Energy Company Boards, Cybersecurity, and Governance – Collected Materials[1]

http://www.EnergyCollection.us/457.pdf - this collection

http://www.EnergyCollection.us/456.pdf - associated paper on Energy Boards and Governance for Cybersecurity

The purpose of this collection is to serve as a reference document to various materials that may be of interest to those responsible for or researching the subject of Cybersecurity and Governance within the context of a Board of Directors.

The organization of the document is simply alphabetical. Articles and reports are generally referenced with the first 3 words in the title of the article or report for ease of finding the reference here. Terms and names of groups are simply inserted alphabetically in the continuous list. And so on.

English "language articles" that were used in titles of various documents are ignored for purposes of alphabetization in this document.

Most of the material has been replicated with a link to the www.EnergyCollection.us site (maintained by the producer of this collection) to ensure availability. There is a renewed effort to quote the original site as well.

This Collection is meant to be a companion documents to a Paper: "Energy Company Boards, Cybersecurity, and Governance" which discusses these subjects from a Board responsibility perspective. The paper can be downloaded at http://www.EnergyCollection.us/456.pdf

With a bit less than 100 pages of references, Board members may face the question – Where do I start? These references are suggested starting points:

- ***NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 3.0*** – NIST Special Publication 1108R3 - Framework 3.0 updates the plan for transforming the nation's aging electric power system into an interoperable smart grid—a network that will integrate information and communication technologies with the power-delivery infrastructure, enabling two-way flows of energy and communications. ***Beginner's Guide*** – http://www.EnergyCollection.us/Companies/NIST/NIST-Framework-Roadmap-1108R3-B.pdf

If you have a good reference that should be included here – email PaulFeldman@Gmail.com [2]and it will be included.

[1] Last updated July 9, 2014

Table of Contents with Links

[2] LinkedIn - www.linkedin.com/in/paulfeldman/

- Tom Alrich's Blog - http://tomalrichblog.blogspot.com/

Boardroom Cyber Watch Survey - 2014 Report

Bound to Fail: Why Cyber Security Risk Cannot Simply Be "Managed" Away

Brookings Center

- Bound to Fail: Why Cyber Security Risk Cannot Simply Be "Managed" Away
- Brookings Center for 21st Century Security and Intelligence

Bulk Power System Cyber Security

The Business Case for Application Security – HP part 2

C-Cubed Program – from DHS

California

- Cybersecurity and the Evolving Role of State Regulation: How it Impacts the California Public Utilities Commission

Can the Power Grid Be Hacked? Why Experts Disagree

Carnegie Mellon University

- Cylab at Carnegie Mellon
- Governance of Enterprise Security: Cylab 2012 Report

Catalog of Control Systems Security: Recommendations for Standards Developers

Categorizing Cyber Systems - An Approach Based on BES Reliability Functions

CERT

Center for the Study of the Presidency & Congress – CSPC

- Securing The U.S. Electrical Grid

Certificate Management for Embedded Industrial Systems

Chertoff Group

- Addressing the Dynamic Threats to the Electric Power Grid Through Resilience

CIP5

CIP Version 5 Supports Unidirectional Security Gateways

CIP Version 5: What Does it Mean for Utilities?

CIP5 FERC Order

CIPAC - Critical Infrastructure Partnership Advisory Council

Cisco 2014 Annual Security Report

Classification Method and Key Measures – Cybersecurity for Industrial Control Systems

Cloud Security Alliance – CSA

COBIT - Control Objectives for Information and Related Technology

Congress

- Congressional Testimony – 2014-04-10
- Congressional Testimony – 2012-07-17

Congressional Research Service

- Cybersecurity: Authoritative Reports and Resources, by Topic
- The Smart Grid and Cybersecurity = Regulatory Policy and Issues
- The Stuxnet Computer Worm: Harbinger of an Emerging Warfare Capability
- Terrorist Use of the Internet: Information Operations in Cyberspace

Connecticut

- Cybersecurity and Connecticut's Public Utilities

Control Center Security at the Bulk Electric System Level

Council on Cybersecurity

Council on Foreign Relations on Cybersecurity

Cost of Failed Trust - 2013 Annual Report

CRISP - Cybersecurity Risk Information Sharing Program

Critical Infrastructure in Wikipedia

Critical Infrastructure Partnership Advisory Council - CIPAC

Critical Infrastructure Protection – Cybersecurity Guidance Is Available, but More Can Be Done to Promote Its Use – GAO-12-92

Critical Infrastructure Protection – Multiple Efforts to Secure Control Systems Are Underway, but Challenges Remain GAO-07-1036

Critical Infrastructure Protection in Wikipedia

Critical Infrastructure Protection - Cybersecurity Guidance Is Available, but More Can Be Done to Promote Its Use - GAO Report

Critical Infrastructure Cybersecurity (by Lockheed Martin)

Critical Infrastructure Sectors_DHS

Critical Infrastructure Protection Standards (CIP)

Critical Infrastructure: Security Preparedness and Maturity

Critical Security Controls for Effective Cyber Defense

CSA - Cloud Security Alliance

CSPC - Center for the Study of the Presidency & Congress ***– see above***

Cyber Attack Task Force (NERC)

Cyber and Grid Security at FERC

Cyber insurance becomes the new cost of doing business

Cyber-Physical Systems Security for Smart Grid

Cyber-Risk Oversight

Cyber Risk and the Board of Directors - Closing the Gap

Cyber Security for DER Systems

Cyber Security and Privacy Program - 2013 Annual Review

Cyber security procurement language for control systems

Cyber Solutions Handbook - Making Sense of Standards and Frameworks

Cyber Security for Smart Grid, Cryptography, and Privacy

Cyber Security Standards in Wikipedia

Cyber Security Standards (NERC) in Wikipedia

Cyber threat Intelligence Integration Center - CTIIC

Cyber threats Proving Their Power over Power Plant Operational Technology

Cyber War - Hardening SCADA

Cyberattack Insurance a Challenge for Business

Cybersecurity and the Audit Committee - Deloitte

Cybersecurity and the Board: Avoiding Personal Liability - Part I of III: Policies and Procedures

Cybersecurity and the Board: Avoiding Personal Liability - Part II of III: Policies and Procedures

Cybersecurity and the Board: Avoiding Personal Liability - Part III of III: Policies and Procedures

Cybersecurity: Authoritative Reports and Resources, by Topic ***– by CRS***

Cybersecurity Best Practices for Small and Medium Pennsylvania Utilities

Cybersecurity: Boardroom Implications - NACD

Cybersecurity and Connecticut's Public Utilities

Cybersecurity Capability Maturity Model - Electricity Subsector

Cybersecurity Challenges in Securing the Electricity Grid – GAO-12-507T - Testimony Before the Committee on Energy and Natural Resources, U.S. Senate

Cybersecurity...Continued in the Boardroom

Cybersecurity and the Evolving Role of State Regulation: How it Impacts the California Public Utilities Commission

Cybersecurity and the North American Electric Grid - New Policy Approaches to Address an Evolving Threat

Cybersecurity and the PUC

Cybersecurity Procurement Language for Energy Delivery Systems

Cybersecurity and Remote Access – SPARK Article

Cybersecurity Risk Information Sharing Program - CRISP
Cybersecurity Risks and the Board of Directors – Harvard Article
Cybersecurity for State Regulators - With Sample Questions for Regulators to Ask
Cybersecurity for Utilities: The Rest of the Story
Cybersecurity Webpage on DHS
Cybersecurity Website Page on DOE
Cyberspace Policy Review
Cylab at Carnegie Mellon
Dark Reading – Cyber News
Data Breach Notification Laws by State
The ***Debate Over Cyber Threats***
Defense Critical Infrastructure – Actions needed to improve the identification and management of electrical power risks and vulnerabilities to DOD Critical Asset
Dell
How Traditional Firewalls Fail Today's Networks - and Why Next-Generation Firewalls Will Prevail - Dell
Deloitte

- ***Cybersecurity and the Audit Committee - Deloitte***
- ***Cybersecurity...Continued in the Boardroom***
- ***Deloitte - Audit Committee Brief - 2014-05-01***
- ***SEC's Focus on Cybersecurity*** – Key insights for investment advisors

Department of Defense – DoD

- ***CERT***
    - ***Insider Threat Center of CERT***
- ***Software Engineering Institute***
    - ***Insider Fraud in Financial Services Illicit Cyber Activity Involving Fraud in the U.S. Financial Services Sector – Software Engineering Institute***
    - ***Insider Threat Study: Illicit Cyber Activity Involving Fraud in the U.S. Financial Services Sector – Software Engineering Institute***

Department of Energy - DOE

- ***2012 DOE Smart Grid Cybersecurity Information Exchange***
- ***AMI Penetration Test Plan***
- ***Analysis of Selected Electric Sector High Risk Failure Scenarios***
- ***Argonne National Lab - DOE***
- ***Cyber security procurement language for control systems***
- ***Energy Sector Cybersecurity Framework Implementation Guidance***
- **ICS-CERT Year in Review - Industrial Control Systems Cyber Emergency Response Team 2013 - DOE**
- ***Electricity Subsector - Risk Management Process***
- ***Gridwise Architecture Council***
- ***High Impact, Low-Frequency Event Risk to the North American Bulk Power System – NERC and DOE***
- ***Idaho National Lab***
- ***Implementing Effective Enterprise Security Governance - DOE***
- ***Industrial Control Systems Joint Working Group (ICSJWG)***
- ***Infrastructure Security and Energy Restoration***
- ***National Electric Sector Cybersecurity Organization - NESCO***
    - ***Electric Sector Failure Scenarios and Impact Analyses - NESCOR***
        - ***ERPI NESCOR Webpage***
        - ***NESCOR Guide to Penetration Testing for Electric Utilities - Version 3***
- ***Office of Electric Delivery & Energy Reliability – NESCO***
- ***Pacific Northwest National Laboratory – PNNL***
- ***Sandia National Lab***

Department of Energy wants electric utilities to create "cybersecurity governance board"

Department of Homeland Security – DHS

- *C-Cubed Program*
- *Catalog of Control Systems Security: Recommendations for Standards Developers*
- *Critical Infrastructure Partnership Advisory Council - CIPAC*
- *Critical_Infrastructure_Sectors_DHS*
- *Electricity Subsector Coordinating Council – ESCC*
- *Electricity Subsector - Cybersecurity Capability Maturity Model*
- *Enhanced Cybersecurity Services*
- *Fusion Centers*
- *Implementation Status of the Enhanced Cybersecurity Services Program*
- *Industrial Control Systems Joint Working Group -ICSJWG*
- *Industrial Control Systems Cyber Emergency Response Team – ICS-CERT*
- *National Cybersecurity and Communications Integration Center – DHS*
- *National Infrastructure Advisory Council – DHS*
- *NESEC V1.0 System Requirements Document Revision 3c – DHS*
- *Partnership for Critical Infrastructure Security*
- *Protective Security Advisor* – DHS free services
- *US-CERT*

Detailed Measures - Cybersecurity for Industrial Control Systems

DHS Cybersecurity Capability Maturity Model - Electricity Subsector

Dragonfly: Western Energy Companies Under Sabotage Threat

Encryption: The answer to all security

Easing the Pain of a NERC CIP Audit

Eastern Interconnection Data Sharing Network

Edison Electric Institute - EEI

- *EEI website cybersecurity page*
- *Technical Conference 2014-04-29 - EEI Comments*

EEI - Edison Electric Institute

Effects-Based Targeting for Critical Infrastructure

Electric Power Research Institute – EPRI

- *Attack Trees for Selected Electric Sector High Risk Failure Scenarios*
- *Cyber Security for DER Systems*
- *Cyber Security and Privacy Program - 2013 Annual Review*
- *ERPI NESCOR Webpage*
- *North America Electric System Infrastructure SECurity (NESEC) System – EPRI*

Electricity for Free - The dirty underbelly of SCADA and Smart Meters

Electricity Grid Modernization

Electricity Subsector Coordinating Council - ESCC

- *ESCC – Overview presentation*

Electric Grid Vulnerability - Industry Responses Reveal Security Gaps

Electric Power Supply Association – EPSA - on Cybersecurity

Electric Utility Cyber Security Standards: Practical Implementation Guidance

Electricity Sector Cybersecurity Capability Maturity Model

Electricity Sector Information Sharing and Analysis Center – ES-ISAC

Electricity Subsector Coordinating Council – ESCC

- *Roadmap to Achieve Energy Delivery Systems Cybersecurity*

Electricity Subsector - Cybersecurity Capability Maturity Model

Electricity Subsector - Risk Management Process

Energetic Bear

Energy Firm's Security So POOR, Insurers REFUSE to take their cash

Energy Sector Control Systems Working Group – ESCSWG

- Cybersecurity Procurement Language for Energy Delivery Systems

Energy Sector Cybersecurity Framework Implementation Guidance

EnergySec

- Network Perimeter Defense – Analyzing the Data
- Network Perimeter Defense – Common Mistakes
- Report and Recommendations – NECPUC Cybersecurity Project

Enhanced Cybersecurity Services

EPRI - Electric Power Research Institute

ES ISAC – Electricity Sector Information Sharing and Analysis Center

ESCC - Electricity Subsector Coordinating Council

Establishing Trust in Distributed Critical Infrastructure Micro Devices

European Network and Information Security Agency

European Union

- ENISA Threat Landscape 2014

Ex-FBI Official: Intel agencies don't share cyber threats that endanger companies

Executive Branch (President)

- Cyberspace Policy Review
- Cyber threat Intelligence Integration Center
- Executive Order – 13636
- Executive Order – Promoting Private Sector Cybersecurity Information Sharing
- Presidential Policy Directive 21

Executive Order – 13636

Expendable ICS Networks?

External Monitoring Security Threats

EY (Ernst & Young)

- How the Grid Will Be Hacked - by E&Y

FBI

- Cyber Crime
- InfraGard
- iGuardian

Federal Energy Regulatory Commission - FERC

- CIP5 FERC Order
- Cyber and Grid Security at FERC - Webpage
- Office of Energy Infrastructure Security – OEIS
- Opening Remarks by Kevin Perry
- Transcript from the Technical Conference ordered in CIP5
- Technical Conference 2014-04-29 - EEI Comments
- Testimony of Joseph McClelland
- Wellinghoff to Markey letter of 2009-04-28

The Federal Government's Track Record on Cybersecurity and Critical Infrastructure

Federal Information Security Management Act of 2002 - FISMA

Federal Laws Relating to Cybersecurity: Overview and Discussion of Proposed Revisions

Feel the Electricity: how situation management empowers utilities for CIP Compliance

FERC

The Financial Impact of Cyber Risk

FINRA

- Report on Cybersecurity Practices

Firewalls

The ***Firewall Loophole - easy, Insecure NERC CIP Compliance***

FISMA - Federal Information Security Management Act of 2002

Foreign Cyber-Spies Inject Spyware into U.S. Grid with Potential for Serious Damage

The ***Forrester Wave: Information Security and Risk Consulting Services, Q3, 2010***

The ***Forrester Wave: Managed Security Services, Q3 2010***

A Framework for Developing and Evaluating Utility Substation Cyber Security

Framework for Improving Critical Infrastructure Cybersecurity - NIST

Frost & Sullivan

Fusion Centers

Future of the Electric Grid

GAO Report - Critical Infrastructure Protection - Cybersecurity Guidance Is Available, but More Can Be Done to Promote Its Use

Gartner Identifies the Top 10 Technologies for Information Security in 2014

Generic Risk Template

Glossary of Key Information Security Terms - NIST 7298

Google Reports Unauthorized Digital Certificates

Governance of Enterprise Security: Cylab 2012 Report

Government Accounting Office

- ***Cybersecurity Challenges in Securing the Electricity Grid – GAO-12-507T*** - Testimony Before the Committee on Energy and Natural Resources, U.S. Senate
- ***Critical Infrastructure Protection*** – Cybersecurity Guidance Is Available, but More Can Be Done to Promote Its Use – GAO-12-92
- ***Critical Infrastructure Protection*** – Multiple Efforts to Secure Control Systems Are Underway, but Challenges Remain GAO-07-1036
- ***Critical Infrastructure Protection*** – Update to National Infrastructure Projection Plan Includes Increased Emphasis on Risk Management and Resilience GAO-10-296
- ***Defense Critical Infrastructure*** – Actions needed to improve the identification and management of electrical power risks and vulnerabilities to DOD Critical Asset
- ***Information Security*** – TVA Needs to Address Weaknesses in Control Systems and Networks – GAO-08-526

Government Asks Utilities, Others to Check Networks after 'Energetic Bear' Cyberattacks

Gramm-Leach-Bliley Act, Interagency Guidelines

Guide to Industrial Control Systems (ICS) Security

Gridwise Architecture Council

Guidance for Secure Interactive Remote Access from NERC – 2011-07-01 –

Hacking the Smart Grid

Hewett Packard – HP

- ***The Best Practices Guide for Application Security – HP part 3***
- ***The Business Case for Application Security – HP part 2***
- ***The Mandate for Application Security – HP part 1***

High Impact, Low-Frequency Event Risk to the North American Bulk Power System – NERC and DOE

Holistic Enterprise Security Solution

Homeland Security - Legal and Policy Issues (a book)

House of Representatives

- ***Testimony – Cybersecurity: Assessing the immediate threat to the United States*** – 2011-05-25

How to Hack the Power Grid for Fun and Profit

How the Grid Will Be Hacked - by E&Y

How to Increase Cyber-Security in the Power Sector: A Project Report from the Australian Power Sector

How Traditional Firewalls Fail Today's Networks - and Why Next-Generation Firewalls Will Prevail - Dell

HSToday (Homeland Security news and information)

IBM

- Best Practices for Cyber Security in the Electric Power Sector
- Holistic Enterprise Security Solution

ICS-CERT - Industrial Control Systems Cyber Emergency Response Team

ICS-CERT Year in Review - Industrial Control Systems Cyber Emergency Response Team 2013 - DOE

ICSJWG - Industrial Control Systems Joint Working Group

Idaho National Lab

Identity Theft Prevention and Identity Management Standards - ANSI

IEC – International Electrotechnical Commission (Standards)

- IEC 61850 Standards
- IEC 61968 – distribution standards
- IEC 61970 – standards for energy management systems
- IEC 62351

IEEE - Institute of Electrical and Electronic Engineers

- IEEE 1686 – Standard for Substation Intelligent Electronic Devices (IED) Cyber Security Capabilities
- IEEE P37.240 – Standard for Cyber Security Requirements for Substation Automation, Protection and Control Systems
- IEEE 1711 – Cryptographic Protocol for Cyber Security of Substation Serial Links
- IEEE 1402 – Standard for Physical Security of Electric Power Substations
- PSRC H22 – Cyber Security for protection related data files

If cyberwar erupts, America's electric grid is a prime target

iGuardian

Implementing Effective Enterprise Security Governance - DOE

Implementation Study Final Report – implementing CIP5

Industrial Control Technology (ICS/OT Systems)

- Cyber threats Proving Their Power over Power Plant Operational Technology

Industrial Control Systems Cyber Emergency Response Team – ICS-CERT – DHS

Industrial Control Systems Cyber Threat Research By Preventia

Industrial Control Systems Joint Working Group -ICSJWG

InfraGard

Infrastructure Security - Wikipedia

Infrastructure Security and Energy Restoration

Information Security – TVA Needs to Address Weaknesses in Control Systems and Networks – GAO-08-526

Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations – NIST 800-137

Information Sharing and Analysis Organizations – ISAOs – see Executive Order – Promoting Private Sector Cybersecurity Information Sharing

Information Systems Security Association – ISSA

Infosecurity Magazine

Insider Fraud in Financial Services Illicit Cyber Activity Involving Fraud in the U.S. Financial Services Sector – Software Engineering Institute

Insider Threat Study: Illicit Cyber Activity Involving Fraud in the U.S. Financial Services Sector – Software Engineering Institute

Insider Threat Center of CERT

Institute of Electrical and Electronic Engineers – IEEE

- Smart Grid Community – IEEE

Insurance (Cybersecurity)

- Cyber insurance becomes the new cost of doing business

International Electrotechnical Commission (Standards) – see IEC above

International Organization for Standardization – ISO

- ISO 27001
- ISO 27002

International Society of Automation – ISA

- ISA99, Industrial Automation and Control Systems Security
- Security for Industrial Automation and Control Systems - ISA-62443
- Top Ten Differences Between ICS and IT Cybersecurity

Interoperability and Security for Converged Smart Grid Networks

Intrusion Detection System for Advanced Metering Infrastructure

ISA - International Society of Automation – see "International Society of Automation" above

ISA-6243 - Security for Industrial Automation and Control Systems

ISACA – (previously the Information Systems Audit and Control Association)

- COBIT - Control Objectives for Information and Related Technology/ISO 27002

ISAOs - Information Sharing and Analysis Organizations – see Executive Order – Promoting Private Sector Cybersecurity Information Sharing

ISSA - Information Systems Security Association

ISO 27001

ISO 27002

IT/OT Integration Done Right and Done Wrong

IT Governance Institute –ITGI

- Data Breach Notification Laws by State

IT Governance Ltd

- Governance Link
- Link to Cyber Security Resources

Journal of Energy Security

Key Steps to Automate IT Security Compliance

Law in the Boardroom in 2014

Least Privilege Principle

Lessons from 5 Advanced Attacks of 2013

Lessons Learned From Snowden

Living in a World Without Trust: When IT's Supply Chain Integrity and Online Infrastructure Get Pwned

Lockheed Martin

- Critical Infrastructure Cybersecurity (by Lockheed Martin)
- Securing Industrial Control Systems – The Basics

LulzSec

Managers Information Security Survival Kit and Checklist

Managing Information Security Risk - NIST Special Publication 800-39

The Mandate for Application Security – HP part 1

The Mask, Attacks on Trust, and Game Over - Kaspersky Labs

Metasploit

Microsoft

- Developing a City Strategy for Cybersecurity

National Association of Corporate Directors – NACD

- Audit Committee Chair Advisory Council
- Cyber-Risk Oversight

- *Cybersecurity: Boardroom Implications - NACD*
- *NACD Summit*
- *Playing For Keeps*

National Association of Regulatory Utility Commissioners – NARUC

- *Cybersecurity for State Regulators - With Sample Questions for Regulators to Ask*
- *Cybersecurity for State Regulators 2.0*

National Cybersecurity Center of Excellence - NCCoE

National Cybersecurity and Communications Integration Center – DHS

National Electric Sector Cybersecurity Organization - NESCO

National Electric Sector Cybersecurity Organization Resource - NESCOR

- *Electric Sector Failure Scenarios and Impact Analyses - NESCOR*
- *ERPI NESCOR Webpage*
- *Wide Area Monitoring, Protection, and Control Systems (WAMPAC) - Standards for Cyber Security Requirements*

National Infrastructure Advisory Council – DHS

National Governors Association – NGA

- *State Roles in Enhancing the Cybersecurity of Energy Systems and Infrastructure*

Network Perimeter Defense – Analyzing the Data

Network Perimeter Defense – Common Mistakes

National Institute of Standards - NIST

National Research Regulatory Institute – NRRI

- *The Role of State Public Utility Commissions in Protecting National Utility Infrastructure*
- A *Summary of State Regulators' Responsibilities Regarding Cybersecurity Issues*

NECPUC Cybersecurity Project – Report and Recommendations

NERC

- *Categorizing Cyber Systems - An Approach Based on BES Reliability Functions*
- *CIP5*
- *NERC CIP-005 Compliance: At-A-Glance*
- *NERC-CIP V5 Encourages Unidirectional Gateways*
- *NERC CIP V5 Standards Position - Unidirectional Security Gateways as Secure Alternatives to Firewalls and Network Intrusion Detection Systems*
- *Critical Infrastructure Protection Standards (CIP)*
- *Cyber Attack Task Force (NERC)*
- *ES ISAC – Electricity Sector Information Sharing and Analysis Center*
- *Guidance for Secure Interactive Remote Access from NERC*
- *High Impact, Low-Frequency Event Risk to the North American Bulk Power System – NERC and DOE*
- *Implementation Study Final Report* – implementing CIP5
- *NERC Reliability Assurance Initiative - RAI*
- *NERC Security Guidelines Working Group -SGWG*
- *Reliability Coordinator Information Sharing Portal (via NERC)*
- *NERC CIP & Smart Grid*

NESCO - National Electric Sector Cybersecurity Organization

NESCOR Guide to Penetration Testing for Electric Utilities - Version 3

NESCOR - National Electric Sector Cybersecurity Organization Resource

NESEC V1.0 System Requirements Document Revision 3c – DHS

News

- *HSToday (Homeland Security news and information)*

- *Infosecurity Magazine*
- *SecurityWeek*
- *TechTarget - SearchSecurity*

At The Nexus of Cybersecurity and Public Policy – Some Basic Concepts and Issues

NIST - National Institute of Standards

- *Framework for Improving Critical Infrastructure Cybersecurity - NIST*
- *Glossary of Key Information Security Terms - NIST 7298*
- *Guide to Industrial Control Systems (ICS) Security – NIST 800-82*
- *Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations – NIST 800-137*
- *Managing Information Security Risk - NIST Special Publication 800-39*
- *National Cybersecurity Center of Excellence - NCCoE*
- *NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 3.0* – NIST Special Publication 1108R3
- *NIST Interagency or Internal Reports (NISTIRS)*
- *NIST SGIP Cyber Security Working Group*
- *NIST Smart Grid Collaboration Wiki for Smart Grid Interoperability Standards*
- *NIST Special Publication 800-39 - Managing Information Security Risk*
- *NISTR 7628 – NIST Interagency Report, Guidelines for Smart Grid Cyber Security*
- *NISTIR 7761 R1 – Smart Grid Interoperability Panel Priority Action Plan 2: Guidelines for Assessing Wireless Standards for Smart Grid Applications*
- *Special Publication 800-53 – Security and Privacy Controls for Federal*
- *Top*

North America Electric System Infrastructure SECurity (NESEC) System – EPRI

NRECA Cyber task Force To Serve Co-ops (ECT.coop)

NRRI - see "National Research Regulatory Institute"

OCIE Cybersecurity Initiative

OEIS - Office of Energy Infrastructure Security at FERC

Office of Energy Infrastructure Security – OEIS at FERC

Office of Electric Delivery & Energy Reliability – NESCO

Pacific Northwest National Laboratory – PNNL

- *CRISP - Cybersecurity Risk Information Sharing Program*

Partnership for Critical Infrastructure Security

Penetration Testing and Red Teams

Ponemon Institute

- *2012 Cost of Cyber Crime Study: United States*
- *Cost of Failed Trust - 2013 Annual Report*
- *Critical Infrastructure: Security Preparedness and Maturity*
- *Ponemon 2014 SSH Security Vulnerability Report - Information Technology's Dirty Secret and Open Backdoors*

Presidential Policy Directive 21

Principle of Least Privilege

PRISEM for Seattle

Procurement

- *Cybersecurity Procurement Language for Energy Delivery Systems*
- *Cyber security procurement language for control systems*

Project Basecamp

Protecting Against Cybersecurity Threats Starts Now

Protective Security Advisor – DHS free services

Protiviti

- Board Perspectives: Risk Oversight
- From Cybersecurity to Collaboration: Assessing the Top Priorities for Internal Audit Functions

Public Utility Commissions

PWC

- PWC- Center for Board Governance
- PWC on Cybersecurity

Questions for asking

The Financial Impact of Cyber Risk

Red Team & Penetration Testing

Regulators

- Cybersecurity and the PUC
- How to Increase Cyber-Security in the Power Sector: A Project Report from the Australian Power Sector
- NECPUC Cybersecurity Project – Report and Recommendations

Reliability Coordinator Information Sharing Portal (via NERC)

Report and Recommendations – NECPUC Cybersecurity Project

Report: Cyber Threats to Energy Sector Happening at Alarming Rate

Risk Management

Electricity Subsector - Risk Management Process

Generic Risk Template

Roadmap to Achieve Energy Delivery Systems Cybersecurity

Is there a Role for Government in Cyber Security - NPR episode

The Role of State Public Utility Commissions in Protecting National Utility Infrastructure

Sandia National Lab

SANS Institute

- Critical Security Controls for Effective Cyber Defense
- Implementing an Effective IT Security Program
- SANS Internet Storm Center
- SANS Securing the Human

SCADA

- How to Stop Malware Attacks on SCADA Systems
- The SCADA Security Survival Guide
- SCADA System Cyber Security - A Comparison of Standards

Schneider Electric

- A Framework for Developing and Evaluating Utility Substation Cyber Security

SearchSecurity - TechTarget

SEC's Focus on Cybersecurity – Key insights for investment advisors

Securing the Human – by SANS

Securing The U.S. Electrical Grid

Security and Exchange Commission

- OCIE Cybersecurity Initiative
- SEC's Focus on Cybersecurity – Key insights for investment advisors

Security for Industrial Automation and Control Systems - ISA-62443

Security and States

Security Wizardry Information Portal

SecurityWeek

Senators ask FERC to helm "expeditious comprehensive" probe of grid security

Smart Energy Profile (SEP)

The Smart Grid and Cybersecurity = Regulatory Policy and Issues

Smart Grid Security Blog

Social Engineering

Software Engineering Institute

Special Publication 800-53 (from NIST)

State Regulators

State Roles in Enhancing the Cybersecurity of Energy Systems and Infrastructure

Stronger than Firewalls

Stuxnet

- The Stuxnet Computer Worm: Harbinger of an Emerging Warfare Capability
- Stuxnet Five Years Later - Did We take the Right Lessons?

