

# ICSJWG CONTROL SYSTEMS BRIEFING



MICHAEL J. KNAPP

Sr. Solutions Architect, CISSP, CEH, MSCE, SEC+



# McAfee – Brief Overview



## **In 2010 McAfee created a separate Energy Vertical**

McAfee's Team consists of 4 dedicated Account Managers, a Director and 3 Engineers covering North America..



## **McAfee is working with Control System manufactures**

McAfee is taking our Commercial off the shelf (COTS) technologies to manufactures to test our products and enhance them to better understand control systems protocols and behaviors unique to the environment.



## **McAfee is focusing on bridging the gaps between IT & Control System groups within organizations**

As these two historically separate groups are being brought together McAfee is attempting to assist bridging the groups to make them more security efficient.

# Understanding the Threat Landscape



Why are these important :  
Because you don't want  
to become a Headline.

“California Canal Management System Hacked”

IDG News – December 2007

“Report: US Air-traffic Control Systems Hacked”

CNET – May 2009

“CIA Official: North American Power Grid Systems Hacked.”

Government Executive.com – January 2008

“Hackers Infiltrate Large Hadron Collider and mock IT security.”

Telegraph UK

“Experts hack Power Grid in no time.” Basic social engineering and browser exploits expose electric production and distribution network. - Network World

# Understanding the Threat Landscape



“While only about 10 percent of industrial control systems are actually connected to the Internet, these systems that run water, wastewater, and utility power plants have suffered an increase in cyber-security incidents over the past five years.” – Dark Reading

