Berkshire Hathaway Energy

PacifiCorp Security

Prevent – Detect – Respond - Recover

Devon Streed

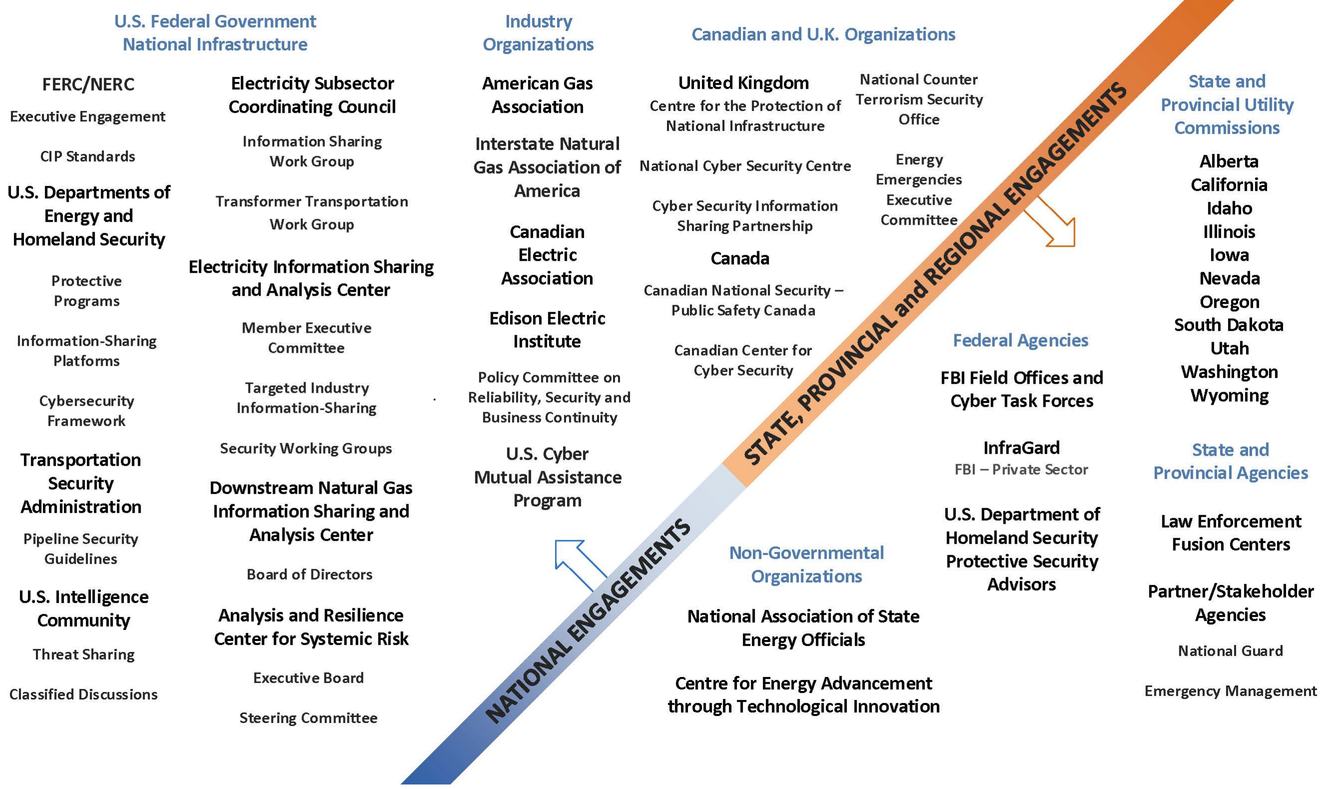
Director, Security and Information Protection

Organization

- Berkshire Hathaway Energy Chief Security Office
- Global Focus / Local Management
  - Information sharing
  - Intelligence
  - Enhanced coverage and efficiencies
- Roles and Responsibilities
  - PacifiCorp: Physical Security, Cyber Security, Business Continuity
  - BHE: Physical Security