Substations

- A Framework for Developing and Evaluating Utility Substation Cyber Security
- IEEE 1402 – Standard for Physical Security of Electric Power Substations
- Unidirectional Security Gateways - Secure Transmission Substations Application
- U.S. Risks National Blackout From Small-Scale Attack

A Summary of State Regulators' Responsibilities Regarding Cybersecurity Issues

Surviving on a Diet of Poisoned Fruit: Reducing the National Security Risks Of America's Cyber Dependencies

Targeted Attacks Against the Energy Sector

TechTarget - SearchSecurity

Telephone Industries Association - Cybersecurity

Terrorist Use of the Internet: Information Operations in Cyberspace

Testimony Before the Committee on Energy and Natural Resources, US Senate

It's Time for Corporate Boards to tackle Cybersecurity. Here's Why

Think Data Breaches Can't Happen To You?

Threat-Intel Sharing Services Emerge, But Challenges Remain

Time report on Smart Grid vulnerability

Top Ten Differences Between ICS and IT Cybersecurity

Training

- Protective Security Advisor – DHS free services

Transcript from the Technical Conference ordered in CIP5

Transformers Expose Limits in Securing Power Grid

Two Factor Authentication

UglyGorilla Hack of US Utility Exposes Cyberwar threat

Understanding the physical and economic consequences of attacks on control systems

Unidirectional Gateways

- Classification Method and Key Measures – Cybersecurity for Industrial Control Systems

Unidirectional Security Gateways - Secure Transmission Substations Application

Unidirectional Security Gateways vs. Firewalls: Comparing Costs

Unveiling "The Mask": Sophisticated malware ran rampant for 7 years

US-CERT

Is U.S. Cybersecurity plan a carrot, stick or legal nightmare?

The U.S. Electric Grid is Safer than you probably think

U.S. Risks National Blackout From Small-Scale Attack

U.S. Steps Up Alarm Over Cyberattacks

U.S. Utility's Control System was hacked, says Homeland Security

Utilities Need Test Bed to Evaluate Legacy Industrial Control System Cybersecurity Technologies

Utilities Report Cyber Incidents to Energy Department

Utilities Telecom Council - UTC

END OF TABLE OF CONTENTS

2012 Utility Cyber Security Survey **-** http://www.EnergyCollection.us/Energy-Security/2012-Utility-Cyber.pdf Top

2013 Annual Cost of Failed Trust Report: Threats & Attacks - reveals that failed key and certificate management threatens every global enterprise with potential exposure of almost US $400M. http://www.EnergyCollection.us/Energy-Security/2013-Annual-Cost.pdf Top

440 Million New Hackable Smart Grid Points **-** By the end of 2015, the potential security risks to the smart grid will reach 440 million new hackable points. Billions are being spent on smart grid cybersecurity, but it seems like every time you turn around, there is yet another vulnerability exposing how to manipulate smart meters or power-grid data. http://eee.EnergyCollection.us/Energy-Security/440-Million-New.pdf Original link - http://blogs.computerworld.com/17120/400_million_new_hackable_smart_grid_points Top

Aberdeen Group **-** The IT security practice examines technologies used to ensure the confidentiality, integrity, availability, and authenticity of enterprise data and data transactions, from application security, endpoint encryption, master material data management, Cloud and Web security, data loss prevention, data protection, email security, Web security and others. http://www.aberdeen.com/_aberdeen/it-security/ITSA/practice.aspx Top

Advanced Cyber Security for Utilities **-** a 2009-05-20 presentation by The Structure Group (25 Pages). http://www.EnergyCollection.com/Energy-Security/Advanced-Cyber-Securities-For-Utilities.pdf Top

Advanced Persistent Threat - http://en.wikipedia.org/wiki/Advanced_persistent_threat Top

AlienVault Open Threat Exchange - http://www.alienvault.com/open-threat-exchange Top

American Public Power Association **-** is a collection of more than 2,000 community-owned electric utilities, serving more than 47 million people or about 14 percent of the nation's electricity consumers. Public power utilities are operated by local governments to provide communities with reliable, responsive, not-for-profit electric service. Public power utilities are directly accountable to the people they serve through local elected or appointed officials. http://www.publicpower.org

- Top

American Gas Association

- ***AGA Report No. 12 - Cryptographic Protection of SCADA Communications*** **-** http://www.EnergyCollection.us/Energy-Security/AGA-Report-12.pdf Top
- Top

American National Standards Institute - ANSI

- ***Company website*** **-** http://www.ansi.org/
- ***ANSI Homeland Defense and Security Standardization Collaborative - HDSSC*** - http://www.ansi.org/standards_activities/standards_boards_panels/hssp/overview.aspx?menuid=3 Top
- ***Identity Theft Prevention and Identity Management Standards*** - http://www.ansi.org/standards_activities/standards_boards_panels/idsp/overview.aspx?menuid=3 Top
- ***Wikipedia -*** http://en.wikipedia.org/wiki/American_National_Standards_Institute
- Top

American Public Power Association – APPA - Public power is a collection of more than 2,000 community-owned electric utilities, serving over 43 million people or about 14 percent of the nation's electricity consumers. Website: http://www.appanet.org APPA webpage for cybersecurity - http://www.publicpower.org/Topics/Landing.cfm?ItemNumber=38507

- ***Bulk Power System Cyber Security*** **-** APPA publication - 2011-02-01 - contains a good history of cybersecurity and the grid. http://www.EnergyCollection.us/Energy-Security/Bulk-Power-System-Cyber.pdf Top
- Top

ANSSI – Agency for National Security Systems and Information

- ***Classification Method and Key Measures - Cybersecurity for Industrial Control Systems*** **-** This document is based on the findings of the working group on Industrial Control System cybersecurity, directed by the French Network and Information Security Agency, the ANSSI12. Composed of actors in the field of automated industrial process control systems and specialists in IT3 Security, the group has undertaken to draft a set of measures to improve the cybersecurity of ICS4. These documents will be used to define the methods for applying the measures set out within the framework of French law No. 2013-1168 of 18 December 2013, known as the Military programming law (LPM5). The objective is to subject all new critical ICSs to an approval process, thus ensuring that their cybersecurity level is acceptable given the current threat status and its potential developments. The document is intended for all actors (e.g. responsible entities, project managers, buyers, manufacturers, integrators, prime contractors) concerned with the design, implementation, operation and maintenance of ICSs. The working group did not focus on any specific business sector. Therefore, the contents of this document are intended to apply to all sectors. Some sectors have special characteristics that have not been detailed or considered in this document. In some cases, it may be necessary to establish a sector-specific version of this document, in collaboration with the coordinating ministries, in order to clarify how to apply techniques and to take specific constraints into account. All of the measures presented have been designed for new ICSs. It is quite possible that these measures cannot be directly applied to existing ICSs; therefore, an exhaustive impact evaluation should be carried out before any implementation. Situations may arise (e.g. compatibility issues with existing ICSs, business-specific constraints) in which certain measures cannot be applied without adapting them. These special cases should be the object of specific studies and the resulting measures should be submitted to the cyber-defense authority for approval. As this work focused exclusively on cybersecurity for ICSs, the definition of organizations' overall IT security strategy is not concerned by this framework. It is therefore up to each responsible entity to integrate their ICSs and their specific constraints into their IT Security Policy. http://www.EnergyCollection.us/Companies/ANSSI/Classification-Method-Key.pdf Top

- ***Detailed Measures - Cybersecurity for Industrial Control Systems*** **-** This document is based on the findings of the working group on Industrial Control System cybersecurity, directed by the French Network and Information Security Agency, ANSSI12. Composed of actors in the field of automated industrial process control systems and specialists in IT Security, the group has undertaken to draft a set of measures to improve the cybersecurity of ICS. The document is intended for all actors (e.g. responsible entities, project managers, buyers, manufacturers, integrators, prime contractors) concerned with the design, implementation, operation and maintenance of ICSs. The working group did not focus on a specific business sector; the contents of this document are intended to apply to all sectors. Some sectors have specific characteristics that may not have been detailed or considered in this document. Therefore, in some cases, a sector-specific version of this document may be required to clarify the application and to take specific constraints into account. All of the measures presented have been designed for new ICSs. It is quite possible that these measures cannot be directly applied to existing ICSs; therefore, an exhaustive impact evaluation should be carried out before any implementation. It is also possible that situations may arise (e.g. compatibility issues with existing ICSs, business-specific constraints) in which measures cannot be applied without adapting them. These special cases should be the object of specific studies and the resulting measures should be submitted to the cyberdefence authority for approval. http://www.EnergyCollection.us/Companies/ANSSI/Detailed-Measures.pdf Top

Anonymous **-** Anonymous (used as a mass noun) is a loosely associated international network of activist and hacktivist entities. A website nominally associated with the group describes it as "an internet gathering" with "a very loose and decentralized command structure that operates on ideas rather than directives".[2] The group became known for a series of well-publicized publicity stunts and distributed denial-of-service (DDoS) attacks on government, religious, and corporate websites. Wikipedia - http://en.wikipedia.org/wiki/Anonymous_%28group%29 Top

Assault On California Power Station Raises Alarm on Potential for Terrorism **-** April Sniper Attack Knocked Out Substation, Raises Concern for Country's Power Grid - 2014-04-04 - http://www.EnergyCollection.us/Energy-Security/Assault-California-Power.pdf Top

Attacks on Trust: The Cybercriminal's New Weapon **-** 3013-07-01 by Forrester for Venafi - The trust established by cryptographic keys and certificates is critical to enabling just about every electronic interaction and process that businesses and governments rely on today. Much like a nation's currency, people who use these keys and certificates need to trust their value if they're to be accepted and facilitate transactions. Yet, this trust can easily be exploited. Cybercrirninals have identified keys and certificates as a weak spot for many organizations today; cybercriminals can become trusted users on your networks, in your clouds, or on mobile devices, evading a multitude of technical controls and gaining undetected access. In 2013, we're seeing cybercriminals accelerate the exploitation of keys and certificates to steal data or enable other attacks against victims. We've seen several high-profile cases that point to magnitude and seriousness of this threat. Recently, rogue Microsoft digital certificates allowed Flame malware to make its way past Windows controls.' This year, attackers gained access to security firm Bit9's trusted certificate and used it to sign malware.' Google also discovered an unauthorized certificate impersonating Google.com for a man-in-the-middle attack.' Cybercriminals are also known to steal SSH keys or manipulate which keys are trusted to gain access to source code and other valuable intellectual property. http://www.EnergyCollection.us/Energy-Security/Attacks-On-Trust.pdf Top

Automation Federation **-** The Automation Federation is an association of member organizations providing awareness, programs, and services that continually advance the automation profession for the betterment of humanity. Cybersecurity link - http://www.automationfederation.org/Content/NavigationMenu/General_Information/Alliances_and_Associations/The_Automation_Federation/Focus_Areas/Cybersecurity/Cybersecurity.htm Top

Axelos **-** AXELOS, the owner of ITIL® and PRINCE2®, is developing a new cybersecurity portfolio designed to help commercial organizations and governments around the world combat the risk of cyber attacks. http://www.axelos.com/?DI=639511 Top

Best Practices Against Insider Threats in All Nations **-** Based on its analysis of more than 700 case studies, the CERT® Insider Threat Center recommends 19 best practices for preventing, detecting, and responding to harm from insider threats. This technical note summarizes each practice, explains its importance, and provides an international policy perspective on the practice. Every nation can use this paper as a succinct educational guide to stopping insider threats and an exploration of international policy issues related to insider threats. 2013-08-01 http://www.EnergyCollection.us/Energy-Security/Best-Practices-Against.pdf Top

Bipartisan Policy Center - is a non-profit organization that drives principled solutions through rigorous analysis, reasoned negotiation and respectful dialogue. With projects in multiple issue areas, BPC combines politically-balanced policymaking with strong, proactive advocacy and outreach. http://bipartisanpolicy.org

- ***Bipartisan Policy Center - Electric Grid Cybersecurity Initiative*** **-** The Electric Grid Cybersecurity Initiative, a joint effort of BPC's Energy and Homeland Security Projects, will develop recommendations for how multiple government agencies and private companies can protect the North American electric grid from cyber-attacks. The initiative will consider how to allocate responsibility for cyber-attack prevention and response, facilitate the sharing of intelligence about cyber threats and vulnerabilities with electric power companies, and ensure appropriate privacy protections for customer data. http://bipartisanpolicy.org/projects/electric-grid-cybersecurity-initiative Top
- ***Cybersecurity and the North American Electric Grid - New Policy Approaches to Address an Evolving Threat*** **-** 2014-02-01 - Bipartisan Policy Center - This report summary highlights key findings and recommendations from the co-chairs of the Bipartisan Policy Center's (BPC) Electric Grid Cybersecurity Initiative. It covers four topic areas: standards and best practices, information sharing, response to a cyber attack, and paying for cybersecurity. Recommendations in these areas target Congress, federal government agencies, state public utilities commissions (PUCs), and industry. The Initiative was launched as a collaboration of BPC's Energy and Homeland Security Projects in May 2013. Its goal was to develop policies—aimed at government agencies as well as private companies—for protecting the North American electric grid from cyber-attacks. http://www.EnergyCollection.us/Energy-Security/Cybersecurity-North-American.pdf Top

- Top

Boardroom Cyber Watch Survey - 2014 Report - The '2014 Boardroom Cyber Watch Survey' is the second annual survey we have undertaken specifically targeting chief executives, board directors and IT professionals. It demonstrates the issues organizations are facing in the constantly changing cyber threat landscape and how the boardroom's and IT function's perception of cyber risks is shifting. http://www.EnergyCollection.us/Energy-Security/Boardroom-Cyber-Watch-2014.pdf Top

Brookings Center **-** is a nonprofit public policy organization based in Washington, DC. Our mission is to conduct high-quality, independent research and, based on that research, to provide innovative, practical recommendations that advance three broad goals: Strengthen American democracy; Foster the economic and social welfare, security and opportunity of all Americans; and Secure a more open, safe, prosperous and cooperative international system. http://www.brookings.edu

- ***Bound to Fail: Why Cyber Security Risk Cannot Simply Be "Managed" Away*** **-** Rather than a much-needed initiative to break the legislative deadlock on the subject in Congress, President Obama's new executive order for improving critical infrastructure cyber security is a recipe for continued failure. In essence, the executive order puts the emphasis on establishing a framework for risk management and relies on voluntary participation of the private sector that owns and operates the majority of U.S. critical infrastructure. Both approaches have been attempted for more than a decade without measurable success. A fundamental reason for this failure is the reliance on the concept of risk management, which frames the whole problem in business logic. Business logic ultimately gives the private sector every reason to argue the always hypothetical risk away, rather than solving the factual problem of insanely vulnerable cyber systems that control the nation's most critical installations. The authors suggest a policy-based approach that instead sets clear guidelines for asset owners, starting with regulations for new critical infrastructure facilities, and thereby avoids perpetuating the problem in systems and architectures that will be around for decades to come. In contrast to the IT sector, the industrial control systems (ICS) that keep the nation's most critical systems running are much simpler and much less dynamic than contemporary IT systems, which makes eliminating cyber vulnerabilities, most of which are designed into products and system architectures, actually possible. Finally, they argue that a distinction between critical and non-critical systems is a bad idea that contradicts pervasiveness and sustainability of any effort to arrive at robust and well-protected systems. http://www.EnergyCollection.us/Energy-Security/Bound-To-Fail.pdf Top
- ***Brookings Center for 21st Century Security and Intelligence*** - http://www.brookings.edu/about/centers/security-and-intelligence Top
- Top

California

- ***Cybersecurity and the Evolving Role of State Regulation: How it Impacts the California Public Utilities Commission*** **-** 2012-09-19 - The purpose of this paper is to examine how the CPUC and other State regulators can further address cybersecurity as it relates to grid resiliency, reliability and safety. In particular, this paper recommends that the CPUC opens an Order Instituting Rulemaking (OIR) to further investigate appropriate cybersecurity policies. http://www.EnergyCollection.us/Energy-Security/Cybersecurity-Evolving-Role.pdf Top

- Top

Carnegie Mellon University

- ***Cylab at Carnegie Mellon*** - is a bold and visionary effort, which establishes public-private partnerships to develop new technologies for measurable, secure, available, trustworthy and sustainable computing and communications systems. CyLab is a world leader in both technological research and the education of professionals in information assurance, security technology, business and policy, as well as security awareness among cyber-citizens of all ages. Building on more than two decades of Carnegie Mellon leadership in Information Technology, CyLab is a university-wide initiative that involves over fifty faculty and one hundred graduate students from more than six different departments and schools. As a vital resource in the effort to address cyber vulnerabilities that threaten national and economic security, CyLab is closely affiliated with CERT® Coordination Center, a leading, internationally recognized center of internet security expertise. https://www.cylab.cmu.edu/ Top
- ***Governance of Enterprise Security: Cylab 2012 Report*** - How Boards & Senior Executives are Managing Cyber Risk - 2012-05-16 - It has long been recognized that directors and officers have a fiduciary duty to protect the assets of their organizations. Today, this duty extends to digital assets, and has been expanded by laws and regulations that impose specific privacy and cyber security obligations on companies. This is the third biennial survey that Carnegie Mellon CyLab has conducted on how boards of directors and senior management are governing the security of their organizations' information, applications, and networks (digital assets). First conducted in 2008 and carried forward in 2010 and 2012, the surveys are intended to measure the extent to which cyber governance is improving. The 2012 survey is the first global governance survey, comparing responses from industry sectors and geographical regions. http://www.EnergyCollection.us/Energy-Security/Governance-Enterprise-Security.pdf Original link at: http://www.rsa.com/innovation/docs/CMU-GOVERNANCE-RPT-2012-FINAL.pdf last accessed 2014-05-23 Top
- Top

Center for the Study of the Presidency & Congress – CSPC

- ***Website*** - http://www.thepresidency.org/
- ***Securing The U.S. Electrical Grid*** – 2014-07-01 – 180 pages - This project has sought to address these challenges and begin a new conversation about the security of a changing grid. Through off-the-record roundtable discussions with experts from government, the private sector, and the policy community, this project has examined the threats of cyberattack, physical attack, electromagnetic pulse, and severe weather. We have explored how the executive branch organizes itself to address the security of critical infrastructure—focusing on the grid. We have analyzed the path of legislation related to grid security and the political obstacles it faces. We have discussed how the private sector can better support and incentivize best practices and innovations for security and reliability. We have looked at what the future of the grid may hold in terms of both new technology and a shift to renewable energy. Top

Certificate Management for Embedded Industrial Systems - 2009-11-11 - presentation by ABB - http://www.EnergyCollection.us/Energy-Security/Certificate-Management-Embedded.pdf Top

Chertoff Group

Addressing the Dynamic Threats to the Electric Power Grid Through Resilience – 2014-11-01 – by the Chertoff Group - The U.S. electric power grid is an interconnected system made up of power generation, transmission, and distribution infrastructure. The grid comprises nearly 6,000 power stations and other small generation facilities; 45,000 substations connected by approximately 200,000 miles of transmission lines; and local distribution systems that move power to customers through overhead and underground cables.1 Often called "the largest machine in the world," the U.S. electric power grid is considered "uniquely critical" 2 because it enables and supports other critical infrastructure sectors, including the oil and natural gas, water, transportation, telecommunications, and financial sectors. The use of electricity is ubiquitous across these critical infrastructure sectors, and our society's dependence on electricity continues to increase. The electric power industry understands the critical service it provides and the impact that could result should the electric grid or the ability to deliver electricity be disrupted or damaged. The industry also recognizes that there is no single solution that can completely eliminate each and every risk to the grid. As a result, the industry works closely with government and other industry partners to apply an effective risk management approach focused on ensuring a reliable and resilient electric grid that can quickly recover and restore critical services to customers when power disruptions occur. This partnership informs necessary investments to better plan for and prevent highly consequential incidents and to strengthen capabilities to respond and recover quickly with minimal disruption or damage. This report reviews the electric power industry's efforts to protect the grid and to protect against possible harm to our nation's power supply. It also recommends further initiatives that can help to strengthen and enhance resiliency. http://www.EnergyCollection.us/Companies/Chertoff/Addressing-Dynamic-Threats.pdf Top

Chertoff Group (above) Top

CIP Version 5 Supports Unidirectional Security Gateways **-** by Paul Feldman and Lior Frenkel - 2013-05-01 - published by DHS ICS-CERT - The NERC CIP Version 5 draft standard was recently submitted to FERC for approval. The submitted draft recognizes that Unidirectional Security Gateways provide security which is stronger than firewalls, and the draft includes measures to encourage the deployment of this strong security technology. The standard also changes how firewalls must be managed and mandates network intrusion detection systems as a second level of defense when control centers deploy firewalls. http://www.EnergyCollection.us/Energy-Security/CIP-Version-5-Supports.pdf and http://ics-cert.us-cert.gov/May-2013-Whitepaper-and-Presentation-Submissions Top

CIP Version 5: What Does it Mean for Utilities? **-** http://www.EnergyCollection.us/Energy-Security/CIP-Version-5.pdf Top

Cisco 2014 Annual Security Report **-** In this report, Cisco offers data on and insights into top security concerns, such as shifts in malware, trends in vulnerabilities, and the resurgence of distributed denial-ofservice (DDoS) attacks. The report also looks at campaigns that target specific organizations, groups, and industries, and the growing sophistication of those who attempt to steal sensitive information. The report concludes with recommendations for examining security models holistically and gaining visibility across the entire attack continuum—before, during, and after an attack. http://www.EnergyCollection.us/Energy-Security/Cisco-2014-Annual.pdf Top

Classification Method and Key Measures – Cybersecurity for Industrial Control Systems - This document is based on the findings of the working group on Industrial Control System cybersecurity, directed by the French Network and Information Security Agency, the ANSSI. Composed of actors in the field of automated industrial process control systems and specialists in IT Security, the group has undertaken to draft a set of measures to improve the cybersecurity of ICS. These documents will be used to define the methods for applying the measures set out within the framework of French law No. 2013-1168 of 18 December 2013, known as the Military programming law (LPM). The objective is to subject all new critical ICSs to an approval process, thus ensuring that their cybersecurity level is acceptable given the current threat status and its potential developments. The document is intended for all actors (e.g. responsible entities, project managers, buyers, manufacturers, integrators, prime contractors) concerned with the design, implementation, operation and maintenance of ICSs. http://www.EnergyCollection.us/Countries/France/Classification-Method-Key.pdf Top

- On page 10 the document defines 3 Classes of assets of increasing importance: ***Class 1:*** ICSs for which the risk or impact of an attack is low. The measures recommended for this class must be able to be applied in complete autonomy. ***Class 2:*** ICSs for which the risk or impact of an attack is significant. There is no state control over this class of ICS, but in the event of inspection or incident, the responsible entity must be able to provide evidence that adequate measures have been implemented. ***Class 3:*** ICSs for which the risk or impact of an attack is critical. In this class, the obligations are heightened and the conformity of ICSs is verified by the state authority or an accredited body.
- Starting on page 15 – requirements for use of unidirectional gateways are spelled out for Class 2 and Class 3 assets:
- Class 2: The following are recommendations regarding different types of interconnection. ICSs: ICSs: Partitions using firewalls should be established between class 2 ICSs. Certified devices should be used for the interconnection. The interconnection of a class 2 ICS and a class 1 ICS should be unidirectional towards the class 1 system. Certified devices should be used for the interconnection. Management Information Systems: Interconnection should be unidirectional from the ICS towards the corporate network. Otherwise, all data streams towards the class 2 ICS should be clearly defined and limited. Associated risks should be identified and evaluated. The interconnection shall be implemented using cybersecurity devices such as a firewall, which should be certified. Public network: ICSs should not be exposed on the Internet unless it is imperatively justified by an operational requirement. Where appropriate, they should not be exposed without protection and the risks associated with such a solution should be clearly identified. The interconnection should be unidirectional towards the public network. Certified devices should be used for the interconnection.
- Class 3: The following are recommendations regarding different types of interconnection. ICSs: Partitions using firewalls shall be established between class 3 ICSs. It is strongly recommended to implement the interconnection using certified devices. The interconnection of a class 3 ICS with an ICS of a lower class shall be unidirectional towards the latter. The unidirectionality shall be guaranteed physically (e.g. with a data diode). Certified devices should be used for the interconnection. Management Information Systems: The interconnection shall be unidirectional towards

the corporate network. The unidirectionality shall be guaranteed physically (e.g. with a data diode). Certified devices should be used for the interconnection. Public network: A class 3 ICS shall not be connected to a public network.

