Kansas City Plant
National Security Asset

Malcolm Baldrige National Quality Award

System Security
"It's Not About Compliance Anymore!"

The Kansas City Plant is operated and managed by Honeywell Federal Manufacturing & Technologies, LLC, for the NNSA.

NNSA National Nuclear Security Administration

Kansas City Plant
National Security Asset

Disclaimer

- My presentation is meant to:
  - Stimulate thought
  - Move away from “That’s the way we have always done it”
  - “Compliance” and “Risk Mitigation” can really work together
  - Share Best Practices
- My presentation is also
  - My conclusions based on material I read daily and events I have analyzed over the past 5 years.

- So I ask that you don’t take it personal.

Kansas City Plant
National Security Asset

WHO AM I ??????

WHO ARE YOU ?????

Malcolm Baldrige National Quality Award

Kansas City Plant
National Security Asset

Agenda

- Threats
  - What Threats????
  - What are you helping to protect against and from what?
- Risk
  - Is there?
- Mitigation
  - Does being in Compliance Help?
- Strategies
  - Some thoughts for the future.

Malcolm Baldrige National Quality Award

Kansas City Plant
National Security Asset

What Threats?

- Employees continue to put data at risk
- Spy Threats Highlighted
- Complexity of Systems could be our Achilles Heal
- Identity Theft Epidemic
- Social Networks Open Door to Data Leaks
- Cell Phones put Company Secrets at Risk
  - Banking apps
- Facebook apps transmit personal info

National Security Institute news headlines. – http://nsi.org/

Malcolm Baldrige National Quality Award

Kansas City Plant
National Security Asset

Do we need to worry?

- ***"These guys on the other side of the table know every bottom line on every significant negotiating point. They had to have gotten this by hacking into [the company's] systems"***

Dr. Joel Brenner – National Counterintelligence Executive

Malcolm Baldrige National Quality Award

Kansas City Plant
National Security Asset

Do we need to worry #2?

- The cyber threat has become one of the most serious economic and national security challenges we face. America's competitiveness and economic prosperity in the 21st century will depend on effective cybersecurity. Every Internet user has a role to play in securing cyberspace and ensuring the safety of ourselves, our families, and our communities online. www.dhs.gov

Malcolm Baldrige National Quality Award

Kansas City Plant
National Security Asset

What Do You Worry About?

Malcolm Baldrige National Quality Award

Kansas City Plant
National Security Asset

Here are my thoughts!!

- External devices
  - USB Drives, Supply Chain
- Mobile Computing
  - Laptops, PDA, iPhones, BlackBerry, VPNs
- Social Engineering
  - Using that which most of us enjoy, DriveBys
- Cyber Espionage
  - Stealing our Technology, legal documents, email
- Cyber Terrorism
  - Control Systems

Malcolm Baldrige National Quality Award

Kansas City Plant
National Security Asset

My BIGGEST Fear is!!!

- THE INSIDER
  - Unwitting
  - Willing
  - Disgruntled

- Based on all the info I have read, I would conclude that over 85% of all compromised that lead to lose of data were the result of an insider.

Malcolm Baldrige National Quality Award

Kansas City Plant
National Security Asset

All of this contributes to:

Advance Persistent Threat

- Refers to advanced and normally clandestine means to gain continual, persistent intelligence on an individual, or group of individuals such as a foreign nation state government. While the APT is more commonly thought of a being an article of the computer era, it has existed since the beginning of intelligence gathering and long before the invention of the computer or internet.

Malcolm Baldrige National Quality Award

Kansas City Plant
National Security Asset

SO WHAT!

- **Reconnaissance**
  - Social Engineering
  - Mobile Computing
  - Insider
- **The Initial Breach**
  - Social Engineering
  - Mobile Computing
  - Insider
  - External Devices
- **Get a Network Backdoor**
  - Social Engineering
  - Mobile Computing
  - Insider
  - External Devices
  - Cyber Espionage
  - Cyber Terrorism

Malcolm Baldrige National Quality Award

Kansas City Plant
National Security Asset

SO WHAT!

- **Grab User Credential**
  - Social Engineering
  - Mobile Computing
  - Insider
  - External Devices
  - Cyber Espionage
  - Cyber Terrorism
- **Install Attack Utilities**
  - Social Engineering
  - Mobile Computing
  - Insider
  - External Devices
  - Cyber Espionage
  - Cyber Terrorism
- **Data Ex-filtration**
- **Maintain Persistent**
  - APT

Malcolm Baldrige National Quality Award

Kansas City Plant
National Security Asset

What's at Risk???

- Reputation
- Competitive Edge
- National Security
- Employees' well being
- Consumers
- Our Economy

- $$$$$$$$$$$$$$$$$$$$$$$$$$$

Malcolm Baldrige National Quality Award

Kansas City Plant
National Security Asset

So What does all of this have to do with Compliance!!!

- Compliance Checklist.
  - Are you patched?
  - Do you have a firewall in place?
  - Do you have Antivirus installed?
  - Do you have all your Paper work in order?
  - Do you have an inventory system for all your computers?
  - Do you have a configuration management process?
  - Do you use strong passwords?
  - Have you implemented a “Separation of Duties” process?
  - Do you have a training and awareness program?

Malcolm Baldrige National Quality Award

Kansas City Plant
National Security Asset

But, It all won't work without:

- Partnering – Internal – This includes Compliance
- Knowing where you are vulnerable
- Know what assets need to be protected, along with operational risk
- Fix or mitigate vulnerabilities
- Understand your adversaries
- Be prepared to prevent an attack or respond quickly
- Prevention is preferred, rapid detection and response a must
- Have a fall back plan
- Communicate with business partners

Malcolm Baldrige National Quality Award

Kansas City Plant
National Security Asset

Reduce Risk while checking the Compliance Box!

- Control the user and raise awareness
- Perform reputation ranking on behavior
- Focus on outbound traffic
- Understand the changing threat
- Manage the endpoint

Log EVERYTHING!!!!!!

Malcolm Baldrige National Quality Award

Kansas City Plant
National Security Asset

Final Thought

- To secure our infrastructure, no matter what business we are in, it is a team effort. It involves everyone in every part of the organization. It's not just about having technology and policies in place. It is about everyone knowing their part to ensure the security of our resources. It's knowing how to act/react to a situation.