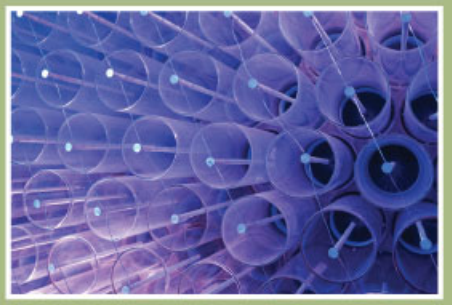
AMERICAN WATER

What Works in Securing Control Systems

Mike Firstenberg, CISSP
American Water
February 3, 2009



Don’t let this happen to you!

Common Needs

- **Need for Operations and IT to work together**
  - Understand the challenges
  - Leverage Expertise
- **Need "security baked in" to the product**
- **Need for better communication**
  - Internal company communications
  - Vendor partnership
  - Threat identification
- **Need to separate compliance and security**
- **Need to do it on a budget**
- **Need for cultural acceptance**

Need for Operations and IT to work together

- **Don’t wait for the other group to reach out as part of on audit, design, or incident.**
- **Start an internal working group comprised of design engineers, SCADA experts, IT people, et. al.**
- **Meet regularly, and meet face-to-face.**
- **Determine goals of the working group**
  - Standard Practices
  - Designs
  - Lay out touch points
  - If nothing else, find common ground

Need "security baked in" to the product

- Leverage the work done by others, specifically the Cyber Security Procurement Language for Control Systems published at http://www.msisac.org/scada/
- Talk with your vendors – hardware and software. Make sure your needs are addressed in their design life cycle(s).
- Work with your Procurement and Contract departments to get the appropriate inclusions in contracts with integrators.
- Communicate – make sure your vendors and integrators are aware of your company's preventative and directive controls that govern implementation and use of systems.
- Foster communication and partnerships among your vendors and integrators.

Need for cultural acceptance

- Aging work force. Most companies have now set up knowledge transfer procedures to ensure that the know-how does not walk out the door.
- There is a training effort underway to educate the new class
- If we can “bake security in” to the product, we can do the same for the personnel.
- Work with HR to add Security Awareness Training to the knowledge transfer processes already underway.

Value in Technology

- Look for products that integrate multiple layers of defense
- Unified Threat Management devices allow for integration of defense-in-depth to arenas that have previously been singular
- Utilize vendors that combine strengths from IT and SCADA/Process Control backgrounds
- Know your vulnerabilities and threats. Employ technology selectively to reduce risk in key arenas.
- Use audits effectively
- Integrate system hardening processes with effective change control toolsets.

Communicate outside your organization

- Have a relationship with law enforcement in place. When an incident does occur should not be the first time you meet.
- Develop communications channels with suppliers (chemical, electric utilities, etc.). Be ready to understand relationships.
- Participate in knowledge sharing communities.
- Publically promote your vendors when they are supporting the cause.

Be Ready

- Have your Incident/Response, Disaster Recovery and Business Continuity Plans and Procedures documented and available
- Must include all contact information
- Don’t expect it to work if you have never tried it – run “war game” excercises.
- Different threats and vulnerabilities require different responses. Be aware that no single plan of action can fit all potential scenarios.

Contact Information

Michael H. Firstenberg, CISSP
American Water - Security Operations
mike.firstenberg@amwater.com
office 856.566.4020
mobile 856.296.5647