Cloud Security Alliance – CSA - is a not-for-profit organization with a mission to promote the use of best practices for providing security assurance within Cloud Computing, and to provide education on the uses of Cloud Computing to help secure all other forms of computing. The Cloud Security Alliance is led by a broad coalition of industry practitioners, corporations, associations and other key stakeholders. https://cloudsecurityalliance.org Top

Congress

- ***Congressional Testimony – 2014-04-10*** **-** Committee on Energy and Natural Resources, United States Senate, hearing on keeping the lights on – are we doing enough to ensure the reliability and security of the U.S. electric grid – http://www.EnergyCollection.us/Energy-Security/Congressional-Testimony-2014-04-10.pdf Top
- ***Congressional Testimony – 2012-07-17*** – Committee on Energy and Natural Resources, United States Senate, Second session to examine the status of action taken to ensure that the electric grid is protected from cyber attacks – http://www.EnergyCollection.us/Energy-Security/Congressional-Testimony-2012-07-17.pdf Top

Congressional Research Service

- ***Website*** – http://www.crs.gov
- ***Cybersecurity: Authoritative Reports and Resources, by Topic*** – http://www.EnergyCollection.us/Companies/Congressional-Research-Service/Cybersecurity-Authoritative-Reports.pdf Top
- ***The Smart Grid and Cybersecurity = Regulatory Policy and Issues*** – 2011-05-15 – http://www.EnergyCollection.us/Companies/Congressional-Research-Service/Smart-Grid-Cybersecurity.pdf Top
    - ***The Stuxnet Computer Worm: Harbinger of an Emerging Warfare Capability*** – http://www.EnergyCollection.us/Companies/Congressional-Research-Service/Stuxnet_Computer_Worm.pdf Top
- ***Terrorist Use of the Internet: Information Operations in Cyberspace*** – 2011-03-08 – 19 pages – http://www.Companies/Congressional-Research-Service/Terrorist_Use_Internet.pdf Top

Connecticut

Cybersecurity and Connecticut's Public Utilities **-** 2-14-04-14 - by the state PUC - Cyber threats pose serious potential damage to Connecticut's public utilities. Connecticut's public officials and utilities need to confront these threats and detect, deter and be prepared to manage the effects of a cyber disruption. Governor Dannel P. Malloy and Connecticut's General Assembly initiated this report through adoption of the state's Comprehensive Energy Strategy in 2013. They directed the Public Utilities Regulatory Authority (PURA) to review the state's electricity, natural gas and major water companies and to assess the adequacy of their capabilities to deter interruption of service and to present to the Governor and General Assembly recommended actions to strengthen deterrence. This report is offered as a starting point toward defining regulatory guidance specifically for defensive cyber strategies.

Top

Council on Cybersecurity -an independent, expert, not-for-profit organization with a global scope committed to the security of the open Internet. Technology practice area is built upon the Critical Security Controls (the Controls), a recommended set of actions for cyber defense that provide specific and actionable ways to thwart the most pervasive attacks. The Controls have been developed and maintained by an international, grass-roots consortium which includes a broad range of companies, government agencies, institutions, and individuals from every part of the ecosystem (threat responders and analysts, security technologists, vulnerability-finders, tool builders, solution providers, front-line defenders, users, consultants, policy-makers, executives, academia, auditors, etc.) who have banded together to create, adopt, and support the Controls. http://www.counciloncybersecurity.org/critical-controls/ Top

Council on Foreign Relations on Cybersecurity **-** is an independent, nonpartisan membership organization, think tank, and publisher. CFR members, including Brian Williams, Fareed Zakaria, Angelina Jolie, Chuck Hagel, and Erin Burnett, explain why the Council on Foreign Relations is an indispensable resource in a complex world. http://www.cfr.org/issue/cybersecurity/ri18 Top

CRISP - Cybersecurity Risk Information Sharing Program **-** CRISP is a pilot program that provides a near-real-time capability for critical infrastructure owners and operators to share and analyze cyber threat data and receive Machine-to-machine mitigation measures. Developed by a number of power sector companies, in conjunction with the ES-ISAC, DOE, Pacific Northwest National Laboratory, and Argonne National Laboratory. CRISP is an information sharing software system that NERC may incorporate into ES-ISAC. http://tinyurl.com/jvn2fcc Top

Critical Infrastructure in Wikipedia **-** Wikipedia - http://en.wikipedia.org/wiki/Critical_infrastructure Top

Critical Infrastructure Protection in Wikipedia **-** Wikipedia - http://en.wikipedia.org/wiki/Critical_infrastructure_protection Top

Critical Infrastructure Protection - Cybersecurity Guidance Is Available, but More Can Be Done to Promote Its Use - GAO Report - 2012-12-01 - A wide variety of cybersecurity guidance is available from national and international organizations for entities within the seven critic a l infrastructure sectors GAO reviewed — banking and finance; communications; energy; health care and public health; information technology; nuclear reactors, material, and waste; and water . Much of this guidance is tailored to business needs of entities or provides methods to address unique risks or operations . In addition, entities operating in regulated environments are subject to mandatory standards to meet their regulatory requirements; entities operating outside of a regulatory environment may voluntarily adopt standards and guidance. While private sector coordinating council representatives confirmed lists of cybersecurity guidance that they stated w ere used within their respective sectors, the representatives emphasized that the lists were not comprehensive and that additional standards and guidance are likely used. http://www.EnergyCollection.us/Energy-Security/Cybersecurity-Guidance-Available.pdf Top

Cyber-Physical Systems Security for Smart Grid **-** Future Grid Initiative White Paper - http://www.EnergyCollection.us/Energy-Security/Cyber-Physical-Systems.pdf Top

Cyber Risk and the Board of Directors - Closing the Gap - http://www.EnergyCollection.us/Energy-Security/Cyber-Risk-Board.pdf Top

Cyber Security for Smart Grid, Cryptography, and Privacy **-** 2011-07-01 - In this paper, we will study smart grid security in more depth. The goal of this paper is to cover the security challenges related to cyber security, and we will also study how cryptography is used in order to eliminate cyber-attacks. Finally, we will also discuss in brief privacy which is another smart grid security concern. The rest of the paper is organized as follows. We start by reviewing the challenges and goals of smart grid in Section 2. This is followed by the smart grid architecture in Section 3. We focus on cyber security in Section 4. Section 5 explains cryptography used for smart grid security in depth. Privacy in context with smart grid security is explained in Section 6. And finally, we conclude in Section 7. http://www.EnergyCollection.us/Energy-Security/Cyber-Security-Smart-Grid.pdf Top

Cyber Security Standards in Wikipedia **-** http://en.wikipedia.org/wiki/Cyber_security_standards Top

Cyber Security Standards (NERC) in Wikipedia **-** *http://en.wikipedia.org/wiki/Cyber_security_standards#NERC* Top

Cyber Solutions Handbook - Making Sense of Standards and Frameworks **-** 2014-03-17 by Booz Allen Hamilton - http://www.EnergyCollection.us/Energy-Security/Cyber-Solutions-Handbook.pdf Top

Cyber threats Proving Their Power over Power Plant Operational Technology – 2015-02-01 by Michael Assante – http://www.EnergyCollection.us/Energy-Security/Cyber-Threats-Proving.pdf Top

Cyber War - Hardening SCADA **-** The year 2011 may have forever changed the way we think about the security of networks and systems. Following a year many are calling the “year of the hack,” security professionals have fundamentally changed their outlook when it comes to the threat of a network breach. Whereas previously, many considered a breach unlikely and more of an “if” scenario, many have shifted to a mindset of “when.” Week after week one company after another was breached with high profile impact. Unfortunately public utilities were no different. In November 2011, the deputy assistant director of the FBI's Cyber Division, Michael Welch, told a London cyber security conference that hackers had recently accessed the critical infrastructure in three U.S. cities by compromising their Internet-based control systems. http://www.EnergyCollection.us/Energy-Security/Cyber-War-Hardening.pdf Top

Cyberattack Insurance a Challenge for Business – http://www.EnergyCollection.us/Energy-Security/Cyberattack-Insurance-Challenge.pdf Top

Cybersecurity Best Practices for Small and Medium Pennsylvania Utilities – http://www.EnergyCollection.us/States/Pennsylvania/Cybersecurity-Best-Practices.pdf Top

Cybersecurity and the Board: Avoiding Personal Liability - Part I of III: Policies and Procedures **-** http://www.EnergyCollection.us/Energy-Security/Cybersecurity-Board-Avoiding-I.pdf   Top

Cybersecurity and the Board: Avoiding Personal Liability - Part II of III: Policies and Procedures **-** http://www.EnergyCollection.us/Energy-Security/Cybersecurity-Board-Avoiding-II.pdf   Top

Cybersecurity and the Board: Avoiding Personal Liability - Part III of III: Policies and Procedures **-** http://www.EnergyCollection.us/Energy-Security/Cybersecurity-Board-Avoiding-III.pdf   Top

Cybersecurity and Remote Access – SPARK Article **-** The conversation regarding IT security is shifting. Until recently, most of the major hacking incidents were conducted by financially-motivated hackers out to steal proprietary data. They often targeted large retail companies that store thousands of credit card records, such as the highly-publicized T.J. Maxx data breach in 2007. But today hacktivism and cyber terrorism are growing as real threats to both public and private organizations. Because hacktivists are motivated by creating disruption versus financial gain, public utilities have been pushed further into the spotlight as potential targets.   http://www.EnergyCollection.us/Energy-Security/Cybersecurity-Remote-Access.pdf   Top

Cybersecurity Risks and the Board of Directors – Harvard Article http://www.EnergyCollection.us/Energy-Security/Cybersecurity-Risks-Board.pdf   Top

Cybersecurity for Utilities: The Rest of the Story **-** by Jim Rowan of SERC - presentation about growing cyber and physical risk to utilities - http://www.EnergyCollection.us/Companies/SERC/Cybersecurity-Utilities-Rest.pdf   Top

Dark Reading – Cyber News **-** is a comprehensive news and information portal that focuses on IT security, helping information security professionals manage the balance between data protection and user access.   Website: http://www.darkreading.com   Top

The ***Debate Over Cyber Threats*** - http://www.EnergyCollection.us/Energy-Security/Debate-Over-Cyber.pdf   Top

Dell

- ***Dell Cybersecurity webpage –*** http://www.dell.com/learn/us/en/84/campaigns/slg-pov-cybersecurity
- **How Traditional Firewalls Fail Today's Networks - and Why Next-Generation Firewalls Will Prevail - Dell** **-** http://www.EnergyCollection.us/Energy-Security/How-Traditional-Firewalls.pdf   Top
- Top

Deloitte **–** see the Center for corporate governance – http://www.corpgov.deloitte.com   Top

- ***Cybersecurity and the Audit Committee - Deloitte*** **-** A Deloitte Audit Committee Brief - http://www.EnergyCollection.us/Energy-Security/Cybersecurity-Audit-

Committee.pdf Original at http://deloitte.wsj.com/riskandcompliance/2013/08/30/cybersecurity-and-the-boardroom/ accessed 2014-05-11 Top

- ***Cybersecurity...Continued in the Boardroom*** **-** The August 2013 Deloitte Audit Committee Brief highlighted organizational roles and responsibilities for cybersecurity, beginning with the board of directors and audit committee. This article continues the discussion with further information on the board's role related to cybersecurity. http://www.EnergyCollection.us/Energy-Security/cybersecurity-Continued-Boardroom.pdf Top
- ***Deloitte - Audit Committee Brief - 2014-05-01*** **-** includes "Questions the audit committee may consider asking management to assess the company's readiness to prevent and respond to cyber attacks" http://www.EnergyCollection.us/Companies/Deloitte/Audit-Committee-Brief-2014-05-01.pdf Top
- ***SEC's Focus on Cybersecurity*** – Key insights for investment advisors – http://EnergyCollection.us/Companies/Deloitte/SECs-Focus-Cybersecurity.pdf
- Top

Department of Energy - DOE

- ***2012 DOE Smart Grid Cybersecurity Information Exchange*** **-** 2012-12-05-06 - Recipients of the American Recovery and Reinvestment Act of 2009 (ARRA) Smart Grid Investment Grants (SGIG) and Smart Grid Demonstration Program (SGDP) are in the midst of installing nearly $8 billion in advanced smart grid technologies and systems that could dramatically change the way electricity is produced, managed, and used in the United States. One of the key challenges for utilities is to implement smart grid devices and systems while ensuring and enhancing the cybersecurity of these digital systems. Toward this end, the 2012 DOE Smart Grid Cybersecurity Information Exchange (2012 Information Exchange) held in Washington, DC on December 5 and 6, 2012, enabled SGIG and SGDP recipients to: (1) share information and lessons learned in developing and implementing their Cybersecurity Plans (CSP); (2) learn about available tools, techniques, and resources for strengthening the security of cyber systems; and (3) gain a common understanding of how to sustain cybersecurity processes once the ARRA projects are completed. Through interactive peer-to-peer exchanges, panel discussions, expert presentations, and poster sessions, attendees of the 2012 Information Exchange discussed critical issues and insights arising from the implementation of their cybersecurity programs and looked to the future of cybersecurity for the electric grid. These discussions produced important lessons learned and best practices from implementing cybersecurity in smart grid systems. http://www.EnergyCollection.us/Energy-Security/2012-DOE-Smart-Grid.pdf Top
- ***AMI Penetration Test Plan*** **-** This security test plan template was created by the National Electric Sector Cybersecurity Organization Resource (NESCOR) to provide guidance to electric utilities on how to perform penetration tests on AMI systems. Penetration testing is one of the many different types of assessments utilities can perform to assess their overall security posture. While NESCOR recommends that utilities engage in all other forms of security assessment, NESCOR created this document to help utilities plan and organize their AMI penetration testing efforts. For a list of other types of Smart Grid security assessments, please see NESCOR's whitepaper titled "Guide to Smart Grid Assessments." For a list of other NESCOR Penetration Test Plan documents that cover other systems such as Wide-Area Monitoring, Protection, and Control (WAMPAC), Home Area Network (HAN), or Distribution Management, please see NESCOR's website or contact one of the persons listed

above. http://www.EnergyCollection.us/Energy-Security/AMI-Penetration-Test.pdf Top

- ***Analysis of Selected Electric Sector High Risk Failure Scenarios*** **-** NESCOR - 2013-09-01 - These provide detailed analyses for a subset of the failure scenarios identified in the short failure scenario document listed above. All analyses presented include an attack tree, which details in a formal notation, the logical dependencies of conditions that allow the failure scenario to occur. Several of the analyses also provide a detailed text write up for the scenario, in addition to the attack trees. Failure scenarios in the short failure scenario document were prioritized for inclusion in this document, based upon level of risk for the failure scenario, and the priorities of NESCOR utility members. http://www.EnergyCollection.us/Energy-Security/Analysis-Selected-Electric.pdf Top
- ***Argonne National Lab*** **-** http://www.dis.anl.gov/projects/cybersecurity.html Top
- ***Cyber security procurement language for control systems*** **-** from DOE at http://energy.gov/oe/downloads/cyber-security-procurement-language-control-systems-version-18 Top
- ***Cybersecurity Website Page on DOE*** **-** http://energy.gov/oe/services/cybersecurity Top
- ***Electricity Subsector - Risk Management Process*** **-** 2012-05-12 - by DOE/OE-0003 - The electricity subsector1 cybersecurity Risk Management Process (RMP) guideline has been developed by a team of government and industry representatives to provide a consistent and repeatable approach to managing cybersecurity risk across the electricity subsector. It is intended to be used by the electricity subsector, to include organizations responsible for the generation, transmission, distribution, and marketing of electric power, as well as supporting organizations such as vendors. The RMP is written with the goal of enabling organizations— regardless of size or organizational or governance structure - to apply effective and efficient risk management processes and tailor them to meet their organizational requirements. This guideline may be used to implement a new cybersecurity program within an organization or to build upon an organization's existing internal cybersecurity policies, standard guidelines, and procedures. http://www.EnergyCollection.us/Energy-Security/Electricity-Subsector-Cybersecurity-Risk.pdf Original Link - http://tinyurl.com/mrtd6n8 Top
- ***Energy Sector Cybersecurity Framework Implementation Guidance*** – 2015-01-01 – the National Institute of Standards and Technology (NIST) released the voluntary Cybersecurity Framework (Framework) in February 2014 to provide a common language organizations can use to assess and manage cybersecurity risk. Developed in response to Executive Order (EO) 13636 "Improving Critical Infrastructure Cybersecurity" of February 2013, the Framework recommends risk management processes that enable organizations to inform and prioritize decisions regarding cybersecurity based on business needs, without additional regulatory requirements. It enables organizations—regardless of sector, size, degree of cybersecurity risk, or cybersecurity sophistication—to apply the principles and best practices of risk management to improve the security and resilience of critical infrastructure. Each sector and individual organization can use the Framework in a tailored manner to address its cybersecurity objectives. Energy sector organizations have a strong track record of working together to develop cybersecurity standards, tools, and processes that ensure uninterrupted service. The U.S. Department of Energy (DOE), as the Energy Sector-Specific Agency (SSA), worked with the Energy Sector Coordinating Councils and other SSAs to develop this Framework Implementation Guidance specifically for energy sector owners and operators. It is tailored to the energy sector's risk environment and existing cybersecurity and risk management tools and processes that organizations can use to implement the Framework. This Framework Implementation Guidance is designed to assist energy sector organizations to: Characterize their current and target cybersecurity posture.

Identify gaps in their existing cybersecurity risk management programs, using the Framework as a guide, and identify areas where current practices may exceed the Framework. Recognize that existing sector tools, standards, and guidelines may support Framework implementation. Effectively demonstrate and communicate their risk management approach and use of the Framework to both internal and external stakeholders. Section 2 provides key Framework terminology and concepts for its application, and Section 3 identifies example resources that may support Framework use. Section 4 outlines a general approach to Framework implementation, followed in Section 5 by an example of a tool-specific approach to implementing the Framework. The tool selected for this example is the DOE- and industry-developed Cybersecurity Capability Maturity Model (C2M2; DOE 2014a). Energy sector organizations, particularly those that are using the Framework to establish a new security risk management program are invited to contact DOE via email at cyber.framework@hq.doe.gov with any questions or requests for direct assistance. http://www.EnergyCollection.us/Companies/DOE/Energy-Sector-Cybersecurity-1.pdf Top

- ***Gridwise Architecture Council*** **-** was formed by the U.S. Department of Energy to promote and enable interoperability among the many entities that interact with the nation's electric power system. The GWAC members are a balanced and respected team representing the many constituencies of the electricity supply chain and users. The GWAC maintains a broad perspective of the GridWise vision and provides industry guidance and tools that make it an available and practical resource for the various implementations of Smart Grid technology. http://www.gridwiseac.org/about/mission.aspx Top
- ***Idaho National Lab*** - http://www.inl.gov/nationalsecurity/capabilities/security/ Top
- ***Implementing Effective Enterprise Security Governance - DOE*** **-** Outline for energy Sector Executives and Boards - As recent attacks, Presidential Executive Order for Improving Critical Infrastructure Cybersecurity, and Presidential Policy Directive 21 for Critical Infrastructure Security and Resilience have illustrated, managing security risks to our most important organizations and systems, including the electric grid, has become a national security priority. Enterprise security program effectiveness for both physical and cyber is now a CEO and Board-level concern and is called out as essential in the Department Of Energy's Electric Sector-Cybersecurity Capability Maturity Model (ES-C2M2). Responsibility for physical and cyber security belongs not solely to technical, risk, or compliance specialists, but rather to the entire organization. It begins with senior leadership and extends throughout the enterprise to foster a more security-aware culture. http://www.EnergyCollection.us/Energy-Security/Implementing-Effective-Enterprise.pdf Original link - http://tinyurl.com/qgqnqcr (DOE Site) Top
- ***Infrastructure Security and Energy Restoration*** - http://energy.gov/oe/mission/infrastructure-security-and-energy-restoration-iser Top
- ***National Electric Sector Cybersecurity Organization - NESCO*** **-** In an attempt to stimulate greater partnership and information sharing, H.R. 3183 required that "...the Secretary shall establish an independent national energy sector cyber security organization..." In response, the Department of Energy issued a Funding Opportunity Announcement (FOA) on March 31, 2010. Two organizations received awards under this FOA. EnergySec and the Electric Power Research Institute (EPRI) were selected to form the National Electric Sector Cybersecurity Organization (NESCO). EPRI serves as the research and analysis resource for NESCO as the National Electric Sector Cybersecurity Organization Resource (NESCOR). The two organizations serve as a focal point to bring together domestic and international experts, developers, and users who are working to strengthen the cybersecurity posture of the electric sector by establishing a broad-based public-private partnership for collaboration and cooperation. This includes

complementing and enhancing the development and implementation of key milestones and objectives called for in the Roadmap to Secure Control Systems in the Energy Sector. It is expected that NESCO/NESCOR will work cooperatively with the Department of Energy, other Federal agencies, the Information Sharing and Analysis Center for the Electric Sector (ES-ISAC), and industry. http://energy.gov/oe/services/cybersecurity/nesco http://www.us-nesco.org/ Top

- ***National Electric Sector Cybersecurity Organization Resource - NESCOR***
  - ***Electric Sector Failure Scenarios and Impact Analyses - NESCOR*** - 2013-09-01 - This document contains cyber security failure scenarios and impact analyses for the electric sector for the six domains: advanced metering infrastructure, distributed energy resources, wide area monitoring, protection, and control, electric transportation, demand response, and distribution grid management. A cyber security failure scenario is a realistic event in which the failure to maintain confidentiality, integrity, and/or availability of sector cyber assets creates a negative impact on the generation, transmission, and/or delivery of power. Also included are evaluation criteria and common mitigations. http://www.EnergyCollection.us/Energy-Security/Electric-Sector-Failure.pdf Top
  - ***ERPI NESCOR Webpage*** **-** http://www.smartgrid.epri.com/nescor.aspx Top
  - ***NESCOR Guide to Penetration Testing for Electric Utilities - Version 3*** - This security test plan template was created by the National Electric Sector Cybersecurity Organization Resource (NESCOR) to provide guidance to electric utilities on how to perform penetration tests on Smart Grid systems. Penetration testing is one of the many different types of assessments utilities can perform to assess their overall security posture. While NESCOR recommends that utilities engage in all other forms of security assessment, NESCOR created this document to help utilities plan and organize their AMI penetration testing efforts. For a list of other types of Smart Grid security assessments, please see NESCOR's whitepaper titled "Guide to Smart Grid Assessments." This document covers penetration test plans for Smart Grid systems in general with specific guidance for Advanced Metering Infrastructure (AMI), Wide-Area Monitoring, Protection, and Control (WAMPAC), and Home Area Network (HAN). Additional guidance for other Smart Grid product domains are expected to be added in later revisions of this document. For more information on this or other NESCOR documents, see the NESCOR's website at www.smartgrid.epri.com/NESCOR.aspx The objective of the NESCOR project is to establish an organization that has the knowledge and capacity to enhance the effort of the National Electric Sector Cybersecurity Organization (NESCO) by providing technical assessments of power system and cybersecurity standards to meet power system security requirements;; provide recommendations for threats and vulnerabilities, and participate in testing emerging security technologies in labs and pilot projects. http://www.EnergyCollection.us/Energy-Security/NESCOR-Guide-Penetration.pdf Top
  - ***Smart Energy Profile (SEP)*** **-** 2011-10-31 - Load control capabilities in Home Area Networks (HANs) are an integral part of the smart grid and energy efficiency modernization efforts currently underway. Like other smart grid systems, HANs are vulnerable to cyber-attacks and adequate security measures are needed. The ZigBee Smart Energy Profile 1.0 and Smart Energy Profile 1.1 (collectively referred to in this white paper as SEP 1.x) present a

communication framework for HAN devices along with a security framework. This white paper builds upon prior efforts that assessed the security of SEP 1.x with a primary objective to help stakeholders understand the vulnerabilities in SEP 1.x and provide them with actionable advice on how to mitigate or minimize these vulnerabilities. This white paper goes beyond prior work in several aspects. Included are several representative system architectures and the Texas public utilities commission architecture. These representative architectures assist in understanding the results of the security analysis. This white paper lists the differences between versions SEP 1.0 and 1.1 of the specifications, which will help the relevant stakeholders to understand the applicability of this document on their HANs. Finally, this document presents potential vulnerabilities, impacts, best practices, and mitigations for SEP 1.x. http://www.EnergyCollection.us/Energy-Security/Smart-Energy-Profile.pdf Top

  - ***Wide Area Monitoring, Protection, and Control Systems (WAMPAC) - Standards for Cyber Security Requirements*** **-** 2012-10-26 - The National Electric Sector Cybersecurity Organization Resource (NESCOR) Technical Working Group 2 (TWG2) has been examining issues of cyber security requirements and coverage in related standards. As a part of that effort, several domain areas of interest were identified. This report summarizes findings related to the cyber security requirements as reflected in the Wide Area Monitoring, Protection, and Control (WAMPAC) standards. The findings are discussed in the context of the recently published WAMPAC Advanced Security Acceleration Project for the Smart Grid (ASAP-SG) and the National Institute of Standards and Technology Interagency Report (NISTIR) 7628 reports, on-going WAMPAC related standards development, existing cyber security standards, and on-going cyber security reviews of standards conducted through the Smart Grid Interoperability Panel (SGIP). This document sets the stage by discussing some general WAMPAC solution characteristics relevant for cyber security considerations. http://www.EnergyCollection.us/Energy-Security/Wide-Area-Monitoring.pdf Top
  -
  - Top

