PacifiCorp Security

Prevent - Detect - Respond - Recover

PACIFICORP

PacifiCorp Security

Nancy Lahti

VP, IT and Security

Devon Streed

Director, Security and Business Continuity

PacifiCorp Security

- Physical Security
  - Security Operations Center
  - Incident Response and Investigations
  - Protective Services and Technology
  - CIPS Compliance (CIP-006, CIP-014)

- Cybersecurity
  - Security Operations Center
  - Incident Response and Investigations
  - Managed Security Services Provider (External threat tracking)
  - Security Analysis / Threat Hunting

PacifiCorp Security (cont'd)

- Business Continuity
  - Technology Recovery Plans
  - Business Recovery Plans
  - Exercises (Physical/Cyber, Cascadia, GridEx)
  - Compliance (CIP-008, CIP-009, CIP-014)

- Security Technology and Controls
  - Security Engineering / Technology
  - Security Oversight of Operational Technology (OT)
  - Security Controls and Compliance (CIP-007)
  - IT Support for Renewable Generation Fleet

Phishing

- Over 90% of personal and commercial data breaches nationwide are the result of a phishing scam.
- National and Industry average phishing click rates range from 12%-30% on test campaigns.
- September 2016: PacifiCorp implemented a Phishing Awareness and Improvement program.
- PacifiCorp click rates on test campaigns dropped from 16% in August 2016 to 1.3% YTD in 2017.
  - Training
  - Technical Controls
  - Testing
  - Accountability

Integrated Threat

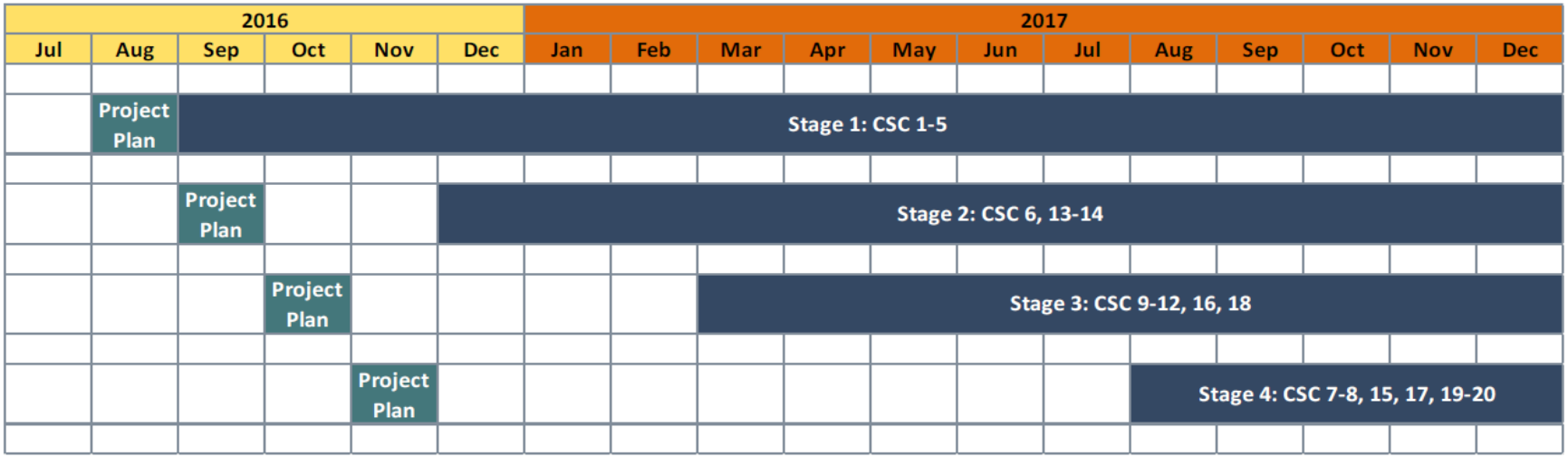
- 2016: An unannounced penetration test by an outside firm was unsuccessful at gaining domain administration rights.
  - The attempt integrated physical access, social engineering, and sophisticated cyber attacks.
  - Testers commented that PacifiCorp's threat detection and response was in the top 10% of government and private entities they've tested.
  - Lessons learned and additional improvements are currently on track for implementation.
- 2017: An audit of PacifiCorp's controls environments had a rating of "above average".
  - During this audit all detection and response measures stood down to allow the audit to proceed.

Training

- All new personnel are required to complete pre-hire security training and all personnel, including contractors and vendors with access, are required to complete annual security training.
- Companywide quarterly security bulletins address a variety of current and relevant security topics.
- Training and bulletin content is updated regularly based on real-world events, new and developing threats, and new defensive tools and capabilities.
- Topics include: physical security, phishing, cybersecurity best practices, process and project requirements for security, information protection, recovery and resilience measures, and available security contacts and resources.

SANS Top 20 Critical Security Controls

- Formalized industry best practices based on data available from public and private threat sources.
- Evaluate existing business cybersecurity practices against the CSCs and close gaps by December 31, 2017.
- Phased approach:



Top 20 CSCs

- 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 and cyber, physical and technical controls to manage an organization's information risk.
- Information Security Management System plus 114 specific controls.
- Customized to the context of the organization.
- 2017 Scope: Residential Customer PII, 1x Thermal Generation Plant, Renewables Fleet, EMS.
- 2018 Scope: Employee PII, Generation Fleet, Third-Party Energy Interfaces