External Engagements

Berkshire Hathaway Energy Corporate Security Engagements



U.S. Federal Government National Infrastructure

FERC/NERC

Executive Engagement

CIP Standards

U.S. Departments of Energy and Homeland Security

Protective Programs

Information-Sharing Platforms

Cybersecurity Framework

Transportation Security Administration

Pipeline Security Guidelines

U.S. Intelligence Community

Threat Sharing

Classified Discussions

Electricity Subsector Coordinating Council

Information Sharing Work Group

Transformer Transportation Work Group

Electricity Information Sharing and Analysis Center

Member Executive Committee

Targeted Industry Information-Sharing

Security Working Groups

Downstream Natural Gas Information Sharing and Analysis Center

Board of Directors

Analysis and Resilience Center for Systemic Risk

Executive Board

Steering Committee

Industry Organizations

American Gas Association

Interstate Natural Gas Association of America

Canadian Electric Association

Edison Electric Institute

Policy Committee on Reliability, Security and Business Continuity

U.S. Cyber Mutual Assistance Program

Canadian and U.K. Organizations

United Kingdom

Centre for the Protection of National Infrastructure

National Cyber Security Centre

Cyber Security Information Sharing Partnership

National Counter Terrorism Security Office

Energy Emergencies Executive Committee

Canada

Canadian National Security – Public Safety Canada

Canadian Center for Cyber Security

NATIONAL ENGAGEMENTS

STATE, PROVINCIAL and REGIONAL ENGAGEMENTS

Non-Governmental Organizations

National Association of State Energy Officials

Centre for Energy Advancement through Technological Innovation

Federal Agencies

FBI Field Offices and Cyber Task Forces

InfraGard

FBI – Private Sector

U.S. Department of Homeland Security Protective Security Advisors

State and Provincial Utility Commissions

Alberta
California
Idaho
Illinois
Iowa
Nevada
Oregon
South Dakota
Utah
Washington
Wyoming

State and Provincial Agencies

Law Enforcement Fusion Centers

Partner/Stakeholder Agencies

National Guard

Emergency Management

Functional Roles

- Security Operations
  - Global Security Operations Center
  - Analysis / threat hunting
  - Protective services
  - Investigations
- Security Engineering
  - Infrastructure / systems
  - Projects
  - Operational technology support
- Security Assurance
  - Business continuity planning
  - Programs: phishing, training, exercises
  - Policies and documentation
  - Compliance reporting

Phishing

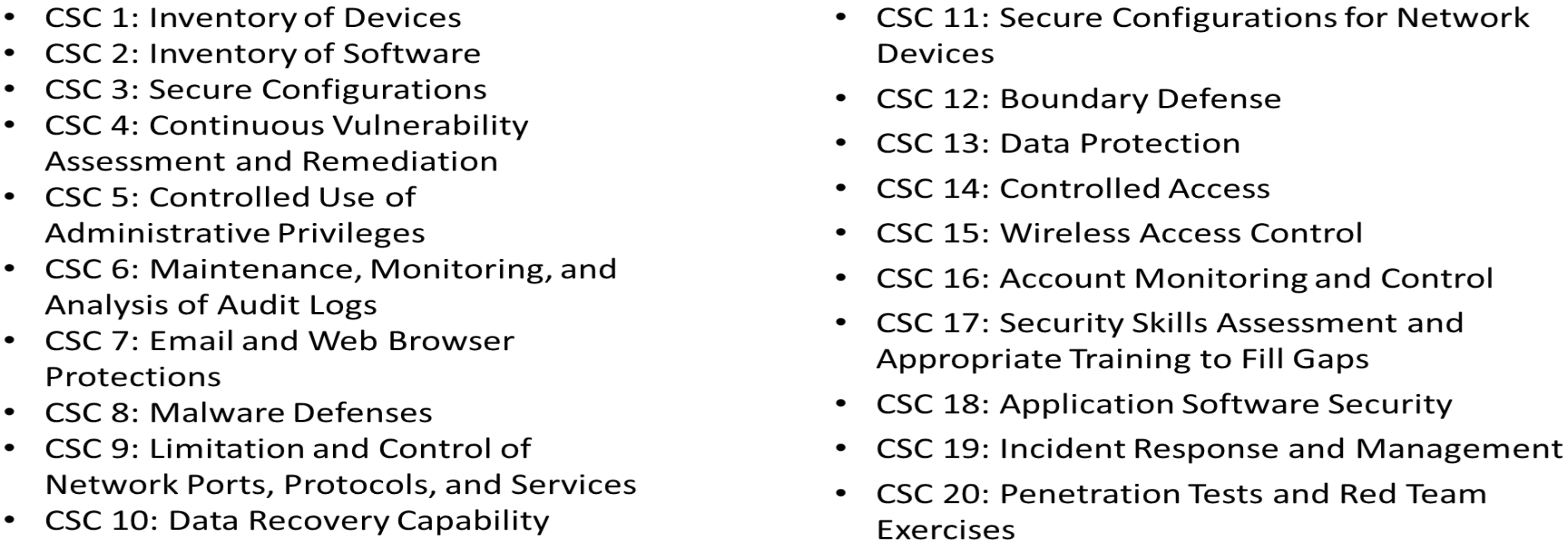
- More than 90% of personal and commercial data breaches result from phishing scams
- National and industry average phishing click rates range from 12%-30% on test campaigns
- September 2016: PacifiCorp implemented a Phishing Awareness and Improvement program
- Average PacifiCorp click rates on test campaigns dropped from 16% in August 2016 to 1.2% in 2017, 0.3% in 2018, 0.1% in 2019, and 0.07% in 2020
  - Training: pre-hire, annual, and following failed test
  - Technical controls: filters, tagging, internet rule
  - Testing: weekly campaigns and targeted spearphishing campaigns
  - Accountability: annual scorecard objective, monthly reporting, progressive discipline processes