- ***Office of Electric Delivery & Energy Reliability – NESCO*** - In an attempt to stimulate greater partnership and information sharing, H.R. 3183 required that "...the Secretary shall establish an independent national energy sector cyber security organization..." In response, the Department of Energy issued a Funding Opportunity Announcement (FOA) on March 31, 2010. Two organizations received awards under this FOA. EnergySec and the Electric Power Research Institute (EPRI) were selected to form the National Electric Sector Cybersecurity Organization (NESCO). EPRI serves as the research and analysis resource for NESCO as the National Electric Sector Cybersecurity Organization Resource (NESCOR). http://energy.gov/oe/services/cybersecurity/nesco Top
- ***Pacific Northwest National Laboratory – PNNL*** - PNNL works across the entire lifecycle of cyber security, from detection through delivery of actionable knowledge, making the most of our successes in: Large-scale situational awareness. PNNL uses an open sensor architecture that incorporates research on the next generation of sensor capabilities; data processing with cost-effective, scalable architectures; and near real-time analysis. Modeling and simulation of cyber systems and networks, featuring cyber flight simulator tools to evaluate security performance, scalable training, and real life exercises that can cross among and between organizations. Critical infrastructure assessments and protection, with an industry-standard control system laboratory to

study vulnerabilities, the ability to work with government and industry leaders to rapidly adapt new secure protocols within a laboratory environment, and a multi-agency partnership approach to further understand how to produce and design safer and more secure control infrastructure systems. Adaptive Systems Cyber analytics for detection and discovery, where human and machine capabilities work collaboratively to ingest, process, and derive knowledge; incorporate nontraditional and heterogeneous information sources; create interactive visual interfaces; discover malicious intent that appears as benign cyber data; and scale across diverse user environments. High-performance data-intensive architectures that collect, manage, analyze, and understand data at volumes and rates which push the frontier of current technologies. http://www.pnl.gov/nationalsecurity/program/homeland/cyber_security/ http://cybersecurity.pnnl.gov/ Top

- **Sandia National Lab** - http://www.sandia.gov/missions/defense_systems/cybersecurity.html Top
- Top

Department of Defense – DoD

- The Office of Cybersecurity and Communications (CS&C) works with state and local government as well as private sector partners to minimize the impact of cybersecurity incidents. Two of CS&C's National Cybersecurity and Communications Integration Center components, the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) and United States Computer Emergency Readiness Team (US-CERT) work to mitigate cybersecurity incidents in close coordination with public and private sector partners. ICS-CERT provides onsite support to owners and operators of critical infrastructure, including incident response, forensic analysis, and site assessments. ICS-CERT also provides tools and training designed to increase stakeholder awareness of the threats posed to industrial control systems. The ICS-CERT website provides various resources for owners and operators of critical infrastructure and the industrial control systems that operate many of the key functions of their facilities, such as SCADA system. The website contains links to resources such as alerts, advisories, newsletters, training, recommended practices, as well as a large list of standards and references. The ICS-CERT website can be found here: https://ics-cert.us-cert.gov. ICS cyber incidents can be reported to: ics-cert@hq.dhs.gov .
- **CERT** – A Division of the Software Engineering Institute (sponsored by DoD) enriched by its connection to the internationally respected Carnegie Mellon University. The CERT Division works closely with the Department of Homeland Security (DHS) to meet mutually set goals in areas such as data collection and mining, statistics and trend analysis, computer and network security, incident management, insider threat, software assurance, and more. The results of this work include exercises, courses, and systems that were designed, implemented, and delivered to DHS and its customers as part of the SEI's mission to transition SEI capabilities to the public and private sectors and improve the practice of cybersecurity. http://www.cert.org/ Top
- ***Insider Threat Center of CERT*** - http://www.cert.org/insider_threat/ Top
- **Software Engineering Institute** - serves the nation as a Federally Funded Research and Development Center (FFRDC) sponsored by the U.S. Department of Defense (DoD) and based at Carnegie Mellon University, a global research university annually rated among the best for its programs in computer science and engineering. http://www.sei.cmu.edu/about/ Top
  - ***Insider Fraud in Financial Services Illicit Cyber Activity Involving Fraud in the U.S. Financial Services Sector – Software Engineering Institute*** - Insiders pose a substantial threat to financial services companies by virtue of their knowledge of and access to proprietary systems and their ability to bypass security measures

through legitimate means. Insider fraud is perpetrated by a malicious insider, which is a current or former employee, contractor, or other business partner who has or had authorized access to an organization's network, system, or data and intentionally exceeded or misused that access in a manner that negatively affected the confidentiality, integrity, or availability of the organization's information or information systems. http://www.EnergyCollection.us/Energy-Security/Insider-Fraud-Financial.pdf Top

- ***Insider Threat Study: Illicit Cyber Activity Involving Fraud in the U.S. Financial Services Sector – Software Engineering Institute*** **-** Cyber-crimes committed by malicious insiders are among the most significant threats to networked systems and data. When developing policies and procedures for responding to cyber security events, it is important to consider the insider threat. A malicious insider is a trusted insider who abuses his trust to disrupt operations, corrupt data, exhilarate sensitive information, or compromise an IT (information technology) system, causing loss or damage. Left unchecked, their rogue actions may compromise the nation's ability to fend off future attacks and safeguard critical infrastructure assets, such as the electric power grid. In fact, some of the most damaging attacks against the government have been launched by trusted insiders. As increased information-sharing exposes sensitive information to more insiders, such attacks will become an increasingly serious threat. Their concerns are shared by the private sector, where corporations maintain valuable, highly sensitive information and financial institutions manage the flow of and access to electronic funds. The research described in this report was sponsored by the Department of Homeland Security Science and Technology Directorate's Homeland Security Advanced Research Projects Agency Cyber Security Division. The work was conducted, and the report written, by members of the CERT® Insider Threat Center at Carnegie Mellon University's Software Engineering Institute. The authors built upon a previous S&T-funded 2004 report, Insider Threat Study: Illicit Cyber Activity in the Banking and Finance Sector, to develop a greater understanding of the behavioral, technical, and organizational factors that lead to insider threat attacks [Randazzo 2004]. Drawing on case files provided by the United States Secret Service, they analyzed actual incidents of insider fraud, from inception to prosecution. As part of their effort, the authors compared the technical security controls commonly used to prevent internal and external attackers. Their findings can be used to inform risk management decisions being made by government and industry and to support law enforcement in cybercrime investigations. 2012-07-01 http://www.EnergyCollection.us/Energy-Security/Insider-Threat-Study.pdf Top

- Top

Department of Homeland Security – DHS

- ***C-Cubed Program*** - The Critical Infrastructure Cyber Community C³ (pronounced "C Cubed") Voluntary Program is the coordination point within the Federal Government for critical infrastructure owners and operators interested in improving their cyber risk management processes. The C³ Voluntary Program aims to: 1) support industry in increasing its cyber resilience; 2) increase awareness and use of the Framework; and 3) encourage organizations to manage cybersecurity as part of an all hazards approach to enterprise risk management. http://www.dhs.gov/about-critical-infrastructure-cyber-community-c%C2%B3-voluntary-program
- ***Catalog of Control Systems Security: Recommendations for Standards Developers*** **-** By DHS,2011-04-01 - This catalog presents a compilation of practices that various industry bodies have recommended to increase the security of control systems from both physical and cyber-attacks. The recommendations in this catalog are

grouped into 19 families, or categories, that have similar emphasis. The recommendations within each family are displayed with a summary statement of the recommendation, supplemental guidance or clarification, and a requirement enhancements statement providing augmentation for the recommendation under special situations. http://www.EnergyCollection.us/Energy-Security/Catalog-Control-Systems.pdf Top

- ***Critical Infrastructure Partnership Advisory Council - CIPAC*** **-** The Department of Homeland Security has established the Critical Infrastructure Partnership Advisory Council (CIPAC) to facilitate effective coordination between federal infrastructure protection programs with the infrastructure protection activities of the private sector and of state, local, territorial and tribal governments. The CIPAC represents a partnership between government and critical infrastructure owners and operators and provides a forum in which they can engage in a broad spectrum of activities to support and coordinate critical infrastructure protection. http://www.dhs.gov/critical-infrastructure-partnership-advisory-council Top
- ***Critical_Infrastructure_Sectors_DHS*** - http://www.dhs.gov/critical-infrastructure-sectors Top
- ***Cybersecurity Webpage on DHS*** **-** http://www.dhs.gov/topic/cybersecurity Top
- ***Electricity Subsector Coordinating Council – ESCC*** - The role of the Electricity Sub-sector Coordinating Council (ESCC) is to foster and facilitate the coordination of sector-wide policy-related activities and initiatives to improve the reliability and resilience of the Electricity Sub-sector, including physical and cybersecurity infrastructure. The ESCC consists of one member from the NERC Board of Trustees (appointed by the board chairperson), the NERC Chief Executive Officer (CEO), five CEO-level executives from NERC member organizations, and the chairperson of the NERC Critical Infrastructure Protection Committee. The key roles of the ESCC are to represent the Electricity Sub-sector, to build relationships with government and other critical infrastructure sectors, and to participate in joint initiatives as part of the "partnership framework" envisioned by the National Infrastructure Protection Plan and Energy Sector-Specific Plan. Some of these initiatives are information requests, while others require regular participation on formally established working groups. The Electricity Sub-sector receives many requests from government departments and agencies and other critical infrastructure sectors to participate in various initiatives. The ESCC keeps informed of these efforts, and participates directly when necessary. It reports to the Department of Homeland Security through the Department of Energy. http://www.nerc.com/pa/CI/Pages/ESCC.aspx and http://www.EnergyCollection.us/Energy-Security/ESCC-Electricity-Subsector.pdf and http://www.nerc.com/comm/Other/Pages/Electricity%20Sub-Sector%20Coordinating%20Council%20ESCC/Electricity-Sub-Sector-Coordinating-Council-ESCC.aspx Council membership - http://www.dhs.gov/energy-electricity-sub-sector Top
    - ***ESCC – Overview presentation*** – 2014-10-06 – http://www.EnergyCollection.us/Energy-Security/ESCC-Overview-2014-10-06.pdf
    - ***Roadmap to Achieve Energy Delivery Systems Cybersecurity*** **-** provides a plan to improve the cybersecurity of the energy sector. The strategic framework within presents the vision of industry, vendors, academia, and government stakeholders for energy delivery systems security, supported by goals and time-based milestones to achieve that vision over the next decade. It marks a continued effort by public and private stakeholders to identify steps to build, deploy, and manage resilient energy delivery systems for the electric, oil, and natural gas industries. http://www.EnergyCollection.us/Energy-Security/Roadmap-Achieve-Energy.pdf Top
- ***Electricity Subsector - Cybersecurity Capability Maturity Model*** **-** 2012-05-31 - This Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2) was

developed in support of a White House initiative led by the Department of Energy (DOE), in partnership with the Department of Homeland Security (DHS), and in collaboration with industry, private sector, and public-sector experts. The model was developed collaboratively with an industry advisory group through a series of working sessions and revised based on feedback from industry experts and pilot evaluations. The advisory group for the initiative included representatives from industry associations, utilities, and government. Additionally, more than 40 subject matter experts (SMEs) from industry participated in development of the model. http://energy.gov/oe/cybersecurity-capability-maturity-model-c2m2-program/electricity-subsector-cybersecurity Top

- ***Enhanced Cybersecurity Services*** - ECS is a voluntary information sharing program that assists critical infrastructure owners and operators as they improve the protection of their systems from unauthorized access, exploitation, or data exfiltration. DHS works with cybersecurity organizations from across the federal government to gain access to a broad range of sensitive and classified cyber threat information. DHS develops indicators based on this information and shares them with qualified Commercial Service Providers (CSPs), thus enabling them to better protect their customers who are critical infrastructure entities. ECS augments, but does not replace, an entities' existing cybersecurity capabilities. http://www.dhs.gov/enhanced-cybersecurity-services Top
- ***Fusion Centers*** - State and major urban area fusion centers (fusion centers) serve as focal points within the state and local environment for the receipt, analysis, gathering, and sharing of threat-related information between the federal government and state, local, tribal, territorial (SLTT) and private sector partners. Located in states and major urban areas throughout the country, fusion centers are uniquely situated to empower front-line law enforcement, public safety, fire service, emergency response, public health, critical infrastructure protection, and private sector security personnel to understand local implications of national intelligence, thus enabling local officials to better protect their communities. Fusion centers provide interdisciplinary expertise and situational awareness to inform decision-making at all levels of government. They conduct analysis and facilitate information sharing while assisting law enforcement and homeland security partners in preventing, protecting against, and responding to crime and terrorism. http://www.dhs.gov/state-and-major-urban-area-fusion-centers Top
- **ICS-CERT Year in Review - Industrial Control Systems Cyber Emergency Response Team 2013 - DOE** - This year, ICS-CERT received and responded to 257 incidents as voluntarily reported by asset owners and industry partners. In 2013, attacks against the Energy sector represented over 56 percent of all incidents reported to ICS-CERT. The scope of incidents encompassed a vast range of threats and observed methods for attempting to gain access to both business and control systems infrastructure, including: • Unauthorized access and exploitation of Internet facing ICS/SCADA devices • Malware infections within air-gapped control system networks (impacting operations) • SQL Injection and application vulnerability exploitation 11 Related to intrusion attempts 9 ICS-CERT Year-in-Review — 2013 • Lateral movement between network zones • Targeted spear phishing campaigns • Watering hole attacks (one of which utilized a zero-day vulnerability) http://www.EnergyCollection.us/Energy-Security/ICS-CERT-Year-In-Review-2013.pdf Top
- ***Implementation Status of the Enhanced Cybersecurity Services Program*** – DHS Office of the Inspector General OIG-14-119 – 2014-07-01 - The National Protection Programs Directorate (NPPD) is primarily responsible for fulfilling the DHS national, non?law enforcement cybersecurity missions. Within NPPD, the Office of Cybersecurity and Communications is responsible for the implementation of the Enhanced Cybersecurity Services program. Our overall objective was to determine the effectiveness of the Enhanced Cybersecurity Services program to disseminate cyber threat and technical information with the critical infrastructure sectors through

commercial service providers. http://www.EnergyCollection.us/Companies/DHS/Implementation-Status-Enhanced.pdf Top

- ***Industrial Control Systems Cyber Emergency Response Team – ICS-CERT*** - The Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) works to reduce risks within and across all critical infrastructure sectors by partnering with law enforcement agencies and the intelligence community and coordinating efforts among Federal, state, local, and tribal governments and control systems owners, operators, and vendors. Additionally, ICS-CERT collaborates with international and private sector Computer Emergency Response Teams (CERTs) to share control systems-related security incidents and mitigation measures. https://ics-cert.us-cert.gov/ Top
- ***Industrial Control Systems Joint Working Group -ICSJWG*** **-** The Department of Homeland Security (DHS) Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) established the Industrial Control Systems Joint Working Group (ICSJWG) to facilitate information sharing and reduce the risk to the nation's industrial control systems. The ICSJWG is a collaborative and coordinating body operating under the Critical Infrastructure Partnership Advisory Council (CIPAC) requirements. The ICSJWG provides a vehicle for communicating and partnering across all Critical Infrastructure and Key Resources Sectors (CIKR) between federal agencies and departments, as well as private asset owners/operators of industrial control systems. The goal of the ICSJWG is to continue and enhance the collaborative efforts of the industrial control systems stakeholder community in securing CIKR by accelerating the design, development, and deployment of secure industrial control systems. https://ics-cert.us-cert.gov/Industrial-Control-Systems-Joint-Working-Group-ICSJWG Top
- ***National Cybersecurity and Communications Integration Center – DHS*** - http://www.dhs.gov/national-cybersecurity-and-communications-integration-center Top
  - FBI encourages reporting of suspected cyber-attacks by critical infrastructure owners. The Pittsburgh Office number is 412-432-4000 and the Philadelphia Office number is 215-418-4000. NATIONAL CYBERSECURITY AND COMMUNICATIONS INTEGRATION CENTER (NCCIC) The NCCIC, within the Office of Cybersecurity and Communications, serves as a centralized location where operational elements involved in cybersecurity and communications reliance are coordinated and integrated. NCCIC partners include all federal departments and agencies; state, local, tribal, and territorial governments; the private sector; and international entities. The center's activities include providing greater understanding of cybersecurity and communications situation awareness vulnerabilities, intrusions, incidents, mitigation, and recovery actions. Cyber incidents can be reported to the NCCIC watch desk at: NCCIC_WatchandWarning@hq.dhs.gov. Top
- ***National Infrastructure Advisory Council – DHS*** **-** The National Infrastructure Advisory Council (NIAC) shall provide the President through the Secretary of Homeland Security with advice on the security of the critical infrastructure sectors and their information systems. The council is composed of a maximum of 30 members, appointed by the President from private industry, academia, and state and local government. http://www.dhs.gov/national-infrastructure-advisory-council http://en.wikipedia.org/wiki/National_Infrastructure_Advisory_Council Top
- ***NESEC V1.0 System Requirements Document Revision 3c – DHS*** **-** March 11, 2004 - The Department of Homeland Security (DHS) has initiated a project to implement a system that will monitor key infrastructures across North America so that major events and disturbances can be identified and anticipated. One of the critical infrastructures that will be monitored is the North American electric system. DHS has contracted with the Electricity Innovations Institute (E2I), an affiliate of the Electric Power Research Institute (EPRI), to plan and implement the system known as the North American

Electric Infrastructure Security Monitoring System (NESEC). EPRI has engaged the services of KEMA, Inc. to assist them. A NESEC Executive Advisory Committee (EAC) has been formed to advise on policy issues and a Technical Advisory Committee (TAC) has been established to review the project and to provide technical expertise. http://www.EnergyCollection.us/Energy-Security/NESEC-V1-System.pdf Top

- ***Partnership for Critical Infrastructure Security*** - http://www.sheriffs.org/content/partnership-critical-infrastructure-security http://www.dhs.gov/critical-infrastructure-partnership-advisory-council Top
- ***Protective Security Advisor*** - The Department of Homeland Security (DHS) Protective Security Advisor (PSA) program offers critical infrastructure owner/operators a conduit to many free services such as security training, site assessments, and assistance with local exercise coordination. http://www.dhs.gov/protective-security-advisors Top
- ***US-CERT*** - has established several important collaboration groups and programs to foster and facilitate information sharing on cybersecurity issues among government agencies. http://www.us-cert.gov/government-users US - Cert - United States Computer Emergency Readiness Team - *http://www.us.cert.gov* Top
- Top

Department of Energy wants electric utilities to create "cybersecurity governance board" - http://www.EnergyCollection.us/Energy-Security/DOE-Wants-Electricity.pdf Top

Dragonfly: Western Energy Companies Under Sabotage Threat – Symantec - An ongoing cyberespionage campaign against a range of targets, mainly in the energy sector, gave attackers the ability to mount sabotage operations against their victims. The attackers, known to Symantec as Dragonfly, managed to compromise a number of strategically important organizations for spying purposes and, if they had used the sabotage capabilities open to them, could have caused damage or disruption to energy supplies in affected countries. http://www.EnergyCollection.us/Energy-Security/Dragonfly_Western_Energy_Companies.pdf Original last accessed 2014-07-10 - http://tinyurl.com/nsyksht Top

Easing the Pain of a NERC CIP Audit - http://www.EnergyCollection.us/Energy-Security/Easing-Pain-NERC.pdf Top

Eastern Interconnection Data Sharing Network – Formed in January 2014 – positioned to build and coordinate the reliable and secure exchange of critical information amongst its members. They are identifying security architectures necessary to safely share critical operational information. Top

Edison Electric Institute - EEI - the association of U.S. shareholder-owned electric companies, international affiliates and industry associates worldwide. Company website - http://www.eei.org

- ***EEI website cybersecurity page*** - http://www.eei.org/issuesandpolicy/cybersecurity/Pages/default.aspx Top
- ***Statement of David K. Owens, Executive Vice President, Business Operations, Edison Electric Institute*** - Before the Committee on Energy and Natural Resources, United States Senate, May 7, 2009 - http://www.eei.org/whatwedo/PublicPolicyAdvocacy/TFB%20Documents/090507OwensSenateCyberSecurity.pdf Top

- ***Technical Conference 2014-04-29 - EEI Comments*** **-** a good discussion of CIP5, NIST standards, and industry specific standards - http://www.EnergyCollection.us/Energy-Security/Technical-Conference-2014-04-19-EEI.pdf Top
- Top

Effects-Based Targeting for Critical Infrastructure **-** 2014-02-24 - How would you infiltrate/attack/affect a wide swath of critical infrastructure in the United States? - http://www.EnergyCollection.us/Energy-Security/Effects-Based-Targeting.pdf Top

Electricity Grid Modernization **-** Progress Being Made on Cybersecurity Guidelines, but Key Challenges Remain to be Addressed - 2011-01-01 - http://www.EnergyCollection.us/Energy-Security/Electricity-Grid-Modernization.pdf Top

Electric Grid Vulnerability - Industry Responses Reveal Security Gaps **-** A report written by the staff of Congressmen Ed Markey (D-MA) and Henry Waxman (D-CA) - 2013-05-21 - http://www.EnergyCollection.us/Energy-Security/Electric-Grid-Vulnerability.pdf Top

Electricity for Free - The dirty underbelly of SCADA and Smart Meters - 2010-07-01 - SCADA Systems control the generation, transmission, and distribution of electric power, and Smart Meters are now being installed to measure and report on the usage of power. While these systems have in the past been mostly isolated systems, with little if no connectivity to external networks, there are many business and consumer issuing driving both of these technologies to being opened to external networks and the Internet. http://www.EnergyCollection.us/Energy-Security/Electricity-Free.pdf Original link - http://tinyurl.com/pa4j6dv Top

Electric Power Research Institute – EPRI

- ***Attack Trees for Selected Electric Sector High Risk Failure Scenarios*** **-** NESCOR - 2013-09-01 - This briefing includes the modified attack tree diagrams from the detailed analysis documents. The goal was to have a briefing that utilities could use. http://www.EnergyCollection.us/Energy-Security/Attack-Trees-Selected.pdf Top
- ***Cyber Security for DER Systems*** **-** 2013-07-01 - The scope of this NESCOR report is to describe the cyber security requirements for Distributed Energy Resources (DER), reflecting DER functions in the smart grid and taking into account variations of DER architectures. These DER architectures are mapped to the DER Actors, Logical Interfaces, and Logical Interface Categories (LICs) in the National Institute of Standards and Technology Interagency Report (NISTIR) 7628, Guidelines for Smart Grid Cyber Security, August 2010, including proposed updates to the existing actors and logical interfaces. The NISTIR 7628 high-level security requirements that are associated with the LICs are assessed for applicability. http://www.EnergyCollection.us/Energy-Security/Cyber-Security-DER.pdf Top
- ***Cyber Security and Privacy Program - 2013 Annual Review*** **-** by EPRI - Addressing Existing and Emerging Threats to an Interconnected Electric System through Technology, Processes, and Standards - http://www.EnergyCollection.us/Energy-Security/Cyber-Security-Privacy.pdf Top

- ***North America Electric System Infrastructure SECurity (NESEC) System – EPRI*** - Critical Infrastructure Protection Committee (CIP-C) - March 25-26, 2004 presentation - http://www.EnergyCollection.us/Energy-Security/North-America-Electric.pdf Top
- Top

Electric Utility Cyber Security Standards: Practical Implementation Guidance - December 14, 2009. Abstract: To tackle problems such as Critical Infrastructure Protection (CIP) compliance, Burton Group recommends that enterprises approach the issues strategically, rather than addressing technologies tactically. Burton Group's Reference Architecture provides a useful framework for these activities. By focusing on translating business requirements to technical standards and considering the various influences on IT decision making, this methodology provides a solid foundation for any utility (or other enterprise) to create standards systematically and comprehensively. This allows IT executives and management to define requirements that any functional IT area can leverage, rather than focusing on tactical gaps first and integrating individual approaches later. 66 page report. Available upon request. Contributing Author - Paul J. Feldman. http://www.EnergyCollection.us/Papers/Electric-Utility-Cyber-Security.pdf Top

Electric Power Supply Association – EPSA - on Cybersecurity - Competition will continue to be one of the dominant issues facing the electric power industry. EPSA members support policies that give all suppliers an equal opportunity to compete and give all customers an equal opportunity to reap the benefits of competition. EPSA represents companies that understand what it means to compete. Since its inception in the early 1980s, the independent power industry--now more aptly termed the competitive power supply industry to include both generation and marketing--has faced intensely competitive conditions. Projects developed by independent power producers continue to face stiff competition from other competitors within the industry. They also must continue to better the self-build options available to the traditional utilities to whom they currently sell their power. Power marketers compete with each other and with utilities and other wholesale power suppliers. EPSA's members contribute jobs and economic strength: as of 2008, they own more than 480 electricity generation plants representing 200,000 megawatts (MW) of capacity in 40 states and the District of Columbia. Company website cybersecurity page - http://www.epsa.org/forms/documents/DocumentFormPublic/ (enter "cybersecurity" in the search box in the upper left) Top

Encryption: The answer to all security - The best way to shed some light on this subject is to describe what security is offered by encryption, but also to address the concerns one should have about the encryption process. First, let's take a look at what it means for the data to be encrypted. Encryption is better described as a property of data than security of data. Whether the data is encrypted (cypher text) at a given time or not encrypted (plain text) -- which is how most people use it -- is similar to being blue in color, bold, underlined, or Ariel font. The security of the data is in the process of getting it from plain text to cypher and back to plain text. http://www.EnergyCollection.us/Energy-Security/Encryption-Answer-All.pdf Top

Energy Firm's Security So POOR, Insurers REFUSE to take their cash - Industrial control plants at power utilities and other energy sector firms, as elsewhere, rely on SCADA (Supervisory Control and Data Acquisition) technology. These legacy systems are increasingly being connected to the internet, essentially to make them easier to manage remotely. At the same time, more and more security problems are being discovered by security researchers investigating industrial plant security in the wake of the infamous