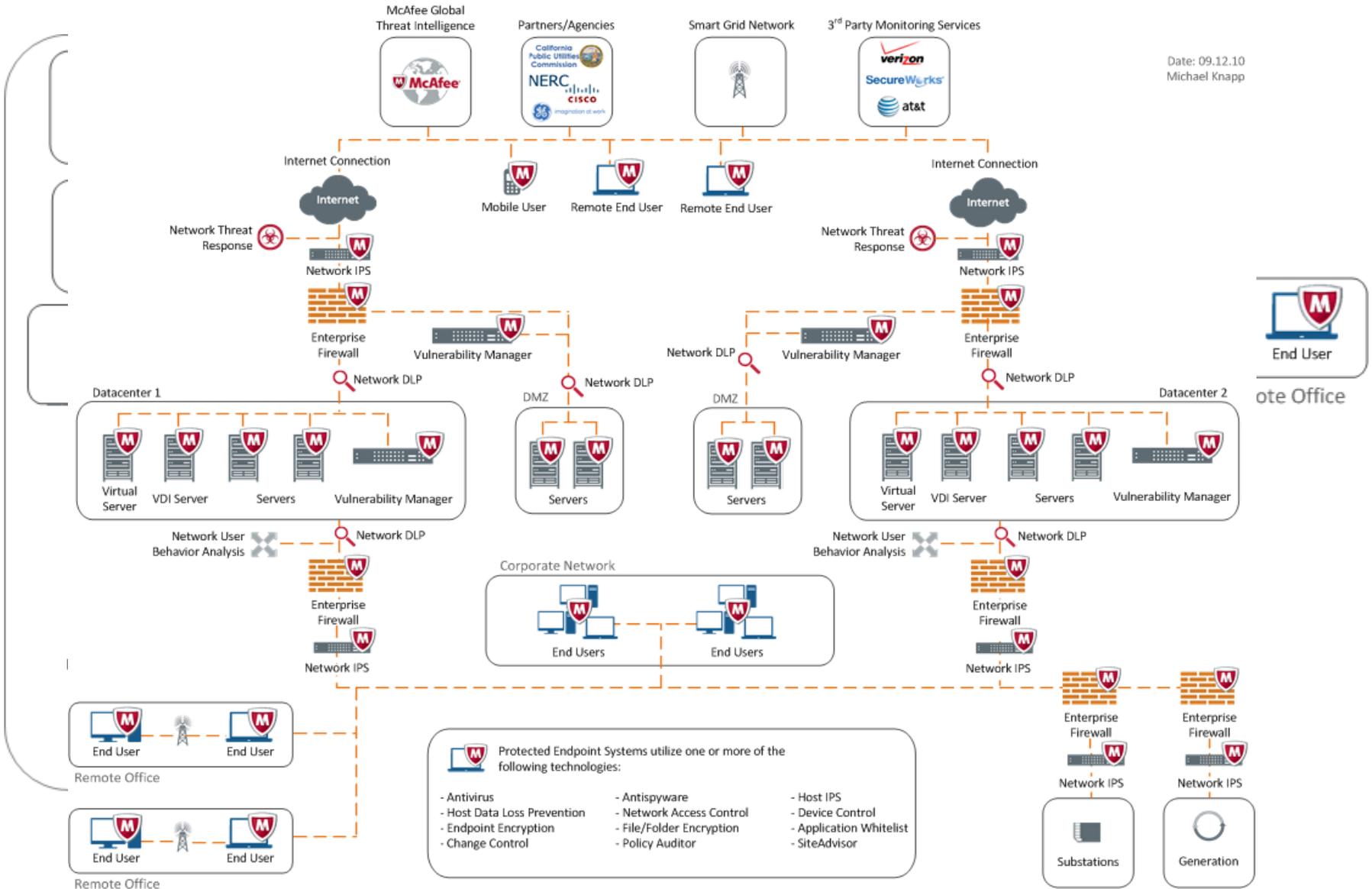


A report based on data gathered by the Repository of Industrial Security Incidents (RISI) database provides a rare look at trends in malware infections, hacks, and insider attacks within these traditionally cloistered operations. Cyber-security incidents in petroleum and petrochemical control systems have declined significantly over the past five years--down more than 80 percent--but water and wastewater have increased 300 percent, and power/utilities by 30 percent, according to the 2009 Annual Report on Cyber Security Incidents and Trends Affecting Industrial Control Systems.

# The New Control System Network...



Date: 09.12.10  
Michael Knapp



# Common Control System Issues



**PROBLEM:** We have to maintain connections from our Control Systems network to our IT department, partners, vendors, government agencies or regulatory bodies. How do I secure that?



A layered approach is necessary anytime you open a network up to other entities permitting access as needed.



Determine and rank your security priorities such as Data Loss, Malware, Regulatory Compliance or Uptime.



Organizations should have a mechanism to detect and deal with Advanced Persistent Threats targeting them.

# Common Control System Issues



**PROBLEM:** Many Control Systems devices that are coming online use Windows or open source operating systems. We are concerned about running typical IT security tools on these systems.



Application Whitelisting takes a different approach to protecting systems by only allowing authorized applications to execute.



Some Application Whitelisting versions can be easily deployed as they learn what is running on the system automatically.



By permitting only known good applications you do not have to consistently update signature files.

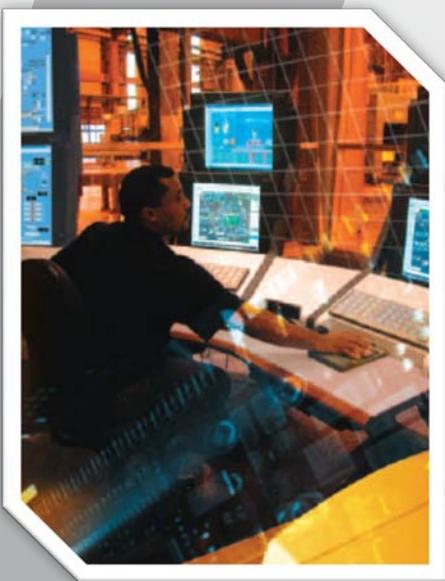


You are *potentially* not exposed to compliance issues due to delays in manufacture testing of security updates.

# Common Control System Issues



**PROBLEM:** How do I control changes made to my Control Systems environment to mitigate accidental and malicious modifications?



A Change Control technology blocks all changes except for those Users, Tools or Publishers that you've Authorized.



The Lockdown process of a system would be automatic and wouldn't require complex configurations.



Systems could be audited against a Base Line image looking for any deviations.