Integrated Threats

- Annual vulnerability assessments
  - Integrate physical access, social engineering, and sophisticated cyber attacks
  - Corporate and operational technology networks
  - Unannounced
  - Successfully detected all covert testing, prevented loss of domain administration rights
- Live fire engagements
- Internal exercises

Critical Security Controls

- Center for Internet Security’s Top 20 Critical Security Controls identify industry best practices to improve a company’s cyber security posture
- Focused on technical controls in corporate and operational technology environments



- CSC 1: Inventory of Devices
- CSC 2: Inventory of Software
- CSC 3: Secure Configurations
- CSC 4: Continuous Vulnerability Assessment and Remediation
- CSC 5: Controlled Use of Administrative Privileges
- CSC 6: Maintenance, Monitoring, and Analysis of Audit Logs
- CSC 7: Email and Web Browser Protections
- CSC 8: Malware Defenses
- CSC 9: Limitation and Control of Network Ports, Protocols, and Services
- CSC 10: Data Recovery Capability
- CSC 11: Secure Configurations for Network Devices
- CSC 12: Boundary Defense
- CSC 13: Data Protection
- CSC 14: Controlled Access
- CSC 15: Wireless Access Control
- CSC 16: Account Monitoring and Control
- CSC 17: Security Skills Assessment and Appropriate Training to Fill Gaps
- CSC 18: Application Software Security
- CSC 19: Incident Response and Management
- CSC 20: Penetration Tests and Red Team Exercises

Information Security Management System

- A benchmark framework of policies and procedures together with cyber, physical, and technical controls to manage an organization’s information risks
- Information Security Management System (ISMS) evaluated against 114 specific controls
- Customized to the context of the organization
- Follows the information, not tied to specific systems

Security Projects

- Digital Identity
  - Implement standards-based requirements for digital identity processes and technology
  - Identity proofing
  - Identity authentication
    - Employees and contractors
    - Customers and external parties
  - Identity federation
- Endpoint Detection and Response
  - Prevention, detection, and response
- Insider Threat
  - Investigations
  - Analysis
  - Collaboration with human resources

Cyber Hygiene Monitoring: BitSight

- BitSight cybersecurity ratings
  - Industry benchmarking
  - Similar to consumer credit scores
  - Score range: 250-900
  - Data-driven, objective
- Externally available information about internet-facing systems
  - Highest risk
  - Toe-hold systems
- Leveraged for vendor risk management
- PacifiCorp’s score: 810 = “Excellent”

Business Continuity and Incident Response

- Cyber Security Incident Response Plan
- 2020: Conducted >100 exercises
  - Themes: system restoration, process continuity, contagious disease, CIP-014, ransomware, terrorist activity, and more
  - Formats: plan reviews, tabletop and functional drills
  - Announced and unannounced
- Cross-business and cross-BHE coordination
- NERC GridEx V lessons learned implementation
- Federal and military engagements

Audits and Reporting

- Internal audit of Information Security Management System (ISMS) in Q2 2020
- Ongoing internal audits
  - Security policies incorporated into standard audit scope
- External audit of ISMS during Q3-Q4 2020
- Operational technology vulnerability assessments from Q2-Q4 2020
- CIPS audit scheduled in 2022
- Presentations to state commissions

Berkshire Hathaway Energy