation Tiers

Tier 1	Partial	Risk management is ad hoc with limited awareness of risks
Tier 2	Risk Informed	Risk management processes in place but not integrated everywhere
Tier 3	Repeatable	Formal policies for risk management processes are in place
Tier 4	Adaptive	Risk management processes are based on lessons learned, embedded in culture

- Tiers provide context on how your organization views cybersecurity risk and the process to manage risk
- NIST recommends progressing towards higher Tiers
- Tiers ≠ Security

Framework Core

- Use the Framework Core to determine your **Current Profile** and **Target Profile**
- Framework does not tell you what your Target Profile should be
  - Target Profile based on risk management program
  - May find a risk is acceptable and do nothing
- Develop an **Action Plan** to close the gap between the Current and Target Profile
- Periodically repeat process

What Can You Do?
Short-Term Recommendations

- Don't be so nice – politely challenge why people need access
- Physically secure computers, devices and networks where possible
- Limit access to less physically secure locations
- Limit remote access
  - Implement two-factor authentication
  - Log all remote access attempts
- Train staff on cybersecurity awareness

What Can You Do?
Short-Term Recommendations

- Restrict access to USB ports
  - Disable USB ports
  - Don't connect phones, tablets or other devices to USB ports for charging
  - Scan dedicated USB drives before each use
- Restrict access to DVD/CD drives
- Limit wireless 802.11 access
- Setup dedicated ICS laptops
  - No business use
  - No Internet access

What Can You Do?
Medium-Term Recommendations

- Developing a cyber security policy
- Separate the ICS network from the business network (e.g., firewall, DMZ)
- Restrict physical access to ICS network and devices
- Protect ICS from exploitation (e.g., security patches, role-based privileges, antivirus)

System Upgrades and Patching

- System upgrades
  - Monitor end of life at least annually
  - Replace software and hardware prior to it reaching the end of life
- Patching
  - Perfect world everything is patched at least monthly
  - Reality – Patch quarterly
  - Focus on patching accessible computers and devices frequently

Recovery

- Set Recovery Time Objectives (RTOs)
- Develop plan to meet the RTOs
  - What is needed to restore the service?
  - How will they be recovered to meet the RTO?
- Do you have the data to recover?
  - Review your backup plans
  - Periodically verify backups are working
- Periodically verify RTO can be met

Redundancy Likely Won't Help

- ICS typically have redundancy
  - Active and hot standby servers
  - Multiple workstations
  - Backup control centers
  - Redundant networks
- Redundancy usually does not help against a cyber attack
  - Attack will compromise redundant system because it is identical and connected

References and Training

- NIST Guide to Industrial Control Systems Security
- NIST Framework for Improving Critical Infrastructure Cybersecurity
- AWWA Process Control System Security Guidance for the Water Sector
- AWWA Roadmap to Secure Control Systems in the Water Sector
- ICS-CERT references
- ICS-CERT training

National Institute of Standards and Technology
U.S. Department of Commerce

Questions