



AMERICAN WATER

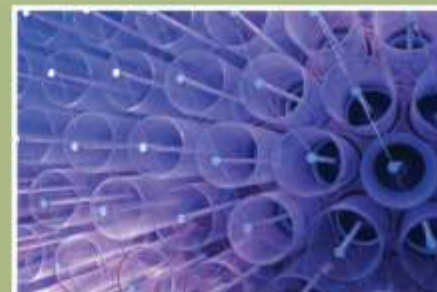
Cyber Security Initiatives and Issues

NARUC Summer Committee Meetings

Robert Schreiber, CISSP, CISA

Director, Client Services and Security Operations ITS

July 19, 2009



Water Utility – History of SCADA

- **Yesterday**
 - We were isolated and proprietary
- **Today**
 - Moving from serial to Ethernet/IP communications
 - Introducing IT based communication protocols (e.g. HTTP)
 - Increasing reliance on open protocols (Modbus/IP, OPC, etc)
 - There is an increased demand to access more data
 - Data used for business intelligence leads to more connections
 - Standardizing on computer operating systems

Cyber Threats to SCADA

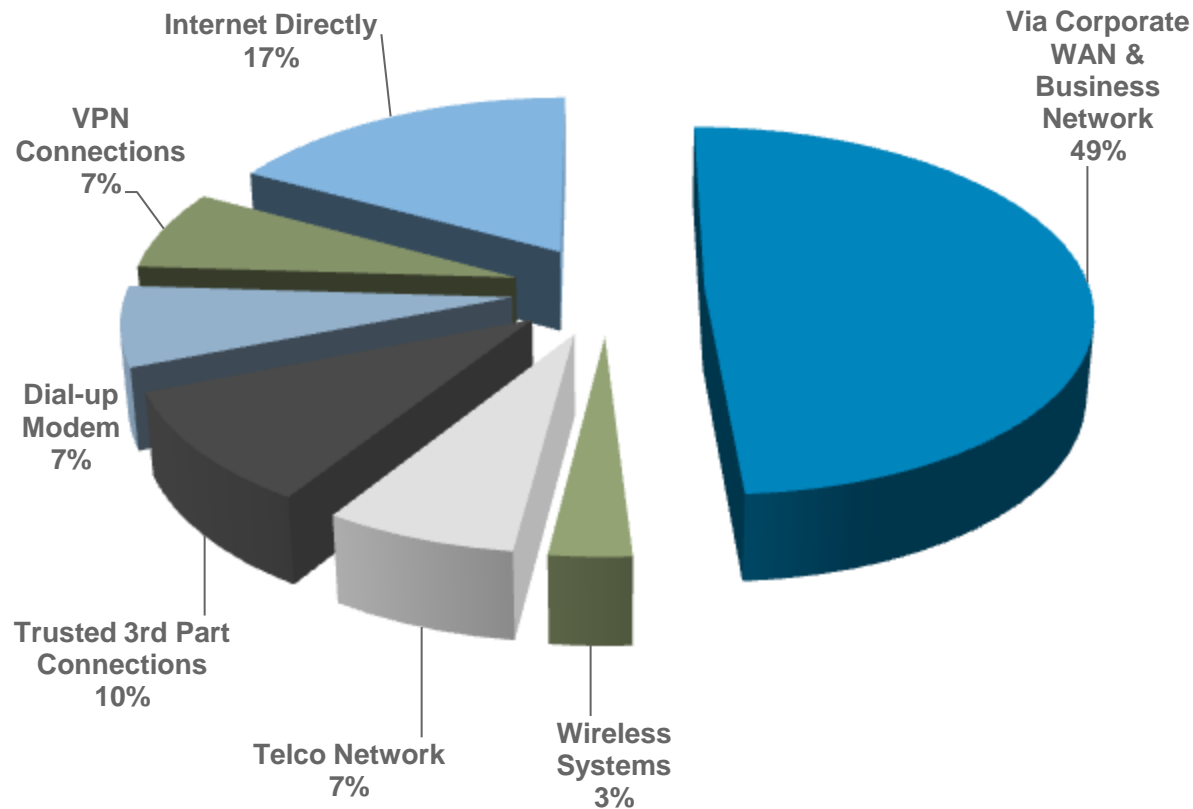
- **Hacker, Cracker**
- **Cyber Criminal**
- **Terrorist**
 - State Sponsored
 - Non-State Sponsored
- **Industrial Espionage**
- **Insiders**
 - Poorly Trained
 - Disgruntled
 - Negligent
 - Malicious
 - Terminated employee
 - Dishonest