Stuxnet worm, which has made research into the formerly overlooked topic "sexy". More and more problems are being discovered in crucial systems that are rarely patched and this creates a recipe for disaster. Jonathan Roach, principal security consultant at Context Information Security, told El Reg: "SCADA systems have not been patched in years for various reasons: isolation of SCADA networks making the process of patching awkward; lack of motivation to perform what is sometimes seen as a risky process to a critical plant component; terms of software support contracts". http://www.EnergyCollection.us/Energy-Security/Energy-Firms-Security.pdf Original - http://www.theregister.co.uk/2014/02/27/energy_sector_refused_cyber_insurance/ Top

EnergySec - We strive to assure that security practices, ideas and principles are shared among energy organizations. It is our mission to drive security excellence among participants in our program through collaboration, careful analysis of security issues, near-instantaneous and confidential information-sharing where identity of discussants remains undisclosed, and through our extensive outreach programs. http://www.energysec.org/ http://tinyurl.com/manp66w

- **Network Perimeter Defense** – Analyzing the Data - An organization or security analyst can quickly become overwhelmed with monitoring logs and responding to security alerts. One problem is that, in order to be thorough, more logs will need to be collected than any team can realistically expect to check and respond to in a reasonable amount of time. Having a mature, effective security analysis operation, however, will allow important events to receive the attention they require. The first key to having a mature security analysis operation is to understand the normal, baseline operation of your networks. The second is to automate the collection and analysis of logs as much as possible, so that human time and resources are only being used to investigate events which require a human intellect to make sense of. The purpose of this paper is to provide tips for how to accomplish these two goals. http://www.EnergyCollection.us/Companies/EnergySec/Network_Perimeter_Defense .pdf Top
- **Network Perimeter Defense –** Common mistakes – 2014-01-01 - There are many things that can go wrong in designing, and then protecting, the perimeter of a network. The purpose of this paper is to highlight some of those problems. While not an exhaustive list of mistakes that can happen in planning and implementing a secure network perimeter, it can be used as a guide to check if you or your organization have any of these problems. We start with some big picture mistakes that are commonly encountered in perimeter defense. Then, the focus turns to some specific problems which are encountered in writing firewall rule sets, and how to help ensure those rule sets can be made more secure. http://www.EnergyCollecgtion.us/Companies/EnergySec/Network_Perimeter_Defense_2.pdf Top
- **Report and Recommendations – NECPUC Cybersecurity Project** – 2014-10-06 - This report has been prepared as part of a consulting contract between Energy Sector Security Consortium, Inc. (EnergySec), and the New England Conference of Public Utility Commissioners (NECPUC). This contract covered the period of October 28, 2013 through June 28, 2014. Under the agreement, EnergySec provided cybersecurity consulting to NECPUC's participating state commissions and their staff.
- Top

Energy Sector Control Systems Working Group – ESCSWG

- ***Company website -*** https://www.controlsystemsroadmap.net/AboutUs/Pages/Working-Group.aspx
- ***Cybersecurity Procurement Language for Energy Delivery Systems*** – 2014-04-01 - A variety of steps need to be taken throughout the life cycle of energy delivery systems to protect them from cyber threats. Embedding cybersecurity in the procurement of energy delivery systems is an important step for protecting these systems and is the focus of this document. Including cybersecurity in the procurement process can ensure that those purchasing and supplying energy delivery systems consider cybersecurity starting from the design phase of system development. This further ensures that cybersecurity is implemented throughout the testing, manufacturing, delivery, installation, and support phases of the product life cycle, improving overall reliability and reducing cybersecurity risks. To assist with embedding cybersecurity in the procurement of energy delivery systems, this document provides baseline cybersecurity procurement language for use by asset owners, operators, integrators, and suppliers during the procurement process. http://www.EnergyCollection.us/Energy-Security/Cybersecurity-Procurement-Language.pdf
- Top

Establishing Trust in Distributed Critical Infrastructure Micro Devices **-** 2014-01-08 - On start-up, the operation of each system needs to use this base secret to prove it was not tampered with since its last operation, and then use the same secrets to securely link to others on the network. In this article we will look at the handling of these root secrets as pertaining to many systems that are distributed across supply chains and operational networks. http://www.EnergyCollection.us/Energy-Security/Establishing-Trust-Distributed.pdf Top

European Network and Information Security Agency **-**
http://www.enisa.europa.eu/ Top

European Union

- ENISA – European Union Agency for Network and Information Security - The European Union Agency for Network and Information Security (ENISA) is a centre of network and information security expertise for the EU, its Member States, the private sector and Europe's citizens. ENISA works with these groups to develop advice and recommendations on good practice in information security. It assists EU Member States in implementing relevant EU legislation and works to improve the resilience of Europe's critical information infrastructure and networks. ENISA seeks to enhance existing expertise in EU Member States by supporting the development of cross-border communities committed to improving network and information security throughout the EU. More information about ENISA and its work can be found at www.enisa.europa.eu Top
- ***ENISA Threat Landscape 2014*** - The ETL 2014 is a continuation of the reports produced in 2012 and 2013: it follows similar approaches for the collection, collation and analysis of publicly available information to produce the cyber-threat assessment. The report contains a description of the methodology followed, together with some details on use-cases of cyber-threat intelligence. The main contribution of the ETL 2014 lies in the identification of top cyber threats within the reporting period. Together with the emerging threat landscape, it makes up the main contribution towards identification of cyber-

threats. http://www.EnergyCollection.us/Companies/ENISA/ENISA-Threat-Landscape-2014.pdf Top

- Top

EY (Ernst & Young)

- ***How the Grid Will Be Hacked - by E&Y*** 2013-10-15 - http://www.EnergyCollection.us/Energy-Security/How-Grid-Will.pdf Top
- ***Search on Cyber -*** http://www.ey.com/US/en/SearchResults?query=cyber&search_options=country_name
- Top

***Ex-FBI Official: Intel agencies don't share cyber threats that endanger companies* -** http://www.EnergyCollection.us/Energy-Security/Ex-FBI-Official.pdf Top

Executive Branch (President)

- ***Cyberspace Policy Review*** – Assuring a Trusted and Resilient Information and Communications Infrastructure - The President directed a 60-day, comprehensive, "clean-slate" review to assess U.S. policies and structures for cybersecurity. Cybersecurity policy includes strategy, policy, and standards regarding the security of and operations in cyberspace, and encompasses the full range of threat reduction, vulnerability reduction, deterrence, international engagement, incident response, resiliency, and recovery policies and activities, including computer network operations, information assurance, law enforcement, diplomacy, military, and intelligence missions as they relate to the security and stability of the global information and communications infrastructure. The scope does not include other information and communications policy unrelated to national security or securing the infrastructure. The review team of government cybersecurity experts engaged and received input from a broad cross-section of industry, academia, the civil liberties and privacy communities, State governments, international partners, and the Legislative and Executive Branches. This paper summarizes the review team's conclusions and outlines the beginning of the way forward towards a reliable, resilient, trustworthy digital infrastructure for the future. http://www.EnergyCollection.us/Energy-Communications/Cyberspace_Policy_Review.pdf
- ***Executive Order – 13636* - 2013-02-12 -** http://www.EnergyCollection.us/Energy-Security/Executive-Order-2013-02-12.pdf
- ***Executive Order - 13636* –** Wikisource - http://en.wikisource.org/wiki/Executive_Order_13636 Top
- ***Executive Order – Promoting Private Sector Cybersecurity Information Sharing* -** http://tinyurl.com/kmrfuaq Top
- ***Presidential Policy Directive 21* -** The Presidential Policy Directive (PPD) on Critical Infrastructure Security and Resilience advances a national unity of effort to strengthen and maintain secure, functioning, and resilient critical infrastructure. http://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil http://tinyurl.com/aglp8qh Top
- Top

Expendable ICS Networks? - In the last half decade, hardware-enforced security measures in the form of Unidirectional Security Gateways have come into widespread use, and are being added to best-practice guidance and documentation. With this hardware alternative now recognized as a best-practice, operations security practitioners are increasingly asking "If software-based security technologies are insufficient to protect even IT networks from compromise, then why would we use them to protect our ICS networks and all of the very costly machinery those networks control? Are ICS networks expendable?" http://www.EnergyCollection.us/Companies/Waterfall-Security/Expendable-ICS-Networks.pdf Top

External Monitoring Security Threats **-** Turbine vendors and many control system vendors and other vendors receive continuous, online feeds of data from large numbers of generating control systems and distribution/energy management control systems. These feeds are all sent to these vendors' central "remote monitoring and diagnostic/support" stations. All of these connections are designed to provide vendor personnel with continuous remote monitoring capabilities. Many of these connections are also designed to provide vendor personnel with the ability to carry out occasional "support" or "diagnostic" operations – other words for "occasional remote control over critical BES control system components." These types of connections pose a cybersecurity risk. http://www.EnergyCollection.us/Energy-Security/External-Monitoring-Security-Threats.pdf Top

FBI

- The Federal Bureau of Investigation (FBI) has two field offices in Pennsylvania, one in Pittsburgh and the other in Philadelphia. The FBI may be able to assist critical infrastructure owner/operators when there is a cyber-attack or suspected cyber incident. The 8 FBI encourages reporting of suspected cyber-attacks by critical infrastructure owners.
- ***Cyber Crime*** - http://www.fbi.gov/about-us/investigate/cyber
- ***InfraGard*** **-** is an information sharing and analysis effort serving the interests and combining the knowledge base of a wide range of members. At its most basic level, InfraGard is a partnership between the Federal Bureau of Investigation and the private sector. https://www.infragard.org/ Top
  - InfraGard is a Federal Bureau of Investigation (FBI) program that began in the Cleveland Field Office in 1996. It was a local effort to gain support from the information technology industry and academia for the FBI's investigative efforts in the cyber arena. The program expanded to other FBI Field Offices, and in 1998 the FBI assigned national program responsibility for InfraGard to the former National Infrastructure Protection Center (NIPC) and to the Cyber Division in 2003. InfraGard and the FBI have developed a relationship of trust and credibility in the exchange of information concerning various terrorism, intelligence, criminal, and security matters. InfraGard is an information sharing and analysis effort serving the interests and combining the knowledge base of a wide range of members. At its most basic level, InfraGard is a partnership between the FBI and the private sector. The goal of InfraGard is to promote ongoing dialogue and timely communication between members and the FBI. InfraGard members gain access to information that enables them to protect their assets and in turn give information to government that facilitates its responsibilities to prevent and address terrorism and other crimes. Membership is free and open to all critical infrastructure owners and operators. More information, including information on membership, can be found here: https://www.infragard.org/.
  - **Cyber threat Intelligence Integration Center** - The CTIIC will provide integrated all-source intelligence analysis related to foreign cyber threats and cyber incidents affecting U.S. national interests; support the U.S. government centers responsible

for cybersecurity and network defense; and facilitate and support efforts by the government to counter foreign cyber threats. Once established, the CTIIC will join the National Cybersecurity and Communications Integration Center (NCCIC), the National Cyber Investigative Joint Task Force (NCIJTF), and U.S. Cyber Command as integral parts of the United States Government's capability to protect our citizens, our companies, and our Nation from cyber threats. http://tinyurl.com/qxvlvoh Top

- ***iGuardian*** - The FBI has released the iGuardian portal as a pilot program designed to give companies a designated location to report cyber threats they've encountered. The iGuardian portal offers a one-stop-shop for cyber incident reporting. Reports received by iGuardian will go to the local FBI office and the FBI may follow up with the reporting entity. More information on becoming an InfraGard member can be found here: https://www.infraguard.org
- Top

Federal Energy Regulatory Commission - FERC

- ***CIP5 FERC Order*** - http://www.EnergyCollection.us/Companies/FERC/CIP-5-Order-2013-11-21.pdf
- ***Cyber and Grid Security at FERC - Webpage*** - http://www.ferc.gov/industries/electric/indus-act/reliability/cybersecurity.asp Top
- ***Office of Energy Infrastructure Security – OEIS*** - https://www.ferc.gov/about/offices/oeis.asp Top
- ***Opening Remarks by Kevin Perry*** - 2014-04-29 - In summary, while the CIP Version 5 standards have made substantive changes that will close a number of security gaps present in the Version 3 standards, two significant communication network gaps remain that should be addressed. The integrity of the data relied upon for Bulk Power System reliability needs to be protected during communication by encryption at a minimum and, where possible, through the application of cryptographic hashing and date/time stamping. The critical communication network Cyber Assets outside of the Electronic Security Perimeter but under the management control of the registered entity need to be protected through the application of an appropriate set of security controls. http://www.EnergyCollection.us/Companies/SPP/Opening-Remarks-Kevin.pdf Top
- ***Testimony of Joseph McClelland*** - 2011-05-05 - http://www.EnergyCollection.us/Energy-Security/Testimony-McClelland-Cyber.pdf Top
- ***Transcript from the Technical Conference ordered in CIP5*** - http://www.EnergyCollection.us/Companies/FERC/FERC-Transcript-2014-04-29.pdf Top
- ***Wellinghoff to Markey letter of 2009-04-28*** – http://www.EnergyCollection.us/Energy-Security/Wellinghoff-to-Markey-2009-04-28.pdf Top
- Top

The ***Federal Government's Track Record on Cybersecurity and Critical Infrastructure*** - 2014-02-04 - http://www.EnergyCollection.us/Energy-Security/Federal-Governments-Track.pdf Top

Federal Information Security Management Act of 2002 - FISMA - Wikipedia - http://en.wikipedia.org/wiki/Federal_Information_Security_Management_Act_of_2002 Top

Federal Laws Relating to Cybersecurity: Overview and Discussion of Proposed Revisions **-** 2013-06-20 - Summary For more than a decade, various experts have expressed increasing concerns about cybersecurity, in light of the growing frequency, impact, and sophistication of attacks on information systems in the United States and abroad. Consensus has also been building that the current legislative framework for cybersecurity might need to be revised. The complex federal role in cybersecurity involves both securing federal systems and assisting in protecting nonfederal systems. Under current law, all federal agencies have cybersecurity responsibilities relating to their own systems, and many have sector-specific responsibilities for critical infrastructure. More than 50 statutes address various aspects of cybersecurity either directly or indirectly, but there is no overarching framework legislation in place. While revisions to most of those laws have been proposed over the past few years, no major cybersecurity legislation has been enacted since 2002. Recent legislative proposals, including many bills introduced in recent Congresses, have focused largely on issues in 10 broad areas (see "Selected Issues Addressed in Proposed Legislation" for an overview of how current legislative proposals would address issues in several of those areas): • national strategy and the role of government, • reform of the Federal Information Security Management Act (FISMA), • protection of critical infrastructure (including the electricity grid and the chemical industry), • information sharing and cross-sector coordination, • breaches resulting in theft or exposure of personal data such as financial information, • cybercrime, • privacy in the context of electronic commerce, • international efforts, • research and development, and • the cybersecurity workforce. For most of those topics, at least some of the bills addressing them have proposed changes to current laws. Several of the bills specifically focused on cybersecurity received committee or floor action in the 112th and 113th Congresses, but none has become law. In the absence of enactment of cybersecurity legislation, the White House issued Executive Order 1336, with provisions on protection of critical infrastructure, including information sharing and standards development. Comprehensive legislative proposals on cybersecurity that received considerable attention in 2012 are The Cybersecurity Act of 2012 (CSA 2012, S. 2105, reintroduced in revised form as S. 3414), recommendations from a House Republican task force, and a proposal by the Obama Administration. They differed in approach, with S. 2105 proposing the most extensive regulatory Federal Laws Relating to Cybersecurity: Overview and Discussion of Proposed Revisions Congressional Research Service framework and organizational changes, and the task force recommendations focusing more on incentives for improving private-sector cybersecurity. An alternative to S. 2105 and S. 3414, S. 3342 (a refinement of S. 2151), did not include enhanced regulatory authority or new federal entities, but did include cybercrime provisions. S. 3414 was debated in the Senate but failed two cloture votes. Several narrower House bills would address some of the issues raised and recommendations made by the House task force. Four passed the House in 2012 but were not considered by the Senate. They were reintroduced in passed the House again, with some amendments, in April 2013: • Cyber Intelligence Sharing and Protection Act (H.R. 624), which focuses on information sharing and coordination, including sharing of classified information; • Cybersecurity Enhancement Act of 2013 (H.R. 756), which addresses federal cybersecurity R&D and the development of technical standards; • Advancing America's Networking and Information Technology Research and Development Act of 2013 (H.R. 967), which addresses R&D in networking and information technology, including but not limited to security; and • Federal Information Security Amendments Act of 2012 (H.R. 1163), which addresses FISMA reform. One bill from the 112th Congress was ordered reported out of the full committee but did not come to the floor: • Promoting and Enhancing Cybersecurity and Information Sharing Effectiveness Act of 2011 or PRECISE Act of 2011 (H.R. 3674), which addressed the role of the Department of Homeland Security in cybersecurity, including protection of federal systems, personnel, R&D, information sharing, and public/private sector collaboration in protecting critical infrastructure. Together, those House and Senate bills have addressed most of the issues listed above, although in different ways. All include proposed revisions to some existing laws covered in this report. http://www.EnergyCollection.us/Energy-Security/Federal-Laws-Relating.pdf Top

Feel the Electricity: how situation management empowers utilities for CIP Compliance **-** 2011-01 - Public Utilities Fortnightly - http://www.EnergyCollection.us/Energy-Security/Feel-Electricity.pdf Top

The Financial Impact of Cyber Risk **-** 50 Questions Every CFO Should Ask - http://www.EnergyCollection.us/Energy-Security/Financial-Impact-Cyber.pdf Top

FINRA

- ***Report on Cybersecurity Practices*** – http://www.EnergyCollecion.us/Companies/Finra/Report-Cybersecurity-Practices.pdf
- Top

Firewalls – see http://en.wikipedia.org/wiki/Firewall_(computing) Top

Foreign Cyber-Spies Inject Spyware into U.S. Grid with Potential for Serious Damage - http://www.smartgridnews.com/artman/publish/alexzhen/Foreign_Cyber-Spies_Inject_Spyware_into_U_S_Grid_with_Potential_for_Serious_Damage-562.html Top

The Forrester Wave: Information Security and Risk Consulting Services, Q3, 2010 - http://www.EnergyCollection.us/Energy-Security/Forrester-Wave-Information.pdf Top

The Forrester Wave: Managed Security Services, Q3 2010 - http://www.EnergyCollection.us/Energy-Security/Forrester-Wave-Managed.pdf Top

Frost & Sullivan - Network Security Research and Consulting practice provides global industry analysis, custom consulting, growth consulting (strategy consulting), and market research and forecasts that help your firm grow. Our global teams of consultants, market analysts, and research executives continuously monitor and evaluate the Intrusion Detection & Prevention Systems, Security Event Correlation, Managed Security Services, Web Application Firewalls, SSL VPN, Hardware Authentication Devices, Endpoint Security, Content Filtering, Anti-Virus, WLAN Security, Identity Management, Firewall/VPN, Biometrics, Policy Management, and Client Integrity market sectors to develop timely, strategic market intelligence. http://www.frost.com/prod/servlet/svcg.pag/ITNT Top

The Future of the Electric Grid **-** 2011-12-01 – by MIT - This report aims to provide a comprehensive, objective portrait of the U.S. electric grid and the challenges and opportunities it is likely to face over the next two decades. It also highlights a number of areas in which policy changes, focused research and demonstration, and the collection and sharing of important data can facilitate meeting the challenges and seizing the opportunities that the grid will face. http://www.EnergyCollection.us/Energy-Educational-Institutions/MIT/Future-Electric-Grid.pdf Top

Gartner Identifies the Top 10 Technologies for Information Security in 2014 - 2014-06-23 - Gartner, Inc. today highlighted the top 10 technologies for information security and their implications for security organizations in 2014 - Security Gateways, Brokers and Firewalls to Deal with the Internet of Things - including - Enterprises, especially those in asset-intensive industries like manufacturing or utilities, have operational technology (OT) systems provided by equipment manufacturers that are moving from proprietary communications and networks to standards-based, IP-based technologies. More enterprise assets are being automated by OT systems based on commercial software products. The end result is that these embedded software assets need to be managed, secured and provisioned appropriately for enterprise-class use. OT is considered to be the industrial subset of the "Internet of Things," which will include billions of interconnected sensors, devices and systems, many of which will communicate without human involvement and that will need to be protected and secured. http://www.EnergyCollection.us/Energy-Security/Gartner-Identifies-Top.pdf Top

Generic Risk Template - http://www.EnergyCollection.us/Energy-Security/Generic-Risk-Template.xlsx Top

Government Accounting Office

- ***Critical Infrastructure Protection*** – Cybersecurity Guidance Is Available, but More Can Be Done to Promote Its Use – GAO-12-92 – 2011-12-01 – http://www.EnergyCollection.us/Companies/GAO/GAO-12-92.pdf Top
- ***Critical Infrastructure Protection*** – Multiple Efforts to Secure Control Systems Are Underway, but Challenges Remain GAO-07-1036 – 2007-10-01 - http://www.EnergyCollection.us/Companies/GAO/GAO_07-1036.pdf Top
- ***Critical Infrastructure Protection*** – Update to National Infrastructure Projection Plan Includes Increased Emphasis on Risk Management and Resilience GAO-10-296 – http://www.EnergyCollection.us/Companies/GAO/GAO-10-296.pdf Top
- ***Cybersecurity Challenges in Securing the Electricity Grid – GAO-12-507T*** - Government Accounting Office - Testimony Before the Committee on Energy and Natural Resources, U.S. Senate - The threats to systems supporting critical infrastructures are evolving and growing. In testimony, the Director of National Intelligence noted a dramatic increase in cyber activity targeting U.S. computers and systems, including a more than tripling of the volume of malicious software. Varying types of threats from numerous sources can adversely affect computers, software, networks, organizations, entire industries, and the Internet itself. These include both unintentional and intentional threats, and may come in the form of targeted or untargeted attacks from criminal groups, hackers, disgruntled employees, nations, or terrorists. The interconnectivity between information systems, the Internet, and other infrastructures can amplify the impact of these threats, potentially affecting the operations of critical infrastructures, the security of sensitive information, and the flow of commerce. Moreover, the electricity grid's reliance on IT systems and networks exposes it to potential and known cybersecurity vulnerabilities, which could be exploited by attackers. The potential impact of such attacks has been illustrated by a number of recently reported incidents and can include fraudulent activities, damage to electricity control systems, power outages, and failures in safety equipment. http://www.EnergyCollection.us/Energy-Security/Cybersecurity-Challenges-Securing.pdf Top
- ***Defense Critical Infrastructure*** – Actions needed to improve the identification and management of electrical power risks and vulnerabilities to DOD Critical Assets – http://www.EnergyCollection.us/Companies/GAO/GAO-10-147.pdf Top

- ***Information Security*** – TVA Needs to Address Weaknesses in Control Systems and Networks – GAO-08-526 – http://www.EnergyCollection.us/Companies/GAO/GAO-08-526.pdf
- ***Website*** – http://www.gao.gov Top

Google Reports Unauthorized Digital Certificates **-** 2013-12-10 - http://www.EnergyCollection.us/Energy-Security/Google-Reports-Unauthorized.pdf Top

Government Asks Utilities, Others to Check Networks after 'Energetic Bear' Cyberattacks **-** http://www.EnergyCollection.us/Energy-Security/Government-Asks-Energy.pdf Top

Gramm-Leach-Bliley Act, Interagency Guidelines **-** The guide summarizes the obligations of financial institutions to protect customer information and illustrates how certain provisions of the Security Guidelines apply to specific situations. A useful reference is http://www.federalreserve.gov/bankinforeg/interagencyguidelines.htm#fn3r Top

Gridwise Architecture Council **-** was formed by the U.S. Department of Energy to promote and enable interoperability among the many entities that interact with the nation's electric power system. The GWAC members are a balanced and respected team representing the many constituencies of the electricity supply chain and users. The GWAC maintains a broad perspective of the GridWise vision and provides industry guidance and tools that make it an available and practical resource for the various implementations of Smart Grid technology. http://www.gridwiseac.org/about/mission.aspx Top

Hacking the Smart Grid **-** The technology could open up all kinds of opportunities for attackers, researchers say - 2010-08-02 - http://www.EnergyCollection.us/Energy-Security/Hacking-Smart-Grid.pdf Original link - http://www.technologyreview.com/news/420061/hacking-the-smart-grid/ Top

Hewett Packard – HP

- ***Company website on Cybersecurity*** **-** http://www8.hp.com/us/en/industries/public-sector.html?compURI=1087494#.U76S5bEuJyI
- ***The Mandate for Application Security – HP part 1*** – http://www.EnergyCollection.us/Energy-Security/Mandate_Application_Security_One.pdf Top
- ***The Business Case for Application Security – HP part 2*** – http://www.EnergyCollection.us/Energy-Security/Business_Case_For_Application_Security.pdf Top
- ***The Best Practices Guide for Application Security – HP part 3*** – http://www.EnergyCollection.us/Energy-Security/Best-Practices-Guide-HP.pdf Top
- Top

High Impact, Low-Frequency Event Risk to the North American Bulk Power System – NERC and DOE **-** June 2010 - A class of risks, called High-Impact, Low-Frequency (HILF) events, has recently become a renewed focus of risk managers and policy makers. These risks have the potential to cause catastrophic impacts on the electric power system, but either rarely occur, or, in some cases, have never occurred. Examples of HILF risks include coordinated cyber, physical, and blended attacks, the high-altitude detonation of a nuclear weapon, and major natural disasters like earthquakes, tsunamis, large hurricanes, pandemics, and geomagnetic disturbances caused by solar weather. HILF events truly transcend other risks to the sector due to their magnitude of impact and the relatively limited operational experience in addressing them. Deliberate attacks (including acts of war, terrorism, and coordinated criminal activity) pose especially unique scenarios due to their inherent unpredictability and significant national security implications. As concerns over these risks have increased, the electric sector is working to take a leadership position among other Critical Infrastructure and Key Resource (CIKR) sectors in addressing these risks. http://www.EnergyCollection.us/Energy-Security/High-Impact-Low.pdf Top

Homeland Security - Legal and Policy Issues (a book)- a search on questions that should be asked - http://tinyurl.com/bvbjv88 Top