# Common Control System Issues



**PROBLEM:** For business continuity reasons I have to connect my control system network to my IT's network. How do I secure this and prevent native control system protocols from leaving the network.



Firewalls that understand control systems protocols and support restricting or blocking their traffic as needed.



Network Intrusion Prevention technologies which support protocol decodes such as ICCP, ModBUS and DNPv3.



The use of Geo-location aware security solutions help reduce security exposure.



Data Diodes provide an excellent secure 'One-Way' communication path for moving data.

# Common Control System Issues



**PROBLEM:** Some management workstations within the control systems network get connected to external networks then reconnect.



No Tech method would be to not install IT or external connections and backing this up by prohibiting thru policy.



Advanced Host IPS & Host Firewalls allow you build permit/deny policies based on where they are connected.

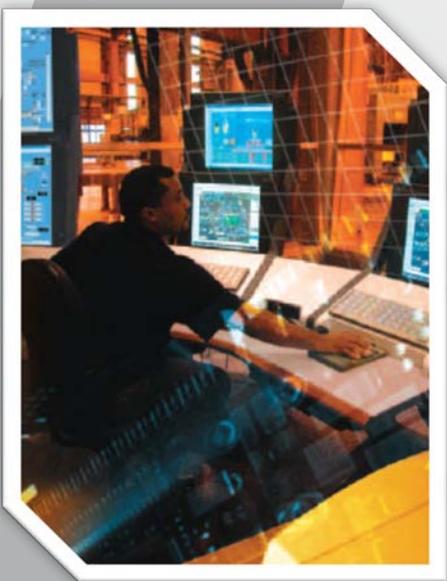


Active Technology which detects & alerts on new devices being connected to the control systems network.

# Common Control System Issues



**PROBLEM:** For those that have segmented their control systems network they have been forced to move data between networks using removable media and other means.



Device Control Technology allows you to specify what peripherals can be connected to a specific device.



Authorize only removable devices which you trust where they are sourced from.



Content written/read from removable devices should be encrypted as well as scanned for malicious code.

# Common Control System Issues



**PROBLEM:** How do I know if my systems are compliant or not to my security policy or to an external regulatory requirement?



The use of Host Based auditing tools allows administrators to verify systems are still configured in a certain way.



The use of a File Integrity Monitoring technology would provide a 'Play by Play' log of any changes made to a system.



Use a technology such as Change Control to prevent configuration drift.

# Better Defense Using Mitigating Technologies



- Application Whitelisting
- Change Control/Prevention
- Device & Peripheral Control Technologies
- Host IPS/Firewall with Location Aware Capabilities
- Network IPS & Firewalls that understand Control System Protocols





# Questions & Answers

# McAfee Resources Available to You...

A large, stylized red number '7' graphic is positioned on the left side of the slide. It is composed of a thick red line that forms the shape of the number. Three white circles with a red glow are placed along the vertical stem of the '7'. The background of the slide is a light gray, and the left edge features a photograph of a modern glass skyscraper against a blue sky with light clouds.

Whitepapers & Solution Briefs

Trials of various technologies which may provide compensating controls for your environment.

Ability to talk to McAfee Security Engineers regarding specific needs or requirements.

# McAfee In the Crossfire Report (2010)



- Survey of 600 IT and security executives from critical infrastructure enterprises across seven sectors in 14 countries
- Reported cost of downtime from major cyber attacks to Critical Infrastructure exceeds **U.S. \$6 million per day**
- Intangible costs – **critical operational failures, loss of life, loss of reputation**, etc. difficult to calculate
- More than half of respondents said they had experienced **Large-scale denial of service attacks** by high level adversary like organized crime, terrorists or nation-state (e.g. like in Estonia and Georgia)
- 59% respondents believed that representatives of **foreign governments had already been involved in targeted infiltrations of critical infrastructure**

# Thank you!



If you provide us your contact information you will be entered into a drawing to win a McAfee Encrypted USB thumb drive.

**FREE**

Simply provide a business card or write down the following contact information:

- Name
- Address
- Phone Number
- Email Address
- Any Resources You Want





**McAfee®**