Source: Alan Paller, SANS Institute, SCADA Summit 01/17/08

Industrial Security Incident Database

External Attacks on Control Systems



Source: Eric Byres, P. Eng, Byres Security, Inc, 05/08/08

Security Incidents in the Water Industry

- SALT River Project SCADA Hack
- Maroochy Shire Sewage Spill
- Software Flaw makes MA Water undrinkable
- Trojan/Keylogger on Ontario Water SCADA System
- Viruses Found on Auzzie SCADA Laptops
- Audit/Blaster Causes Water SCADA Crash
- DoS Attack on Water System via Korean Telecom
- Penetration of California Irrigation District Wastewater Treatment Plant SCADA
- SCADA System Tagged with Message, "I enter in your server like you in Iraq."
- SCADA Breach in Harrisburg, PA by an external hacker

Source: Guy Richards, Institute of Engineering and Technology, 11/08/08

Security Incidents in the Water Industry


Good Morning America | World News | 20/20 | Primetime | Nightline | This Week | ABC News Now | i-Caught

Search GO

Home | News Brief | World | U.S. | Investigative | Politics | Money | Health | Entertainment | ESPN Sports | SciTech | Law | Travel | More

THE BLOTTER

Home > [Brian Ross & The Investigative Team](#) > [The Blotter](#)



BRIAN ROSS
THE INVESTIGATIVE TEAM

Editor: Simon Surowicz

Subscribe to 'The Blotter'

BRIAN ROSS REPORTS

-  Despite Downturn, Lobbyists Raking In Record Revenues
-  Pressure Mounts on Renzi to Resign
-  2nd McCain Official to Face Federal Charges
-  Ameriquest Owner to Quit Post as Ambassador to the Netherlands
-  Cop Shooter 'Loco

« Military Reservist Wins Big in Court | Main | Not Enough People, Not Enough Training: Airport Screeners Continue to Miss Hidden Weapons »

Hackers Penetrate Water System Computers

October 30, 2006 3:15 PM ✉ Email
🖨 Print
➦ Share

Richard Esposito Reports:



A foreign hacker who penetrated security at a water filtering plant near Harrisburg, Pa., is under investigation by the FBI for planting malicious software capable of affecting the plant's water treatment operations, ABC News has learned.

The hacker tried to covertly use the computer system as its own distribution system for e-mails or pirated software, officials told ABC.

"The concern was high because it is a computer that controls an important infrastructure system, and if, for some reason, it caused it to fail, it would have disrupted service," said Special Agent Jerri Williams of the FBI's Philadelphia field office.

THE BLOTTER RECOMMENDS [The Columbus Day](#)

in 2007

127 Million

had their personal info exposed

Based on information provided by the Identity Theft Resource Center

Enroll Now



LifeLock
Guaranteed Your Good Name
www.lifelock.com

Sponsored Links

Hugh Downs Reports:
Common pain pill raises your blood pressure. Drug Makers Aren't Talking
Healthsecrets.com

Lose 25 lbs in 2008!
Get your Free Diet Patch. Oprah & CBS featured Hoodia, a dieting miracle!
CurbYourCravings.com

Southern Living - Moving
Charlotte, NC Home Searches, Schools, Taxes, Relocation information
www.LocateCharlotteHome.com

Buy a link here

How Cyber Events can affect Water Operations

- **Compromising a SCADA system can result in the following:**
 - Interfere with the operation of water treatment equipment; chemical over or under-dosing.
 - Disable service, reduced pressure flows of water into fire hydrants, or overflow of untreated sewage into public waterways.
 - Block data or send false information to operators to prevent them from being aware of conditions or to initiate inappropriate actions.
 - Change alarm thresholds or disable them completely
 - Lockout access to system accounts
 - Although many facilities have manual backup procedures in place, failures of multiple systems may overtax staff resources - even if each failure is manageable in itself
 - Be used as ransomware

Universal Security Challenge

“The problem is that IT people don’t understand SCADA and SCADA people don’t understand security” *[Gary Sevounts, Director, Symantec]*

Need for Operations and IT to work together

- **Don't wait for the other group to reach out as part of an 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 into 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.

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 Prepared

- **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” exercises.**
- **Different threats and vulnerabilities require different responses. Be aware that no single plan of action can fit all potential scenarios.**