House of Representatives

- ***Testimony – Cybersecurity: Assessing the immediate threat to the United States*** – before the subcommittee on National Security, Homeland Defense and Foreign Operations of the Committee on Oversight and Government reform - 2011-05-25 – http://www.EnergyCollection.us/Energy-Government/US-Representatives/Testimony-Cybersecurity-2011-05-25.pdf Top

Top

How to Hack the Power Grid for Fun and Profit - MIT Technology Review - Attackers could manipulate poorly protected data to make money or cause blackouts. http://www.EnergyCollection.us/Energy-Security/How-Hack-Power.pdf Original Link - http://www.technologyreview.com/news/421112/how-to-hack-the-power-grid-for-fun-and-profit/page/2/ Top

HSToday (Homeland Security news and information) - company website - http://www.hstoday.us Cybercom - http://www.hstoday.us/blogs/critical-issues-in-national-cybersecurity.html Cybersecurity - http://www.hstoday.us/focused-topics/cybersecurity/landing-page.html Weekly news - http://www.hstoday.us/newsletter-new/wnb-cybersecurity-today.html Top

IBM

- ***Best Practices for Cyber Security in the Electric Power Sector*** - With rare exceptions; utilities do an excellent job of managing traditional types of risks facing their operations. However, cyber security is the one category of risk that remains stubbornly opaque and resistant to attempts to manage, monitor, and measure. Determining the likelihood and severity of cyber security risks, as well as the efficacy of an organization's approaches to mitigate them, continues to be a challenge. IBM believes there are now practical ways to greatly improve management and execution of enterprise-wide cyber security. To help stakeholders understand the landscape of cyber security threats currently facing utilities, IBM introduces "best practices" that any utility organization can implement. http://www.EnergyCollection.us/Companies/IBM/Best-Practices-Cyber.pdf Top
- ***Holistic Enterprise Security Solution*** - IBM approach to cybersecurity in energy companies - http://www.slideshare.net/Prolifics/prolifics-ibm-cybersecurity Top
- Top

If cyberwar erupts, America's electric grid is a prime target – 2014-23 – http://www.EnergyCollection.us/Energy-Security/If-Cyberwar-Erupts.pdf Top

IEC – International Electrotechnical Commission (Standards)

- ***Organization*** **-** Founded in 1906, the IEC (International Electrotechnical Commission) is the world's leading organization for the preparation and publication of International Standards for all electrical, electronic and related technologies. These are known collectively as "electrotechnology". IEC provides a platform to companies, industries and governments for meeting, discussing and developing the International Standards they require. All IEC International Standards are fully consensus-based and represent the needs of key stakeholders of every nation participating in IEC work. Every member country, no matter how large or small, has one vote and a say in what goes into an IEC International Standard. http://www.iec.ch/about/?ref=menu Top
  - ***List of IEC Standards -*** http://en.wikipedia.org/wiki/IEC_62325
- ***IEC 61850 Standards*** **-** IEC 61850[1] is a standard for the design of electrical substation automation. IEC61850 is a part of the International Electrotechnical Commission's (IEC) Technical Committee 57 (TC57)[2] reference architecture for electric power systems. The abstract data models defined in IEC61850 can be mapped to a number of protocols. Current mappings in the standard are to MMS (Manufacturing Message Specification), GOOSE, SMV, and soon to Web Services. These protocols can run over TCP/IP networks and/or substation LANs using high speed switched Ethernet to obtain the necessary response times of < 4ms for protective relaying. Wikipedia - http://en.wikipedia.org/wiki/IEC61850 Top
- ***IEC 61968*** - is a series of standards under development that will define standards for information exchanges between electrical distribution systems. These standards are being developed by Working Group 14 of Technical Committee 57 of the IEC (IEC TC 57 WG14). IEC 61968 is intended to support the inter-application integration of a utility enterprise that needs to collect data from different applications that are legacy or new and each has different interfaces and run-time environments. IEC 61968 defines interfaces for all the major elements of an interface architecture for Distribution Management Systems (DMS) & is intended to be implemented with middleware services that broker messages among applications. Wikipedia - http://en.wikipedia.org/wiki/IEC_61968 Top
- ***IEC 61970*** - The IEC 61970 series of standards deals with the application program interfaces for energy management systems (EMS). The series provides a set of guidelines and standards to facilitate: The integration of applications developed by different suppliers in the control center environment; The exchange of information to systems external to the control center environment, including transmission, distribution and generation systems external to the control center that need to exchange real-time data with the control center; The provision of suitable interfaces for data exchange across legacy and new systems. Wikipedia - http://en.wikipedia.org/wiki/IEC_61970 Top
- ***IEC 62351*** - is a standard developed by WG15 of IEC TC57. This is developed for handling the security of TC 57 series of protocols including IEC 60870-5 series, IEC 60870-6 series, IEC 61850 series, IEC 61970 series & IEC 61968 series. The different security objectives include authentication of data transfer through digital signatures, ensuring only authenticated access, prevention of eavesdropping, prevention of playback and spoofing, and intrusion detection. http://en.wikipedia.org/wiki/IEC_62351 Top

Industrial Control Systems Cyber Threat Research By Preventia **-** Revision 1.1, by Preventia - This research is presented on the assumption the Cyber Security Threats to

Industrial Control Systems (ICS) and Supervisory Control and Data Acquisition (SCADA) systems are understood by the reader, who will also have a basic understanding of SCADA systems, their function and networking infrastructure, along with general Cyber Security awareness. This document is intended for Cyber Security Professionals who are responsible for reducing risk of Cyber Threats to ICS and SCADA Systems. It will guide you through the resources available to research this specific topic independently, and, more importantly attempt to enhance your understanding of why the Cyber Security issues are so challenging to address, not just that they exist. Tactical Cyber Security technologies and use cases are also shared to highlight how the risks can be mitigated, whilst allowing critical infrastructure to function continuously. There is purposely no conclusion because the two worlds of Cyber Security and SCADA Systems are continuously evolving, as such there will be further updated editions with industry leaders contributing. http://www.EnergyCollection.us/Energy-Security/Industrial-Control-Systems.pdf Top

Information Systems Security Association – ISSA - http://www.issa.org/ Top

Infosecurity Magazine - http://www.infosecurity-magazine.com/ Top

Infrastructure Security - Wikipedia - http://en.wikipedia.org/wiki/Infrastructure_security Top

Institute of Electrical and Electronic Engineers – IEEE

- ***Organization website*** - http://www.ieee.org/index.html Top
- ***IEEE 1686 – Standard for Substation Intelligent Electronic Devices (IED) Cyber Security Capabilities*** - http://standards.ieee.org/findstds/standard/1686-2007.html
- ***IEEE P37.240 – Standard for Cyber Security Requirements for Substation Automation, Protection and Control Systems***
- ***IEEE 1711 – Cryptographic Protocol for Cyber Security of Substation Serial Links*** - http://standards.ieee.org/findstds/standard/1711-2010.html
- ***IEEE 1402 – Standard for Physical Security of Electric Power Substations*** - http://standards.ieee.org/develop/project/1402.html
- ***PSRC H22 – Cyber Security for protection related data files*** - http://www.pes-psrc.org/h/h22/h22.html
- ***Smart Grid Community – IEEE*** - https://www.ieee.org/membership-catalog/productdetail/showProductDetailPage.html?product=CMYSG735 Top
- ***Wikipedia*** - http://en.wikipedia.org/wiki/Institute_of_Electrical_and_Electronics_Engineers Top
- Top

Insurance (Cybersecurity)

- ***Cyber insurance becomes the new cost of doing business*** – 5-04 – in FierceCIO – http://www.EnergyCollection.us/Energy-Security/Cyber-Insurance-Becomes.pdf Top
- ***Cyberattack Insurance a Challenge for Business***
- ***Energy Firm's Security So POOR, Insurers REFUSE to take their cash***
- Top

International Organization for Standardization – ISO

- ***ISO 27001*** **-** is an information security standard that was published on the 25 September 2013. It cancels and replaces ISO/IEC 27001:2005, and is published by the International Organization for Standardization (ISO) and the International Electro-technical Commission (IEC) under the joint ISO and IEC subcommittee, ISO/IEC JTC 1/SC 27. It is a specification for an information security management system (ISMS). Organizations which meet the standard may be accredited by an independent accreditor. Wikipedia - http://en.wikipedia.org/wiki/ISO/IEC_27001:2013
- ***ISO 27002*** **-** ISO/IEC 27002 is an information security standard published by the International Organization for Standardization (ISO) and by the International Electrotechnical Commission (IEC), entitled Information technology – Security techniques – Code of practice for information security management. ISO/IEC 27002 provides best practice recommendations on information security management for use by those responsible for initiating, implementing or maintaining information security management systems (ISMS). Information security is defined within the standard in the context of the C-I-A triad: the preservation of confidentiality (ensuring that information is accessible only to those authorized to have access), integrity (safeguarding the accuracy and completeness of information and processing methods) and availability (ensuring that authorized users have access to information and associated assets when required). Wikipedia - http://en.wikipedia.org/wiki/ISO/IEC_27002 Top
- ***Website -*** http://www.iso.org/iso/home.html
- ***Wikipedia -*** http://en.wikipedia.org/wiki/International_Organization_for_Standardization
- Top

International Society of Automation – ISA **-** is a leading, global, nonprofit organization that is setting the standard for automation by helping over 30,000 worldwide members and other professionals solve difficult technical problems. See https://www.isa.org/ Top

- ***ISA99, Industrial Automation and Control Systems Security*** - The ISA99 standards development committee brings together industrial cyber security experts from across the globe to develop ISA standards on industrial automation and control systems security. This original and ongoing ISA99 work is being utiilized by the International Electro-technical Commission in producing the multi-standard IEC 62443 series. See https://www.isa.org/isa99/
and http://isa99.isa.org/ISA99%20Wiki/Home.aspx Top
- ***Security for Industrial Automation and Control Systems - ISA-62443***-3-3 (99.03.03) Part 3-3: System Security Requirements and Security Levels - Draft 4 - January 2013 - The IACS community audience for this specification is intended to be asset owners, system integrators, product suppliers, service providers and, where appropriate, compliance authorities. Compliance authorities include government agencies and regulators with the legal authority to perform audits to verify compliance with governing laws and regulations. System integrators, product suppliers and service providers will use this document to evaluate whether their products and services can provide the functional security capability to meet the asset owner's target security level (SL-T) requirements. As with the assignment of SL-Ts, the applicability of individual control system requirements (SRs) and requirement enhancements (REs) needs to be based on an asset owner's security policies, procedures and risk assessment in the context of their specific site. Note that some SRs contain specific conditions for permissible exceptions, such as where meeting the SR will violate fundamental operational requirements of a control system (which may trigger the need for compensating countermeasures). http://www.EnergyCollection.us/Energy-Security/Security-Industrial-Automation.pdf Unidirectional Gateways - see page 42, 49, 51. Top

- ***Top Ten Differences Between ICS and IT Cybersecurity*** – understanding the different needs of ICS and IT system security leads to cooperation and collaboration between historically disconnected camps – http://www.EnergyCollection.us/Energy-Security/Top-Ten-Differences.pdf Top

Interoperability and Security for Converged Smart Grid Networks **-** This paper investigates interoperability and cyber security issues that arise with the use of Converged Smart Grid Networks in distribution utilities. Due to the interoperability proffered by IP, several progressive utilities are considering placing control communications such as Advanced Metering Infrastructure (AMI) and Distribution Automation (DA) on the same network that is also used to offer other services, such as utility Intranet and residential customer broadband. Two case studies of planned AMI and DA deployments, one using Fiber-To-The-Premise and the other using WiMax with a fiber backbone, are analyzed to determine cyber security risks and requirements that arise from AMI and DA communications being carried over the same infrastructure that is used to deliver residential broadband, voice, video, and public Internet services. Directly applying typical best practices for secure control system design such as NIST SP800-83 is not possible, because these best practices call for the control system network to be physically separated from the corporate network. Instead, strong logical separation of network traffic must be achieved using appropriate networking protocols, security tools, and defense-in-depth architecture. This paper examines the challenges that arise in implementing strong logical traffic separation for converged smart grid networks and explores potential solutions - http://www.EnergyCollection.us/Energy-Smart-Grid/Interoperability-Security-Converged.pdf Top

Introduction to Waterfall Unidirectional Security Gateways: True Unidirectionality, True Security

Intrusion Detection System for Advanced Metering Infrastructure **-** This Intrusion Detection Systems (IDSes) for Advanced Metering Infrastructure (AMI) document is a product of the EPRI AMI Incident Response Project. The document is intended to give AMI vendors and asset owners a clear understanding of the unique monitoring requirements of AMI and to identify key research challenges related to intrusion detection technology and large-scale deployment. The effective design and deployment of IDSes in a utility's AMI environment have several characteristics that differentiate them from design and deployment in traditional information technology (IT) environments. For example, simply deploying a perimeter IDS may not provide the coverage necessary for an AMI system. Since there tend to be mesh networks in addition to IP-based backhaul networks, positioning an IDS at the AMI head-end system could miss malicious activity in the mesh network. In addition, there can be scalability issues, as some utilities deploy millions of meters in their service territories. The scope of this document includes monitoring requirements for the core components of an AMI (i.e., collection engine, meter data management system, data collection unit, and meters) and does not cover the home area network (HAN) or third-party communication equipment. http://www.EnergyCollection.us/Energy-Metering/Intrustion-Detection-System.pdf Top

ISACA – (previously the Information Systems Audit and Control Association) - As an independent, nonprofit, global association, ISACA engages in the development, adoption and use of globally accepted, industry-leading knowledge and practices for information systems. Previously known as the Information Systems Audit and Control Association, ISACA now goes by its acronym only, to reflect the broad range of IT governance professionals it serves. Company website - http://www.isaca.org Top

- **COBIT - Control Objectives for Information and Related Technology** - in Wikipedia - (COBIT) is a framework created by ISACA for information technology (IT) management and IT governance. It is a supporting toolset that allows[citation needed] managers to bridge the gap between control requirements, technical issues and business risks. http://en.wikipedia.org/wiki/COBIT Top

IT Governance Ltd

- Governance - http://www.itgovernance.co.uk/cyber-governance.aspx#.VHuUVDHF98E
- Link to Cyber Security Resources - http://www.itgovernance.co.uk/what-is-cybersecurity.aspx#.VHuTaTHF98E
- Top

IT Governance Institute – ITGI - was established in 1998 in recognition of the increasing criticality of information technology to enterprise success. In many organizations, success depends on the ability of IT to enable achievement of business goals. In such an environment, governance over IT is as critical a board and management discipline as corporate governance or enterprise governance. Effective IT governance helps ensure that IT supports business goals, maximizes business investment in IT, and appropriately manages IT-related risks and opportunities. ITGI conducts research on global practices and perceptions of governance of IT for the business community. ITGI aims to help enterprise leaders understand how effective governance can make IT successful in supporting the enterprise's mission and goals. Company website - http://www.itgi.org Top

- ***Data Breach Notification Laws by State*** **-** Despite support from President Obama's administration and from the US Attorney General , no single federal law has yet been enacted that requires organizations to notify individuals when their personal information has been compromised by a security breach. Consumer data in the United States is currently protected by a patchwork of industry-specific federal laws and state legislation whose scope and jurisdiction vary. The challenge of compliance for organizations that conduct business across all 50 states is therefore considerable. This page provides a summary of the requirements of each of the 47 state data breach notification laws as of August 2014. Copy from 2014-09-02 – http://www.EnergyCollection.us/Energy-Security/Data-Breach-Notification.pdf Original link last accessed 2014-09-02 - http://tinyurl.com/ovdb2k5 Top

Journal of Energy Security **-** http://www.ensec.org/ Top

Key Steps to Automate IT Security Compliance - http://www.EnergyCollection.us/Energy-Security/4-Key-Steps.pdf Top

Law in the Boardroom in 2014 **-** Cyber risk, M&A, shareholder engagement, and compliance dominate today's legal oversight environment. Here are the results of our nationwide survey of directors and general counsel on the risks that matter most in 2014. http://www.EnergyCollection.us/Energy-Security/Law-Boardroom-2014.pdf
Original link accessed 2014-07-11 - http://tinyurl.com/pge8azn Top

Lessons from 5 Advanced Attacks of 2013 **-** From Cryptolocker to the destructive attacks on Korean firms to the massive flood that made Spamhaus inaccessible, attackers delivered some hard lessons in 2013. Note that 4 of the 5 involved mis-use of digital certificates. http://www.EnergyCollection.us/Energy-Security/Lessons-From-5.pdf Top

Lessons Learned From Snowden **-** http://www.EnergyCollection.us/Energy-Security/Lessons-Learned-Snowden.pdf Top

Living in a World Without Trust: When IT's Supply Chain Integrity and Online Infrastructure Get Pwned **-** Published: 5 October 2012 by Maverick Research - Enterprise IT supply chains will be targeted and compromised, forcing changes in the structure of the IT marketplace and how IT will be managed moving forward. (Maverick research deliberately exposes unconventional thinking, and may not agree with Gartner's official positions.) Key Findings > A lack of trust in information security technology solutions will fragment information security spending along geopolitical lines by 2018. > Supply chain issues don't end when a system is delivered. Supply chain integrity must extend to include "operational supply chain" issues, such as updates and maintenance. > Open source does not eliminate software supply chain integrity issues. Rogue or outdated open-source libraries and frameworks are significant risks. > An architectural shift to software-defined IT architectures running on standardized hardware will result in more transparency and higher IT supply chain assurance. > Within an IT system, trusted virtualization platforms on trusted CPUs will be used to establish a stronghold of trust on systems that are otherwise considered untrustable. Recommendations > IT procurement processes must be updated to address IT supply chain integrity issues. > Shift to architectures using standardized hardware, which moves intelligence out of hardware and into software layers that can be more readily tested. > If open source is used, ensure that the frameworks and libraries used are legitimate and up-todate, and that the compiler used hasn't been compromised. > Adopt trust models that reduce the scope of trust to defendable strongholds, and then extend the trust to allow the use of untrusted systems and components. > In the longer term, all sensitive data, including fixed desktops and servers within enterprise data centers, should be encrypted, reducing the scope of trust required. http://www.EnergyCollection.us/Energy-Security/Living-World-Without-Trust-Filed.pdf Top

Lockheed Martin

- ***Critical Infrastructure Cybersecurity (by Lockheed Martin)*** **-** 2014-07-23 - LM presentation about its capabilities in the energy business - http://www.EnergyCollection.us/Companies/Lockheed-Martin/Critical-Infrastructure-Cybersecurity.pdf Top
- ***Securing Industrial Control Systems*** – The Basics – http://www.EnergyCollection.com/Companies/Lockheed-Martin/Securing-ICS-Basics.pdf Top
- Top

LulzSec **-** Lulz Security, commonly abbreviated as LulzSec, was a black hat computer hacker group that claimed responsibility for several high profile attacks, including the compromise of user accounts from Sony Pictures in 2011. The group also claimed responsibility for taking the CIA website offline.[2] Some security professionals have commented that LulzSec has drawn attention to insecure systems and the dangers of password reuse.[3] It has gained attention due to its high profile targets and the sarcastic messages it has posted in the aftermath of its attacks. One of the founders of LulzSec was a computer security specialist who used the online moniker Sabu. The man accused of being Sabu has helped law enforcement track down other members of the organization as part of a plea deal. At least four associates of LulzSec were arrested in March 2012 as part of this investigation. British authorities had previously announced the arrests of two teenagers they allege are LulzSec members T-flow and Topiary. At just after midnight (BST, UT+01) on 26 June 2011, LulzSec released a "50 days of lulz" statement, which they claimed to be their final release, confirming that LulzSec consisted of six members, and that their website is to be shut down. This breaking up of the group was unexpected.[4] The release included accounts and passwords from many different sources. Despite claims of retirement, the group committed another hack against newspapers owned by News Corporation on 18 July, defacing them with false reports regarding the death of Rupert Murdoch. The group helped launch Operation AntiSec, a joint effort involving LulzSec, Anonymous, and other hackers.   Wikipedia - http://en.wikipedia.org/wiki/LulzSec   Top

Managers Information Security Survival Kit and Checklist - http://www.EnergyCollection.us/Energy-Security/Managers-Information-Security.pdf   Top

The Mask, Attacks on Trust, and Game Over - Kaspersky Labs - has identified and documented what it terms as “one of the most advanced threats.” Known by its Spanish name “Careto,” The Mask operation is a sophisticated, organized attack using multiple attack methods to steal data. Its alarming set of targets include a variety of SSL, VPN, and SSH cryptographic keys and digital certificates.   http://www.EnergyCollection.us/Energy-Security/Mask-Attacks-Trust.pdf   Top

Metasploit - provides useful information to people who perform penetration testing, IDS signature development, and exploit research. This project was created to provide information on exploit techniques and to create a useful resource for exploit developers and security professionals. The tools and information on this site are provided for legal security research and testing purposes only. Metasploit is a community project managed by Metasploit LLC. http://www.metasploit.com/   Top

Microsoft

- ***Developing a City Strategy for Cybersecurity*** – http://www.EnergyCollection.us/Companies/Microsoft/City-Strategy-Cybersecurity.pdf   Top
- Top

National Association of Corporate Directors – NACD

- ***Audit Committee Chair Advisory Council*** - 2014-09-30 – discussion about Audit Committees and Cybersecurity – available to NARC members – password protected copy – http://www.EnergyCollection.com/Energy-Security/Audit-Committee-Chair.pdf
- ***Cyber-Risk Oversight*** – NADC publication 2014 – see http://www.nacdonline.org/Resources/Article.cfm?itemNumber=10688 password protected copy - here
- ***Cybersecurity: Boardroom Implications - NACD*** – http://tinyurl.com/pdcwva7   Top
- ***NACD Summit*** – NACD’s first cybersecurity summit helps directors better understand and mitigate new risks – password protected copy - here

- ***Playing For Keeps*** – NACD article - keeping cyber issues in check – http://www.EnergyCollection.com/Companies/NACD/Playing-For-Keeps.pdf - password protected copy.
- Top

National Association of Regulatory Utility Commissioners – NARUC

- ***Cybersecurity for State Regulators - With Sample Questions for Regulators to Ask*** **-** 2012-06-01 - This primer addresses cybersecurity – particularly for the electric grid – for State utility regulators, though we hope that it will be useful for a wide audience of policymakers in this field. The primer provides some conceptual cybersecurity basics for the electric grid and provides links to how regulators can: • Develop internal cybersecurity expertise; • Ask good questions of their utilities; • Engage in partnerships with the public and private sector to develop and implement cost-effective cybersecurity; and • Begin to explore the integrity of their internal cybersecurity practices. http://www.EnergyCollection.us/Cybersecurity/Cybersecurity-State-Regulators.pdf Top
- ***Cybersecurity for State Regulators 2.0*** **-** with sample questions for regulators to ask utilities - 2013-02-01 - http://www.EnergyCollection.us/Energy-Security/Cybersecurity-State-Regulators.pdf Top
- Top

National Governors Association

- ***State Roles in Enhancing the Cybersecurity of Energy Systems and Infrastructure*** - Governors face several challenges in protecting critical energy assets from cyber threats and adequately responding to disruptions caused by a cyber-attack. They include limited state-level experience with cyber-related response and recovery activities in general, limited understanding of the threats and risks associated with cyber-attacks on the energy system, and an energy system that is interstate and interdependent with other critical infrastructure networks. Governors can confront those challenges and enhance the cybersecurity of the energy infrastructure within their state through the actions described in this paper http://www.EnergyCollection.us/Companies/NGA/State-Roles-Enhancing.pdf Top
- Top

National Research Regulatory Institute – NRRI

- ***The Role of State Public Utility Commissions in Protecting National Utility Infrastructure*** **–** 2005-03-01 http://www.EnergyCollection.us/Companies/NRRI/Role-State-Public.pdf Top
- A ***Summary of State Regulators' Responsibilities Regarding Cybersecurity Issues*** – 2014-12-01 – http://www.EnergyCollection.us/Companies/NRRI/Summary-State-Regulators.pdf Top
- Top

NERC

- ***Categorizing Cyber Systems - An Approach Based on BES Reliability Functions*** **-** NERC Cyber Security Standards Drafting Team for Order 706 - 06/15/2009 -

http://www.EnergyCollection.us/Energy-Security/Categorizing-Cyber-Systems.pdf Top

- ***CIP5***
  - ***Implementation Study Final Report*** – CIP Version 5 Transition Program – 2014-10-01 NERC conducted a study, referred to as the Implementation Study for the CIP Version 5 Transition Program in which six industry participants(the study participants) implemented elements of CIP Version 5 in an accelerated time frame to help the ERO understand the challenges entities may face transitioning to CIP Version 5, identify guidance topics, and provide feedback to other entities on such topics to help ensure an efficient and effective transition industry-wide. This report discusses the results of the Implementation Study and was developed in collaboration with the study participants. – http://www.EnergyCollection.us/Companies/NERC/Implementation-Study-Final.pdf Top
  - ***NERC CIP-005 Compliance: At-A-Glance*** - http://www.EnergyCollection.us/Energy-Security/NERC-CIP5-Glance.pdf Top
  - ***NERC-CIP V5 Encourages Unidirectional Gateways*** - The provisionally-approved CIP V5 standards address a wider spectrum of cyber-security technologies than were addressed in previous versions, and in particular the draft V5 standards address and encourage the use of hardware-enforced Unidirectional Security Gateways. Unidirectional Gateways are a secure alternative to firewalls, and are used in defense-in-depth security architectures for the control systems which operate the power grid. Like firewalls, the gateways integrate control system data sources with business information systems through Electronic Security Perimeters. Unlike firewalls, the gateways cannot introduce security vulnerabilities as a result of this integration. The gateway hardware is "deterministic" - no misconfiguration of any software can cause the gateway hardware to put the safety or the reliability of industrial servers at risk. See page 11 of http://www.EnergyCollection.us/Energy-Security/NERC-CIP-V5-Encourages.pdf and the full article at: http://www.EnergyCollection.us/Energy-Security/NERC-CIP-V5-Encourages-1.pdf Top
  - Top
- ***Cyber Attack Task Force (NERC)*** - The North American bulk power system (BPS) is one of the most critical of infrastructures and is vital to society in many ways. The electric power industry has well-established planning and operating procedures in place to address the "normal" emergency events (e.g., hurricanes, tornadoes, and ice storms) that occur from time to time and disrupt electricity reliability. However, the electricity industry has much less experience with planning for and responding to high-impact events that have a low probability of occurring or have not yet occurred. To help the electricity industry better understand these low probability risks, in June 2010, NERC and the U.S. Department of Energy issued a report titled, "High-Impact, Low-Frequency Event Risk to the North American BPS"3. Subsequently, the NERC board approved a Coordinated Action Plan4 under the leadership of the NERC Technical Committees to establish four Task Forces needed to address this work. This report provides the conclusions of one of them – the Cyber Attack Task Force (CATF). http://www.EnergyCollection.us/Companies/NERC/Cyber-Attack-Task-Force.pdf Top
- ***Critical Infrastructure Protection Standards (CIP)*** - active requirements - http://www.nerc.com/page.php?cid=2|20 http://www.nerc.com/pa/Stand/Pages/CIPStandards.aspx
- ***ES ISAC – Electricity Sector Information Sharing and Analysis Center*** - https://www.esisac.com/SitePages/Home.aspx Top

