

Cybersecurity within the Applications of Environmental Standards

By Erik Buschardt
Webster University
December 2016

Roadmap Goals and Objectives



- List 16 Specific DHS National Critical Infrastructure Sectors.
- Describe Components and Critical Assets Specific to that Sector.
- Explain Cybersecurity Threats and Known Vulnerabilities.
- Introduce Environmental Alternatives that may address these threats.
- Describe Controls and Countermeasures to these Threats and/or Alternatives.

1. The Chemical Sector

Critical Assets Include:

- Corporate Laboratories
- Manufacturing Plants
- Distribution Sites

Cybersecurity Threats:

- Sabotage of Chemical Plants
- Espionage of Trade Secrets

Environmental Alternatives:

- Organic, Non-growth-hormones (Agricultural)

Controls and Countermeasures:

- Physical Security
- Classification of Documents, Least Privilege



2. The Commercial Facilities Sector

Critical Assets Include:

- Corporate Real Estate Property
- Tourism Hotspots
- Commercial Centers such as malls

Cybersecurity Threats:

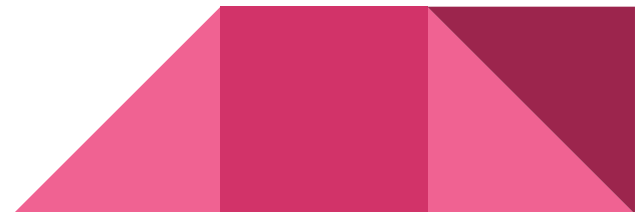
- Data Breach (Home Depot, Target, et al.)
- Identity Theft (Amazon, online shopping)

Environmental Alternatives:

- Sustainable Power and Utility Sources

Controls and Countermeasures:

- Maintain a physical presence during holiday rushes
- Better Encryption Technologies, Upgrade POS systems.



3. The Communications Sector

Critical Assets Include:

- International Telecommunications
- Internet Traffic and Streaming
- Telephone Lines, Cables, Hubs

Cybersecurity Threats:

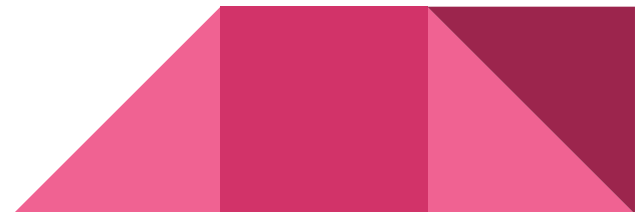
- Data Theft (both residential and commercial)
- DDOS attacks, Man In The Middle
- Physical Blackouts for any reason

Environmental Alternatives:

- Redundant Sustainable Power and Utility Sources (solar/wind)

Controls and Countermeasures:

- Encryption and Redundancy.



4. The Critical Manufacturing Sector



Critical Assets Include:

- Sourcing sites such as mines and oil fields
- Industrial Grade Machinery / Robotics
- Fabrication Plants and Factory Floors
- All Points of Distribution

Cybersecurity Threats:

- Industrial Control Systems Cybersecurity Emergency Response Team (ICS-CERT):
Malware-based attacks doubled in 2015.
- Outdated Hardware and Software solutions on factory floor (built in a previous era of computing, COBOL and FORTRAN).

Environmental Alternatives:

- Recycle Metals such as Aluminum, Plastics, Glasswares

Controls and Countermeasures:

- Isolate Sensitive Equipment from Corporate Network.