- ***Guidance for Secure Interactive Remote Access from NERC*** – 2011-07-01 – This guidance document provides an overview of interactive remote access concepts, and includes example technology and policy solutions that Registered Entities may consider to strengthen security for interactive remote access to control system networks. Included in this document are case studies describing the steps that six companies have taken to implement secure interactive remote access. These case studies represent a range of entity size, perceived cost, and level of sophistication. Each case study is accompanied by a description of the secure interactive remote access implementation, and a network architecture diagram to aid Registered Entities in designing their own secure interactive remote access architecture. http://www.EnergyCollection.us/Companies/NERC/Guidance-Secure-Interactive.pdf Original at http://tinyurl.com/kgo72kh last accessed 2014-07-17 Top
- ***NERC Reliability Assurance Initiative - RAI*** **-** The Reliability Assurance Initiative (RAI) program is the ERO's strategic initiative to transform the current compliance and enforcement program into one that is forward-looking, focuses on high reliability risk areas, and reduces the administrative burden on registered entities. http://www.nerc.com/pa/comp/Pages/Reliability-Assurance-Initiative.aspx Top
- ***NERC Security Guidelines Working Group -SGWG*** **-** http://www.nerc.com/filez/sgwg.html Top
- ***Reliability Coordinator Information Sharing Portal (via NERC)*** – enables incident and threat sharing based on information and reliability data. Top
- ***NERC CIP & Smart Grid*** - How do they fit together? http://www.EnergyCollection.us/Energy-Security/NERC-CIP-Smart-Grid.pdf Top

At The *Nexus of Cybersecurity and Public Policy – Some Basic Concepts and Issues* – a very excellent and readable primer. By the National Research Council of the National Academies. Developed by the Committee on Developing a Cybersecurity Primer: Leveraging Two Decades of National Academies Work, the present report leverages past insights developed in this body of work to provide a concise primer on the fundamentals of cybersecurity and the nexus between cybersecurity and public policy (see Box P.2 for the project's statement of task). This report is based primarily on earlier CSTB work, and for readability, direct extracts from that work are not set in quotation marks, nor are paraphrases from such work identified as such. However, the report also addresses issues not covered in earlier CSTB work. As a primer, this report presents fundamental concepts and principles that serve as points of departure for understanding specific cybersecurity incidents or proposals to improve security. The specifics of cybersecurity change rapidly—but the fundamental concepts and principles endure, or at least they change much more slowly. These concepts and principles are approximately independent of particular cybersecurity technologies or incidents, although they manifest themselves in a wide variety of different technologies and incidents. http://www.EnergyCollection.us/Energy-Security/Nexus-Cybersecurity-Public.pdf Original accessed 2014-06-01 at http://www.nap.edu/catalog.php?record_id=18749 Top

NIST - National Institute of Standards

- ***Computer Security Division -*** http://www.nist.gov/itl/csd/
- ***Framework for Improving Critical Infrastructure Cybersecurity - NIST*** **-** Version 1.0 - 2014-02-12 - http://www.EnergyCollection.us/Energy-Security/Framework-Improving-Critical.pdf - It should be noted that the NIST

Framework is good for measuring progress and breath of security program coverage, but does not address which Best Practices will accomplish true in-depth security protection. http://www.nist.gov/cyberframework/ Top

- ***Glossary of Key Information Security Terms - NIST 7298*** **-** The National Institute of Standards and Technology (NIST) has received numerous requests to provide a summary glossary for our publications and other relevant sources, and to make the glossary available to practitioners. As a result of these requests, this glossary of common security terms has been extracted from NIST Federal Information Processing Standards (FIPS), the Special Publication (SP) 800 series, NIST Interagency Reports (NISTIRs), and from the Committee for National Security Systems Instruction 4009 (CNSSI-4009). This glossary includes most of the terms in the NIST publications. It also contains nearly all of the terms and definitions from CNSSI-4009. This glossary provides a central resource of terms and definitions most commonly used in NIST information security publications and in CNSS information assurance publications. For a given term, we do not include all definitions in NIST documents – especially not from the older NIST publications. Since draft documents are not stable, we do not refer to terms/definitions in them. Each entry in the glossary points to one or more source NIST publications, and/or CNSSI-4009, and/or supplemental sources where appropriate. The NIST publications referenced are the most recent versions of those publications (as of the date of this document). http://www.EnergyCollection.us/Energy-Security/Glossary-Key-Information.pdf Original link last accesses 2014-06-22 - http://tinyurl.com/p866ouf Top
- ***Guide to Industrial Control Systems (ICS) Security – NIST 800-82*** - Supervisory Control and Data Acquisition (SCADA) systems, Distributed Control Systems (DCS), and other control system configurations such as Programmable Logic Controllers (PLC) http://www.EnergyCollecion.us/Energy-Security/Guide-Industrial-Control.pdf Top
- ***Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations – NIST 800-137*** – 2011-09-01 - The Risk Management Framework (RMF) developed by NIST,1 describes a disciplined and structured process that integrates information security and risk management activities into the system development life cycle. Ongoing monitoring is a critical part of that risk management process. In addition, an organization's overall security architecture and accompanying security program are monitored to ensure that organization-wide operations remain within an acceptable level of risk, despite any changes that occur. Timely, relevant, and accurate information is vital, particularly when resources are limited and agencies must prioritize their efforts. Information security continuous monitoring (ISCM) is defined as maintaining ongoing awareness of information security, vulnerabilities, and threats to support organizational risk management decisions. http://www.EnergyCollection.us/Companies/NIST/NIST-800-137.pdf Top
- ***Managing Information Security Risk - NIST Special Publication 800-39*** **-** 2011-03-01 - NIST Special Publication 800-39 is the flagship document in the series of information security standards and guidelines developed by NIST in response to FISMA. The purpose of Special Publication 800-39 is to provide guidance for an integrated, organization-wide program for managing information security risk to organizational operations (i.e., mission, functions, image, and reputation), organizational assets, individuals, other organizations, and the Nation resulting from the operation and use of federal information systems. Special Publication 800-39 provides a structured, yet flexible approach for managing risk that is intentionally broad-based, with the specific details of assessing, responding to, and monitoring

risk on an ongoing basis provided by other supporting NIST security standards and guidelines. The guidance provided in this publication is not intended to replace or subsume other risk-related activities, programs, processes, or approaches that organizations have implemented or intend to implement addressing areas of risk management covered by other legislation, directives, policies, programmatic initiatives, or mission/business requirements. Rather, the risk management guidance described herein is complementary to and should be used as part of a more comprehensive Enterprise Risk Management (ERM) program. http://www.EnergyCollection.us/Energy-Security/Managing-Information-Security.pdf Original link - http://csrc.nist.gov/publications/nistpubs/800-39/SP800-39-final.pdf Top

- ***National Cybersecurity Center of Excellence - NCCoE*** - http://csrc.nist.gov/nccoe/The-Center/The-Center.html Top
- ***NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 3.0*** – NIST Special Publication 1108R3 - Framework 3.0 updates the plan for transforming the nation's aging electric power system into an interoperable smart grid—a network that will integrate information and communication technologies with the power-delivery infrastructure, enabling two-way flows of energy and communications. The NIST Smart Grid Framework 3.0 responds to recent developments in grid modernization, including advances in architecture, cybersecurity, and testing and certification. The 239-page document includes a detailed list of 74 standards and protocols that have been identified by NIST as supporting interoperability of the smart grid, including seven new standards not previously listed in the 2.0 Framework. Framework 3.0 also reflects the April 2013 operational transition of the Smart Grid Interoperability Panel (SGIP) from the government-funded, public-private partnership launched by NIST in December 2009 to an industry-led non-profit organization. http://www.EnergyCollection.us/Companies/NIST/NIST-Framework-Roadmap-1108R3.pdf Top
  - ***Beginner's Guide*** – http://www.EnergyCollection.us/Companies/NIST/NIST-Framework-Roadmap-1108R3-B.pdf
- ***NIST Interagency or Internal Reports (NISTIRS)*** - NIST Interagency or Internal Reports (NISTIRs) describe research of a technical nature of interest to a specialized audience. The series includes interim or final reports on work performed by NIST for outside sponsors (both government and nongovernment). NISTIRs may also report results of NIST projects of transitory or limited interest, including those that will be published subsequently in more comprehensive form. http://csrc.nist.gov/publications/PubsNISTIRs.html Top
- ***NIST SGIP Cyber Security Working Group*** - http://collaborate.nist.gov/twiki-sggrid/bin/view/SmartGrid/CyberSecurityCTG Top
- ***NIST Smart Grid Collaboration Wiki for Smart Grid Interoperability Standards*** - http://collaborate.nist.gov/twiki-sggrid/bin/view/SmartGrid/CyberSecurityCTG Top
- ***NISTR 7628 – NIST Interagency Report, Guidelines for Smart Grid Cyber Security*** – Revision 1 - presents a comprehensive framework that organizations can use to develop effective cybersecurity strategies tailored to their particular combinations of smart grid-related characteristics, risks, and vulnerabilities. Organizations in the diverse community of smart grid stakeholders can use the methods and supporting information presented in this report as guidance for assessing cybersecurity risk and identifying and applying appropriate security requirements. 2014-09-01 http://www.EnergyCollection.us/Companies/NIST/NISTR-7628-R1-Overview.pdf Top

- ***NISTIR 7761 R1 – Smart Grid Interoperability Panel Priority Action Plan 2: Guidelines for Assessing Wireless Standards for Smart Grid Applications*** – 2014-06-01 - This report is a draft of key tools and methods to assist smart grid system designers in making informed decisions about existing and emerging wireless technologies. An initial set of quantified requirements have been brought together for advanced metering infrastructure (AMI) and initial distribution automation (DA) communications. These two areas present technological challenges due to their scope and scale. These systems will span widely diverse geographic areas and operating environments and population densities ranging from urban to rural. http://www.EnergyCollection.us/Companies/NIST/NISTR-7761-R1.pdf Top
- ***Special Publication 800-53 – Security and Privacy Controls for Federal*** **-** "Security and Privacy Controls for Federal Information Systems and Organizations," provides a catalog of security controls for all U.S. federal information systems except those related to national security. It is published by the National Institute of Standards and Technology, which is a non-regulatory agency of the United States Department of Commerce. NIST develops and issues standards, guidelines, and other publications to assist federal agencies in implementing the Federal Information Security Management Act of 2002 (FISMA) and to help with managing cost effective programs to protect their information and information systems. Wikipedia - http://en.wikipedia.org/wiki/NIST_Special_Publication_800-53 Revision 4 – http://www.EnergyCollection.us/Companies/NIST/800-53A-Revision-4.pdf Top
- Top

NRECA Cyber task Force To Serve Co-ops (ECT.coop) **-** https://www.nreca.coop/cyber-task-force-serve-co-ops-ect-coop/ Top

Ponemon Institute

- ***Ponemon Institute*** **-** Ponemon Institute conducts independent research on privacy, data protection and information security policy. Our goal is to enable organizations in both the private and public sectors to have a clearer understanding of the trends in practices, perceptions and potential threats that will affect the collection, management and safeguarding of personal and confidential information about individuals and organizations. Ponemon Institute research informs organizations on how to improve upon their data protection initiatives and enhance their brand and reputation as a trusted enterprise. Company website - http://www.ponemon.org Top
- ***2012 Cost of Cyber Crime Study: United States*** **-** sponsored by HP, conducted by the Ponemon Institute - 2013-10-10 - The purpose of this benchmark research is to quantify the economic impact of cyber attacks and observe cost trends over time. We believe a better understanding of the cost of cyber crime will assist organizations in determining the appropriate amount of investment and resources needed to prevent or mitigate the devastating consequences of an attack. Our goal is to be able to quantify with as much accuracy as possible the costs incurred by organizations when they have a cyber-attack. In our experience, a traditional survey approach would not capture the necessary details required to extrapolate cyber crime costs. Therefore, we decided to pursue field-based research that involved interviewing senior-level personnel and collecting details about actual cyber crime incidents. Approximately nine months of effort was required to recruit companies, build an activity-based cost model, collect source information and analyze results. http://www.EnergyCollection.us/Energy-Security/2012-Cost-Cyber.pdf Original link at: http://www.ponemon.org/local/upload/file/2012_US_Cost_of_Cyber_Crime_Study_FINAL6%20.pdf last accesses 2014-05-22 Top

    - ***2014 update –*** http://www.EnergyCollection.us/Companies/Ponnemon/2014-Cost-Cyber.pdf
- ***Cost of Failed Trust - 2013 Annual Report*** **-** Threats & Attacks - by the Ponemon Institute - http://www.EnergyCollection.us/Energy-Security/Cost-Failed-Trust-2013.pdf Top
- ***Critical Infrastructure: Security Preparedness and Maturity*** – 2014-07-01 - The purpose of this research is to learn how utility, oil and gas, alternate energy and manufacturing organizations are addressing cyber security threats. http://www.EnergyCollection.us/Energy-Security/Critical-Infrastructure-Security.pdf Top
- ***Ponemon 2014 SSH Security Vulnerability Report - Information Technology's Dirty Secret and Open Backdoors*** - Global organizations are under attack, and the attackers are more dangerous and persistent than ever. Armed with a litany of next-generation cybercrime tools, they're vastly different from yester-year hackers and better enabled with targeted and persistent tools. While the motivations vary, the goal of today's cybercriminal and nation-state attacker is to become and remain trusted on targeted network in order to gain full access to sensitive, regulated and valuable data and intellectual property, and circumvent all existing controls. Enterprises are increasingly turning to "next-generation" cybersecurity controls to detect advanced attacks, safeguard sensitive data and IP, and reduce the risk of compliance violations and data breaches. While the trend to deploy bigger, better and smarter end user devices and lower-cost, scalable software, and virtualized hardware continues, the basic technology building blocks of network trust remain firmly rooted within virtually all Global 2000 organizations. Research findings in this report reveal that enterprises are dependent and rely heavily on the Secure Shell cryptographic protocol (SSH) to ensure online trust and to protect valuable information, just as they should. When used correctly, SSH is a solid IT security protocol that keeps an organization's virtual security doors firmly locked and accessible by only the appropriate networked systems and users. Unfortunately, when left unprotected-through lack of visibility and controls-this security technology can be misused by malicious insiders and other cybercriminals, allowing them to authenticate into systems, servers and databases. The use of SSH keys provides adversaries with privileged and root status, which allows unfettered access to systems and data. The research also found that most respondents have no way to control, account for, or protect the thousands of SSH keys in use within their IT environments. A finding proving that the lessons learned from Edward Snowden's attack on the NSA, where SSH keys provided undetected access that allowed him to steal droves of classified documents, has changed little within Global 2000 organization's policies, procedures or controls for unprotected SSH keys. http://www.EnergyCollection.us/Energy-Security/Ponemon-2014-SSH.pdf Top
- Top

Principle of Least Privilege - In information security, computer science, and other fields, the principle of least privilege (also known as the principle of minimal privilege or the principle of least authority) requires that in a particular abstraction layer of a computing environment, every module (such as a process, a user or a program depending on the subject) must be able to access only the information and resources that are necessary for its legitimate purpose. Wikipedia - http://en.wikipedia.org/wiki/Least_privilege Top

PRISEM for Seattle **-** Public Regional Information Security Event Management (PRISEM) system, not to be confused with the National Security Agency's controversial PRISM project, the platform allows the City of Seattle's information security team to collect threat information from federal agencies and security firms, develop indicators of compromise, and look for malicious activity across the networks of PRISEM members. Top

Project Basecamp **-** Project Basecamp is a research effort by Digital Bond and a team of volunteer researchers to highlight and demonstrate the fragility and insecurity of most SCADA and DCS field devices, such as PLC's and RTU's. The goal of Project Basecamp is to make the risk of these fragile and insecure devices so apparent and easy to demonstrate that a decade of inaction will end. SCADA and DCS owner/operators will demand a secure and robust PLC, and this will drive vendors to finally provide a product worthy of being deployed in the critical infrastructure. http://www.digitalbond.com/tools/basecamp/ Top

Protecting Against Cybersecurity Threats Starts Now **-** The cybersecurity landscape today is littered with threats: botnets, insiders, worms, covert channels, ransomware, SQL injection, social engineering, spoofing, phishing, BYOD, DDOS, hacking, APT, cyber terrorism, and so many other threats that they cannot all be listed here. The reality is that there are many different cyber-attack vectors that affect every organization each day. November 2013 was the 25th anniversary of the Morris Internet worm and from that we learned that Internet-connected systems were vulnerable and need to be protected. To protect these devices, we built perimeter defenses to thwart worm, viruses, DDOS, and other external attacks. While traditional perimeter defenses are needed, the porous perimeters that have arisen from ubiquitous access via WIFI, Bluetooth, cellular, VPNs, mobile devices, and IP everything open new entry points into your enterprise network. http://www.EnergyCollection.us/Energy-Security/Protecting-Against-Cybersecurity.pdf Top

Protiviti

- ***From Cybersecurity to Collaboration: Assessing the Top Priorities for Internal Audit Functions*** – 2015 internal audit capabilities and needs survey http://www.EnergyCollection.us/Companies/Protiviti/From-Cybersecurity-Collaboration.pdf
- ***Board Perspectives: Risk Oversight*** – http://www.EnergyCollection.us/Companies/Protiviti/Board-Perspectives-Risk.pdf
- Top

PWC

- ***PWC- Center for Board Governance*** – http://www.pwc.com/us/en/corporate-governance/index.jhtml Top
- ***PWC on Cybersecurity*** **-** http://www.pwc.com/us/en/cfodirect/issues/cyber-security/index.jhtml Top
- Top

Red Team & Penetration Testing – see Wikipedia - Penetration testers assess organization security, often unbeknownst to client staff. This type of Red Team provides a more realistic picture of the security readiness than exercises, role playing, or announced assessments. The Red Team may trigger active controls and countermeasures within a given operational environment. http://en.wikipedia.org/wiki/Red_team Top

Regulators

- ***Cybersecurity and the PUC*** – article includes questions a state regulator should be asking utilities. http://www.EnergyCollection.us/Energy-Security/Cybersecurity-PUC.pdf Top
- ***How to Increase Cyber-Security in the Power Sector: A Project Report from the Australian Power Sector*** - To drive cyber-capabilities and resilience collectively a private-public partnership under the leadership of E-Control was carried out for the Austrian power sector in 2013 to systematically understand which assets need to be protected and define efficient and adequate defense mechanisms. The project goal was to identify and mitigate cyber-risks at organizational and system level and provide decision makers with simple actionable steps to improve cyber-resilience. http://www.EnergyCollection.us/Energy-Security/How-Increase-Cyber.pdf Top
- A ***Summary of State Regulators' Responsibilities Regarding Cybersecurity Issues***

Top

Report: Cyber Threats to Energy Sector Happening at Alarming Rate - Internet-based attacks on critical U.S. energy infrastructure are occurring at a greater rate than previously understood, according to a new government report. The report, issued by a cyber-security team that operates within the Department of Homeland Security, found that thousands of control systems used in critical infrastructure are linked directly to the Internet and are vulnerable to attack by viruses and other malware. http://www.EnergyCollection.us/Energy-Security/Report-Cyber-Threats.pdf Top

Is there a Role for Government in Cyber Security - NPR episode - 2012-08-07 - The Cyber Security Act of 2012 failed in the Senate, despite growing alarm in the intelligence community about the vulnerabilities of the nation's infrastructure. The episode highlights a unique problem for politicians concerned about the balance between national security and federal regulation. http://www.EnergyCollection.us/Energy-Security/Is-There-A-Role.pdf Top

SANS Institute - The SANS (SysAdmin, Audit, Network, Security) Institute was established in 1989 as a cooperative research and education organization. The SANS Institute enables more than 165,000 security professionals, auditors, system administrators, and network administrators to share the lessons they are learning and find solutions to the challenges they face. At the heart of SANS are the many security practitioners in government agencies, corporations, and universities around the world who invest hundreds of hours each year in research and teaching to help the entire information security community Company website - http://www.sans.org Top

- ***Critical Security Controls for Effective Cyber Defense*** - The Critical Security Controls focuses first on prioritizing security functions that are effective against the latest Advanced Targeted Threats, with a strong emphasis on "What Works" - security controls where products, processes, architectures and services are in use that have demonstrated real world effectiveness. Standardization and automation is another top priority, to gain operational efficiencies while also improving effectiveness. The actions defined by the Controls are demonstrably a subset of the comprehensive catalog defined by the National Institute of Standards and Technology (NIST) SP 800-53. The Controls do not attempt to replace the work of NIST, including the Cybersecurity Framework developed in response to Executive Order 13636. The Controls instead prioritize and focus on a smaller number of actionable controls with high-payoff, aiming for a "must do first" philosophy. Since the Controls were derived from the most common attack patterns and were vetted across a very broad community of government and industry, with very strong consensus on the resulting set of controls, they serve as the basis for immediate high-value action. http://www.sans.org/critical-security-controls/ http://www.EnergyCollection.us/Companies/SANS/Critical-Security-Controls.pdf Top

- ***Implementing an Effective IT Security Program*** - The purpose of this paper is to take the wide variety of US federal laws, regulations, and guidance combined with industry best practices and define the essential elements of an effective IT security program. The task may seem impossible given the thousands of pages of security documentation published by the National Institute of Standards and Technology (NIST), the Office of Management and Budget (OMB), the National Security Agency (NSA), and the General Accounting Office (GAO), just to name a few. http://www.EnergyCollection.us/Companies/SANS/Implementing_Effective_IT.pdf
- ***SANS Internet Storm Center*** **-** gathers millions of intrusion detection log entries every day, from sensors covering over 500,000 IP addresses in over 50 countries. It is rapidly expanding in a quest to do a better job of finding new storms faster, identifying the sites that are used for attacks, and providing authoritative data on the types of attacks that are being mounted against computers in various industries and regions around the globe. https://isc.sans.edu/ Top
- ***SANS Securing the Human*** – provides materials to support a high impact security awareness program - http://www.securingthehuman.org/ Top

SCADA

- ***How to Stop Malware Attacks on SCADA Systems*** **–** http://www.EnergyCollection.us/Energy-Security/How-Stop-Malware.pdf Top
- **The *SCADA Security Survival Guide*** **-** http://www.csoonline.com/article/731294/the-scada-security-survival-guide Top
- ***SCADA System Cyber Security - A Comparison of Standards*** **-** 8 pages - http://www.EnergyCollection.us/Energy-Security/SCADA-System-Cyber.pdf Top
- Top

Schneider Electric

A Framework for Developing and Evaluating Utility Substation Cyber Security - The utility industry is under pressure to improve substation automation cyber security. Manufacturers of substation products use proprietary or product-specific methodologies for managing device security. As a result, standardization and ease of management of these devices is lacking. This paper reviews processes and procedures for securing a substation, offers advice for overcoming substation asset management challenges, and describes some of the tools available. http://www.Companies/Schneider/Framework-Developing-Cybersecurity.pdf Top

Top

Security and Exchange Commission

- ***OCIE Cybersecurity Initiative*** – 2014-04-15 - The U.S. Securities and Exchange Commission's Office of Compliance Inspections and Examinations (OCIE) previously announced that its 2014 Examination Priorities included a focus on technology, including cybersecurity preparedness.2 OCIE is issuing this Risk Alert to provide additional information concerning its initiative to assess cybersecurity preparedness in the securities industry. Original Link – http://www.EnergyCollection.us/Energy-Security/OCIE-Cybersecurity-Initiative.pdf http://www.sec.gov/ocie/announcement/Cybersecurity+Risk+Alert++%2526+Appendix+-+4.15.14.pdf – last accessed 2014-07-01 Top

- Top

Security and States **-** No state regulator wants to wake up one day and learn that hackers have brought down the power grid in his or her state. At the same time, many state regulators want to encourage modernization of the electric grid. They realize that making the grid smarter could make it more vulnerable to cyber attacks. But state regulators struggle to define their role in promoting cybersecurity. State commissions face several dilemmas. Even the largest states must work with tight budgets and limited expertise. Nor are individual electric utilities well prepared to handle the novel and complex challenges of cybersecurity. Cybersecurity standards at the federal and industry level are slow to be adopted. And it isn't clear how regulation, state or federal, can be effective in producing desired results. http://www.EnergyCollection.us/Energy-Security/Security-States.pdf Top

Security Wizardry Information Portal **- *i***s a FREE Information Security portal containing a directory of our users favorite security products, all of which are open to be rated or slated. It is also home to the famous Talisker Radar Page used by thousands, even the US NSA. Company website - http://www.securitywizardry.com Top

SecurityWeek **-** Company website - http://www.securityweek.com Top

Senators ask FERC to helm "expeditious comprehensive" probe of grid security **-** 2012-07-19 - http://www.EnergyCollection.us/Energy-Security/Senators-Ask-FERC.pdf Top

Smart Grid Security Blog **-** http://smartgridsecurity.blogspot.com/ Top

Social Engineering

- ***The Basics*** - http://www.EnergyCollection.us/Energy-Security/Social-Engineering-Basics.pdf Original referenced 2014-06-01 - http://www.csoonline.com/article/2124681/security-awareness/social-engineering-the-basics.html Top
- ***Wikipedia*** **-** http://en.wikipedia.org/wiki/Social_engineering_(security)
- Top

Stuxnet **-** It is now recognized that air-gapped systems are still vulnerable despite the air gap. (most notable example is Stuxnet). http://en.wikipedia.org/wiki/Stuxnet and http://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet# Top