5. The Dams Sector

Critical Assets Include:

- Dam Structures and Reservoirs
- Internal Generators, Turbines and Plants
- Downstream Communities

Cybersecurity Threats:

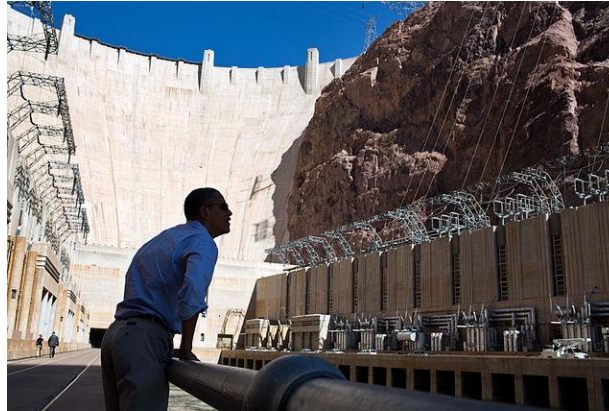
- SCADA-type malware payloads
- Theft of Intellectual Property

Environmental Alternatives:

- Maintain Balance of Hydraulic Flow to balance needs of surrounding ecology, vs. needs of communities served.

Controls and Countermeasures:

- Maintain Physical Security.



6. The Defense Industrial Base Sector



Critical Assets Include:

- Classified Research Facilities
- Manufacturing Plants
- Test Airfields and Bases

Cybersecurity Threats:

- Intellectual Property Theft by State Actors such as Russia and China

Environmental Alternatives:

- Equipment can run on renewable sources

Controls and Countermeasures:

- Maintenance of Classification System,
System of Least Privilege.



7. The Emergency Services Sector

Critical Assets Include:

Hospitals, Clinics, Disaster Centers
Support Vehicles such as ambulances, helicopters, Wildfire vehicles and aircraft

Cybersecurity Threats:

DDOS attacks against internal communications systems
Social Engineering and Populist-based Hacktivism
Delivery of Criminal Ransomware

Environmental Alternatives:

Reduction in use of Hazardous Materials within Industrial Sectors will help to reduce overall emissions and reduce threat of life to first responders.

Controls and Countermeasures:

Interaction with the Community, Access to Real-Time Data.



**American
Red Cross**



8. The Energy Sector

Critical Assets Include:

Generation Plants (coal, oil, solar, wind, etc)
Power lines and Transmission Stations, etc.

Cybersecurity Threats:

Internal Sabotage, Physical Breaches
48% of IT execs believe an attack is imminent within the next three years for the Energy sector.

Environmental Alternatives:

Solar, Wind, Hydro (ocean-wave) plants.

Controls and Countermeasures:

Increased Physical Security, Encryptions against malware payloads
such as STUXNET attack



9. The Financial Services Sector



Critical Assets Include:

Retail Banks, Financial Centers, Wall Street, US Mint/Treasury

Cybersecurity Threats:

Internal Embezzlement
Consumer Identity Theft
Credit Card Fraud, Income Tax Fraud

Environmental Alternatives:

Digital Currency to reduce paper notes and coinage
Organic and recycled materials to be made into currency

Controls and Countermeasures:

More Transparency to Reduce Corporate Crimes such as Enron (2001-2) and Great Recession (2008-9)



10. The Food and Agriculture Sector

Critical Assets Include:

Restaurant, Grocery Stores, Food manufacturing plants, cold storage and refrigeration.

Cybersecurity Threats:

Sabotage of storage depots and processing centers

Environmental Alternatives:

“Smart Farming” - Using GPS to coordinate planting and harvesting times for higher yields.

Controls and Countermeasures:

Increased Encryption Technologies, Physical Security Presence especially in Rural areas.



JOHN DEERE



11. The Government Facilities Sector



Critical Assets Include:

Overseas Embassies, Government Buildings
National Parks, Military Bases, Government-Run Facilities, Etc.

Cybersecurity Threats:

Foreign Espionage
Data manipulation and hacking

Environmental Alternatives:

Similar to Commercial Facilities:
Use of Sustainable and Renewable Power Supply and Utilities



Controls and Countermeasures:

Antiterrorism controls in place at federal sites.

12. The Healthcare and Public Health Sector

Critical Assets Include:

Hospitals, clinics, corporate offices, prescription plants, etc.

Cybersecurity Threats:

Theft of trade secrets, industrial espionage

Physical plant sabotage (killing the power, for example).

Environmental Alternatives:

Backups to include not diesel but solar, wind

Controls and Countermeasures:

Physical Security measures in place,

Increased Situational Awareness by Employees.



13. The Information Technology Sector

Critical Assets Include:

Data Center Hardware, Software, Routers, Hubs,
Internet infrastructure, Communication Satellites

Cybersecurity Threats:

Theft of Corporate Intellectual Property
Theft of Consumer Data
Distribution of Malware Payloads

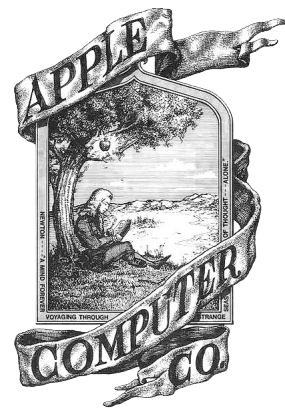
Environmental Alternatives:

Recycled power sources, efficient use of power generation for
worldwide data centers (Google Green)

Controls and Countermeasures:

Encryption in place, Physical presence at Critical Assets.

Easter Egg: Apple's Original Logo (1976)



14. The Nuclear Reactors Sector

Critical Assets Include:

Nuclear Plants and surrounding areas

Cybersecurity Threats:

Sabotage of site equipment and facilities

Environmental Alternatives:

Renewable Sources, reduction of nuclear fuels and waste, Fusion.

Controls and Countermeasures:

Policy Awareness maintained for all staff.



15. The Transportation Sector

Critical Assets Include:

Road, Rail, Airports, Seaports, etc.

Cybersecurity Threats:

Physical Destruction or terrorism event

Environmental Alternatives:

Alternative fuels such as electricity or solar

Controls and Countermeasures:

Upgrade firmware in vehicles



16. The Water and Wastewater Sector

Critical Assets Include:

Water Supply Depots, Sewage plants, (see Dams Sector), pipelines, power outlets in event of brownouts or blackouts

Cybersecurity Threats:

Industrial Sabotage of equipment and/or facilities

Environmental Alternatives:

Redundant processes, “rain gardens” to reduce stormwater pollution

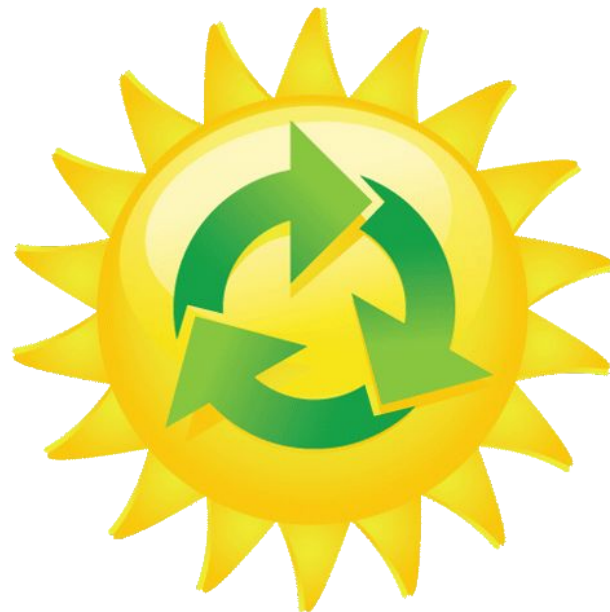
Controls and Countermeasures:

Maintain policies and procedures to prevent a terrorism event.
Isolate and carefully/safely resolve, (both in cases of water treatment and wastewater treatment).



Conclusions and Final Thoughts

- The identification of critical assets within a sector is important for a company or organization to identify.
- Environmentally-sensitive enhancements to manufacture or outsourcing of raw goods will help mitigate conflict of resources.
- Increased physical security will eliminate some threats such as insider exploitation, (Office Space, 1999).
- Other malware payloads can be mitigated by user education and improvements in network architecture.
- Threats are increasing daily. It's a good time to be a cybersecurity professional. Job Security!



Final Thoughts and Questions

Thank you for your time and attention.