- ***Stuxnet Five Years Later - Did We take the Right Lessons?*** **-** The 5th anniversary is approaching, of the day the Stuxnet worm came into public view. The worm triggered changes in industrial control systems products, networks and methodologies. Looking back - what did we learn? Did we look for lessons where the light was brightest? Or did we look in the dark corners where our need was greatest? The bright light shining was "best practice violations." What did the light show us? 2015-03-10 http://www.EnergyCollection.us/Companies/Waterfall-Security/Stuxnet-Five-Years.pdf Top

Surviving on a Diet of Poisoned Fruit: Reducing the National Security Risks Of America's Cyber Dependencies – 2014-07-01 - The first part of this paper illuminates this intertwining. The second part surveys the evolution of strategies to achieve greater cybersecurity. Disadvantaged by early design choices that paid little attention to security, these strategies provide some needed protection, especially when applied collectively as a coordinated "defense in depth." But they do not and never can assure comprehensive protection; these strategies are typically costly, and users will commonly choose to buy less security than they could obtain because of the operational, financial or convenience costs of obtaining that security. http://www.EnergyCollection.us/Energy-Security/Surviving-Diet-Poisoned.pdf Top

Targeted Attacks Against the Energy Sector **-** 2014-01-13 - by Symantec - The energy sector has become a major focus for targeted attacks and is now among the top five most targeted sectors worldwide. Companies in the sector are facing a growing risk of having their services interrupted or losing data. The threat to energy firms is only likely to increase in the coming years as new developments, such as further extensions of smart grids and smart metering expose more infrastructure to the Internet. Equipment that is not connected to the Internet and other networks is not immune to threats and there has already been a number of successful attacks against isolated systems. Operators of critical infrastructure, as well as energy utility companies, need to be aware of these threats and prepare accordingly. The threat to energy firms comes from several different sources. In some cases, espionage from competitors is the primary motive, with data on new projects, exploration and finances being targeted. Disruption and destruction are the goals of other attacks. Some instances appear to be state sponsored, such as the disruption of the Iranian nuclear program by the Stuxnet worm in 2010, one of the attacks that began this trend. Others appear to be the work of hacktivists with political or environmental agendas. Internal attackers, like disgruntled employees, are also a major source of attacks that often lead to service disruption. The majority of the actors behind these attacks have grown more sophisticated in the way they attack. During the monitoring period from July 2012 to June 2013, we observed an average of 74 targeted attacks per day globally. Of these, nine attacks per day targeted the energy sector. Accounting for 16.3 percent of all attacks, the energy sector was the second most targeted vertical in the last six months of 2012, with only the government/public sector exceeding it with 25.4 percent of all attacks. The high ranking was mainly due to a major attack against a global oil company, which we observed in September 2012. However, in the first half of 2013 the energy sector continued to attract a high proportion of attacks, ranking in fifth place with 7.6 percent of targeted attacks. Not all of the attacks analyzed used highly sophisticated tools. Most of them could have been prevented by following best practice guidelines for protecting the IT infrastructure and the industrial components, indicating that despite high revenues and strategic importance, many energy sector companies are not prioritizing cybersecurity. http://www.EnergyCollection.us/Energy-Security/Targeted-Attacks-Against.pdf Top

- Page 7 - "Historically most industrial control systems (ICS) and supervisory control and data acquisition (SCADA) systems were in separated networks not connected to the Internet or any other network. Unfortunately this security through segregation approach does not fully protect against cyberattacks. In reality, networks are rarely completely isolated. Often some configuration updates are periodically installed or log files are transferred. If systems are not directly connected, the method of choice for these types of interactions is usually through a USB stick or a non-permanent modem connection, which provides a way into the restricted networks. This allows malware to spread into such isolated networks as demonstrated many times by threats such as Stuxnet. If networks are truly segregated, this would mean that there would be no software updates installed, leaving old vulnerabilities open. There are also issues around processes. For example, the revocation lists for digital certificates are seldom updated and therefore certificates which are no longer valid cannot be checked properly and would still be accepted. " Top

- Page 11 - "Part of the malware code [Stuxnet] was signed with stolen digital certificates making it harder to detect by security tools." Top
- Page 26 - as part of the discussion regarding the Incursion Phase of an attack - "Depending on the protection measures implemented by the target, the attackers may also digitally sign their malware creation. In the past there have been quite a few cases where code signing certificates were stolen and later misused to sign malware in order to pass it unnoticed to high value targets." Top

TechTarget - SearchSecurity **-** IT security pros turn to SearchSecurity.com and Information Security Magazine Online for the information they require to keep their corporate data, systems and assets secure. We're the only information resource that provides immediate access to breaking industry news, virus alerts, new hacker threats and attacks, security certification training resources, security standard compliance, webcasts, white papers, podcasts, Security Schools, a selection of highly focused security newsletters and more -- all at no cost. Nowhere else will you find such a highly targeted combination of resources specifically dedicated to the success of today's IT-security professional. http://searchsecurity.techtarget.com/ Top

Telephone Industries Association - Cybersecurity **-** http://www.tiaonline.org/policy/cybersecurity Top

Testimony Before the Committee on Energy and Natural Resources, US Senate **-** Cybersecurity, Challenges in Securing the Electricity Grid - http://www.EnergyCollection.us/Energy-Security/Challenges-Securing-Electricity.pdf Top

Think Data Breaches Can't Happen To You? **-** A look into recent breaches and how to defend against them - http://www.EnergyCollection.us/Energy-Security/Think-Data-Breaches.pdf Top

Threat-Intel Sharing Services Emerge, But Challenges Remain **-** http://www.EnergyCollection.us/Energy-Security/Threat-Intel-Sharing.pdf Original link: http://tinyurl.com/nv74g9o accessed 2014-06-22 Top

It's Time for Corporate Boards to tackle Cybersecurity. Here's Why **-** http://www.EnergyCollection.us/Energy-Security/Time-Corporate-Boards.pdf Top

Time report on Smart Grid vulnerability **-** http://www.time.com/time/nation/article/0,8599,1891562,00.html Top

Training

- ***Protective Security Advisor*** **–** DHS free services
- Top

Transformers Expose Limits in Securing Power Grid **-** 2014-03-04 - WSJ - The U.S. electric grid could take months to recover from a physical attack due to the difficulty in replacing one of its most critical components. http://www.EnergyCollection.us/Energy-Security/Transformers-Expose-Limits.pdf Top

Two Factor Authentication - provides unambiguous identification of users by means of the combination of two different components. These components may be something that the user knows, something that the user possesses or something that is inseparable from the user. A good example from everyday life is the withdrawing of money from a cash machine. Only the correct combination of a bank card (something that the user possesses) and a PIN (personal identification number, i.e. something that the user knows) allows the transaction to be carried out. http://en.wikipedia.org/wiki/Two_factor_authentication Top

UglyGorilla Hack of US Utility Exposes Cyberwar threat **-** Somewhere in China, a man typed his user name, “ghost,” and password, “hijack,” and proceeded to rifle the computers of a utility in the Northeastern U.S. He plucked schematics of its pipelines. He copied securityguard patrol memos. He sought access to systems that regulate the flow of natural gas. He cruised channels where keystrokes could cut off a city’s heat, or make a pipeline explode. That didn’t appear to be his intention, and neither was economic espionage. While he was one of the Chinese officers the U.S. charged last month with infiltrating computers to steal corporate secrets, this raid was different. The hacker called UglyGorilla invaded the utility on what was probably a scouting mission, looking for information China could use to wage war. http://www.EnergyCollection.us/Energy-Security/UglyGorilla-Hack-US.pdf Top

Understanding the physical and economic consequences of attacks on control systems **-** This paper describes an approach for developing threat models for attacks on control systems. These models are useful for analyzing the actions taken by an attacker who gains access to control system assets and for evaluating the effects of the attacker's actions on the physical process being controlled. The paper proposes models for integrity attacks and denial of service (DoS) attacks, and evaluates the physical and economic consequences of the attacks on a chemical reactor system. The analysis reveals two important points. First, a DoS attack does not have a significant effect when the reactor is in the steady state; however, combining the DoS attack with a relatively innocuous integrity attack rapidly causes the reactor to move to an unsafe state. Second, an attack that seeks to increase the operational cost of the chemical reactor involves a radically different strategy than an attack on plant safety (i.e., one that seeks to shut down the reactor or cause an explosion). http://www.EnergyCollection.us/Energy-Security/Understanding-Physical-Economic.pdf Top

Unidirectional Gateways **-** See http://en.wikipedia.org/wiki/Unidirectional_network and suppliers http://www.waterfall-security.com/ and http://somerdata.com/ Top

Unidirectional Security Gateways vs. Firewalls: Comparing Costs **-** Which costs more: a solution based on Waterfall Unidirectional Security Gateways, or one based on conventional firewalls? In principle, the question has no clear answer, because it is not possible to configure conventional firewalls to be as secure as a hardware-enforced

Unidirectional Gateway solution. In practice though, one can compare the costs of best-practice firewall-based solutions to the cost of a Waterfall solution, even though the security benefits of the “best practice” architecture are inherently inferior to those of a Waterfall Unidirectional Gateway. This report compares the perimeter-protection capital, support and operating costs of Unidirectional Gateways to those of best-practice firewalls. Throughout this discussion, we assume that the perimeter in question is the perimeter separating a “control system” or “plant” network from a corporate/business network. Best-practice configurations and advice are drawn from industrial sources, including NERC-CIP, API-1164 and ISA SP-99, as they apply to the plant/business perimeter. http://www.EnergyCollection.us/Companies/Waterfall-Security/Unidirectional-Security-Gateways-Firewalls.pdf Top

Unveiling "The Mask": Sophisticated malware ran rampant for 7 years - A cyber espionage operation that used highly sophisticated multi-platform malware went undetected for more than five years and compromised computers belonging to hundreds of government and private organizations in more than 30 countries. Details about the operation were revealed Monday in a paper by security researchers from antivirus firm Kaspersky Lab who believe the attack campaign could be state sponsored. The Kaspersky researchers dubbed the whole operation “The Mask,” the English translation for the Spanish word Careto, which is what the attackers called their main backdoor program. Based on other text strings found in the malware, the researchers believe its authors are probably proficient in Spanish, which is unusual for an APT (advanced persistent threat) campaign. http://www.EnergyCollection.us/Energy-Security/Unveiling-The-Mask.pdf “Different variants of the backdoor programs used in The Mask over the years have been identified, the oldest of which appears to have been compiled in 2007. Most samples were digitally signed with valid certificates issued to a company called TecSystem Ltd. from Bulgaria, but it’s not clear if this company is real. One certificate was valid between June 28, 2011 and June 28, 2013. The other was supposed to be valid from April 18, 2013 to July 18, 2016, but has since been revoked by VeriSign." Kaspersky Paper - http://www.EnergyCollection.us/Energy-Security/Unveiling-Careto.pdf Top

Is U.S. Cybersecurity plan a carrot, stick or legal nightmare? - a discussion about legal implications of the NIST Cybersecurity Framework should court action follow from a utility cyber breach - http://www.EnergyCollection.us/Energy-Security/US-Cybersecurity-Plan.pdf Top

The U.S. Electric Grid is Safer than you probably think – 2014-09-10 – http://www.EnergyCollection.us/Energy-Security/US-Electric-Grid.pdf Top

U.S. Risks National Blackout From Small-Scale Attack - Federal Analysis Says Sabotage of Nine Key Substations Is Sufficient for Broad Outage - http://www.EnergyCollection.us/Energy-Reliability/US-Risks-National.pdf Top

U.S. Steps Up Alarm Over Cyberattacks - 2013-03-13 - Wall Street Journal - http://www.EnergyCollection.us/Energy-Security/US-Steps-Up.pdf Top

U.S. Utility’s Control System was hacked, says Homeland Security – 2014-05-20 - (Reuters) - A sophisticated hacking group recently attacked a U.S. public utility and compromised its control system network, but there was no evidence that the utility's operations were affected, according to the Department of Homeland Security. DHS did not identify the utility in a report that was issued this week by the agency's Industrial Control Systems Cyber Emergency Response Team, or ICS-

CERT. http://www.EnergyCollection.us/Energy-Security/US-Utilities-Control.pdf Original at: http://tinyurl.com/mvfawtn last accessed 2015-03-15 Top

Utilities Need Test Bed to Evaluate Legacy Industrial Control System Cybersecurity Technologies **-** Industrial control systems (ICSs) are technologically and administratively different than information technology (IT) systems. ICSs are purpose-built systems engineered for highly reliable operations in harsh settings 24/7/365 and operate like a well-engineered clock. They often use older, resource-constrained systems and devices. They are deterministic systems that must function precisely within well-defined and regulated periods often within tens to hundreds of milliseconds. Drifting beyond that precise cycle time through variations of latency can lead to denial-of-service or worse. http://www.EnergyCollection.us/Energy-Security/Utilities-Need-Test.pdf Top

Utilities Report Cyber Incidents to Energy Department **–** Subsidiaries of ITC Holdings, Duke Energy and NRG Energy Tell DOE of suspected Cyberattacks – 2014-07-02 - The utilities, subsidiaries of ITC Holdings Corp. , Duke Energy Corp. and NRG Energy Inc., each filed a report to the Energy Department in the past year detailing suspected cyberattacks. The reports highlight the interest by hackers in targeting energy firms, and the vulnerabilities of IT systems used to run power generation and distribution equipment. http://www.EnergyCollection.us/Energy-Security/Utilities_Report_Cyber_Incidents.pdf Original link last accessed 2014-07-10 - http://tinyurl.com/q3z2qfo Top

Utilities Telecom Council - UTC **-** UTC is the source and resource for information and communications technology (ICT) solutions, collaboration, and advocacy for utilities and other critical infrastructure industries. Company website link - http://www.utc.org/cybersecurity/all Top

Venafi Predicts: 100 Percent of Mobile Malware Will Misuse Compromised Digital Certificates by the End of 2014 **-** IT Security 'Achilles Heel' Will Emerge; Certificate Authorities Will Become More Transparent SALT LAKE CITY, UT--(Marketwired - Jan 22, 2014) - Venafi, the leading provider of Next-Generation Trust Protection, today released predictions for cybersecurity market trends in 2014. Key predictions provide insights into how cybercriminals and nation-backed operators will continue to exploit trust-infrastructure security vulnerabilities to launch advanced attacks to compromise networks, inject malware, and steal valuable data and IP. These attacks on trust adversely impact the financial and business stability of targeted organizations, the majority of which are unaware of this new threat vector. http://www.EnergyCollection.us/Energy-Security/Venafi-Predicts-100-Percent.pdf Top

Verizon

- ***5 Tips to Cybersecure the Power Grid*** **-** 2014-04-22 - Since 2012, McGurk has led Verizon's Investigative Response team for industrial control and automated and embedded systems security, where he's taken on the industry-spanning cybersecurity threats faced by a global telecommunications provider. Verizon's annual Data Breach Investigations Report (DBIR) tracks these threats, and the latest version released Tuesday shows that the number of threats is growing. All told, Verizon's report found 63,437 security incidents in 2013, compared to about 47,000 in the previous year, as well as 1,367 confirmed data breaches, up from 621 in the previous year. And while the majority of these reports come from the public sector, finance, IT and retail sectors, this latest DBIR includes expanded details on how utilities, manufacturers and other non-financial partners are being affected, he said. http://www.EnergyCollection.us/Energy-Security/5-Tips-Cybersecure.pdf Top

- ***2013 Data Breach Investigations Report [of 2012]* -** Perhaps more so than any other year, the large scale and diverse nature of data breaches and other network attacks took center stage. But rather than a synchronized chorus making its debut on New Year's Eve, we witnessed separate, ongoing movements that seemed to come together in full crescendo throughout the year. And from pubs to public agencies, mom-and-pops to multi-nationals, nobody was immune. As a result—perhaps agitated by ancient Mayan doomsday predictions—a growing segment of the security community adopted an "assume you're breached" mentality. Motives for these attacks appear equally diverse. Money-minded miscreants continued to cash in on low-hanging fruit from any tree within reach. Bolder bandits took aim at better-defended targets in hopes of bigger hauls. Activist groups DoS'd and hacked under the very different—and sometimes blurred—banners of personal ideology and just-for-the-fun-of-it lulz. And, as a growing list of victims shared their stories, clandestine activity attributed to state-affiliated actors stirred international intrigue. All in all, 2012 reminded us that breaches are a multi-faceted problem, and any one-dimensional attempt to describe them fails to adequately capture their complexity. The 2013 Data Breach Investigations Report (DBIR) corroborates this and brings to bear the perspective of 19 global organizations on studying and combating data breaches in the modern world1. The list of partners is not only lengthy, but also quite diverse, crossing international and public/private lines. It's an interesting mix of law enforcement agencies, incident reporting/handling entities, a research institution, and other incident response (IR)/forensic service firms. What's more, these organizations contributed a huge amount of data to the report. All told, we have the privilege of setting before you our analysis of more than 47,000 reported security incidents and 621 confirmed data breaches from the past year. Over the entire nine-year range of this study, that tally now exceeds 2,500 data breaches and 1.1 billion compromised records. We continue to learn a great deal from this ongoing study, and we're glad to have the opportunity once again to share these findings with you. As usual, we begin with a few highlights. http://www.EnergyCollection.us/Energy-Security/2013-Data-Breach.pdf Top
    - "20% of network intrusions involved manufacturing, transportation, and utilities" Page 5
    - "14% of network intrusions involved insiders: Page 5
    - "76% of network intrusions exploited weak or stolen credentials" Page 6
    - "66% of network intrusions took months or more to discover" Page 6
- ***2014 Data Breach Investigations Report*** - http://www.EnergyCollection.us/Energy-Security/2014-Data-Breach.pdf Top
- Top

Virus Infection At An Electric Utility - 2012 infection in a turbine control system - see page 2 of http://www.EnergyCollection.us/Energy-Security/Virus-Infection-Electric.pdf
Top

VLANs

VLAN Definition - See Wikipedia - In computer networking, a single layer-2 network may be partitioned to create multiple distinct broadcast domains, which are mutually isolated so that packets can only pass between them via one or more routers; such a domain is referred to as a virtual local area network, virtual LAN or VLAN. http://en.wikipedia.org/wiki/Virtual_LAN Top

Waterfall Security

- ***13 Ways Through a Firewall*** **-** what you don't know can hurt you - http://www.EnergyCollection.us/Energy-Security/13-Ways-Through-2.pdf Top
- ***BES-Control Centers - Secure ICCP and IEC 60870-104 Communications*** **-** Waterfall for Bulk Electric System (BES) Control Centers securely transmits Inter Control Center Protocol (ICCP) and IEC 60870-104 data and commands between BES Control Centers and other BES utilities. BES Control Centers fundamentally need to both send commands to and receive status information from other utilities, utilities such as generating utilities, transmission utilities and other BES Control Centers. The information and commands exchanged range from generating, transmission and balancing authority status information, to generator peaking orders, transmission capacity scheduling and real-time market orders. With this fundamental requirement for continuous interactive information flow, BES Control Centers are fundamentally at risk. Firewalls cannot provide the security essential to BES Control Centers. http://www.EnergyCollection.us/Companies/Waterfall-Security/BES-Control-Centers.pdf Top
- ***Can the Power Grid Be Hacked? Why Experts Disagree*** **-** UTC Journal - 2013-04-01 - Pages 51-53 – http://www.EnergyCollection.us/Energy-Security/Can-Power-Grid.pdf Top
- ***Introduction to Waterfall Unidirectional Security Gateways: True Unidirectionality, True Security*** **-** Historically industrial sites were secured by so-called “air gaps.” Most control system networks were not connected to any public network at all, and so the spread of malware over connections from public networks to control networks was impossible, as was the remote control of industrial control systems by adversaries using public networks. That changed in the mid-1990's – operators of these sites learned there were significant profits possible from the use of real-time inventory data, equipment usage data and other information drawn from control systems. Sites started connecting their control system networks to their corporate networks, exposing the formerly isolated control networks to attack. For the last decade, securing these connections between control networks and external networks has received steadily increasing attention. In the last 24 months, high-profile "advanced persistent threat" attacks have successfully compromised an appalling number of seemingly well-secured critical infrastructures and utilities, as well as military, government and corporate networks. Imagine learning that parts of your safety-critical control system are under the thumb of adversaries on the other side of the planet. In response to these trends, corporate security teams increasingly deploy Waterfall’s Unidirectional Security Gateways. A Unidirectional Gateway is simple in concept - a transmitting (TX) appliance in the control system network contains a laser, and a receiving (RX) appliance in the corporate network contains a photocell. The TX can send to the RX, but not vice-versa. http://www.EnergyCollection.us/Companies/Waterfall-Security/Introduction-Waterfall-Unidiretional.pdf Top
- ***IT/OT Integration Done Right and Done Wrong*** **-** Discussion of issues integrating IT and OT networks and solutions. Original at http://www.bluetoad.com/publication/?i=218589&p=19 Permanent copy at - http://www.EnergyCollection.us\Companies\Waterfall-Security\IT-OT-Integration.pdf
- The ***Firewall Loophole - easy, Insecure NERC CIP Compliance*** **-** Security is taking all reasonable steps to protect the reliability of the Bulk Electric System from enemies seeking to impair that system. Compliance is doing whatever some authority tells us to, whether such action is useful or not. Much has been debated about so-called loopholes in NERC CIP. The biggest loophole in NERC CIP is not whether some communications pattern is routable, or the maximum time a site has to apply security updates. The biggest loophole in NERC CIP is CIP's continued endorsement of the use of firewalls. The

NERC CIP standards permit firewalls, and the NERC organization has published countless firewall-based network architectures and evaluated those architectures for compliance. No CIP authority is on record cautioning utilities as to the very real security risks of using the firewall loophole. This in spite of the widespread understanding that firewalls do not provide adequate protection for critical assets, because of the many well-known and fundamental limits of firewalls. Penetration testers, ethical hackers and other experts all report breaching perimeter firewalls on their way to demonstrating cyber-sabotage or data theft capabilities inside a compliant critical network. http://www.EnergyCollection.us/Companies/Waterfall-Security/Firewall-Loophole.pdf Top

- ***NERC CIP V5 Standards Position - Unidirectional Security Gateways as Secure Alternatives to Firewalls and Network Intrusion Detection Systems*** - 2014-09-01 - The CIP V5 standards recognize that Unidirectional Security Gateways provide security which is stronger than firewalls, and position the gateways as an alternative to firewalls and costly Network Intrusion Detection Systems (NIDS). The V5 CIP standards have 103 requirements overall, and provide exemptions from 37 Medium-Impact requirements, and 5 High-Impact requirements, when Waterfall's Unidirectional Security Gateways are used to protect an Electronic Security Perimeter (ESP) rather than using firewalls and NIDS. Unidirectional Security Gateways increase the security of critical control systems, simplify and reduce the ongoing cost of CIP V5 compliance programs, and eliminate the need to use high-maintenance firewalls and NIDS. http://www.EnergyCollection.us/Companies/Waterfall-Security/NERC-CIP-V5.pdf Top
- ***Stronger than Firewalls*** - And Cheaper Too - The cost of deploying hardware-enforced unidirectional security gateways are dominated by up-front capital expenses and easily-identified recurring operational expenses. Plant/enterprise firewall costs are dominated by less-visible management and labor costs. Join Joel Langill and Andrew Ginter to examine the cost of managing firewalls according to ICS best-practice guidelines, standards and regulations. We explore hidden firewall costs in depth, including routine/monthly firewall management costs, extraordinary/annual recurring costs, the costs of compensating measures recommended by some authorities, such as NIDS systems, and the cost of preventable incidents. http://www.waterfall-security.com/recorded-webinar-stronger-than-firewalls-%E2%80%93-and-cheaper-too/ Presentation PDF - http://www.EnergyCollection.us/Companies/Waterfall-Security/Stronger-Than-Firewalls-Preso.pdf Top
- ***Unidirectional Security Gateways - Secure Transmission Substations Application*** **-** Substation automation solutions are essential to the safe and reliable operation of Bulk Electric Systems (BESs). Real-time data produced by substation automation systems and Intelligent Electronic Devices (IEDs) is vital to Energy Management Systems (EMSs), as well as BES situational awareness and fault tree analysis. Public Internet Protocol (IP) and Wide Area Networks (WANs) are used increasingly as a way to reduce communications systems costs, while maximizing the flexibility and capability of substation communications. Conventional thinking is that utilities must deploy firewalls, monitor them closely, and manage them very carefully, to ensure that network-based threats and vulnerabilities do not combine to become reliability-threatening incidents. This thinking is increasingly being questioned. Using firewalls to protect transmission and distribution substations introduces unacceptable risks to the security and reliability of substation operations. http://www.EnergyCollection.us/Companies/Waterfall-Security/USG-Secure-Transmission-Substations.pdf Top
- ***Company website*** – http://www.waterfallsecurity.com Top

Why VLAN Security isn't SCADA Security at all – http://www.EnergyCollection.us/Energy-Security/Why-VLAN-Security.pdf Original last reviewed 2014-07-29 at https://www.tofinosecurity.com/blog/why-vlan-security-isnt-scada-security-all Top

Wardriving the Smart Grid: practical approaches to attacking utility packet radios - http://www.EnergyCollection.us/Energy-Security/Wardriving-Smart-Grid.pdf Top

Watering Hole Attacks – see http://en.wikipedia.org/wiki/Watering_Hole Top

What Are the Top Three Things Every Utility CIO Should Worry About When it Comes to Cybersecurity - http://www.EnergyCollection.us/Energy-Security/What-Are-Top.pdf Top

What Not To Do In a Cyberattack - http://www.EnergyCollection.us/Energy-Security/What-Not-Do.pdf Top

X.509 Certificate Management: Avoiding Downtime and Brand Damage - Gartner Research - Organizations rely on X.509 digital certificates to secure their digital presences inside and outside their environments. System downtime often results from certificate expiration, resulting in brand damage. Organizations must manage their inventories of certificates and eliminate unplanned expiry. http://www.EnergyCollection.us/Energy-Security/X509-Certificate-Management.pdf Top

Paul Feldman

PaulFeldman@Gmail.com

LinkedIn - www.linkedin.com/in/paulfeldman/

Comments on how to improve this resource are welcome at the above address.

It my intent to maintain and improve this resource over time as an assist to Boards of Directors involved in the Electricity and Natural Gas Sector.