Cybersecurity Discussion
with Utah Public Service Commission

February 23, 2021

Dominion Energy®

Dominion Energy®

Agenda

- Introductions
- Security at Dominion Energy
- Today’s Threat Landscape
- Dominion Energy Cybersecurity Approach
- Dominion Energy Cyber Incident Response

Introductions

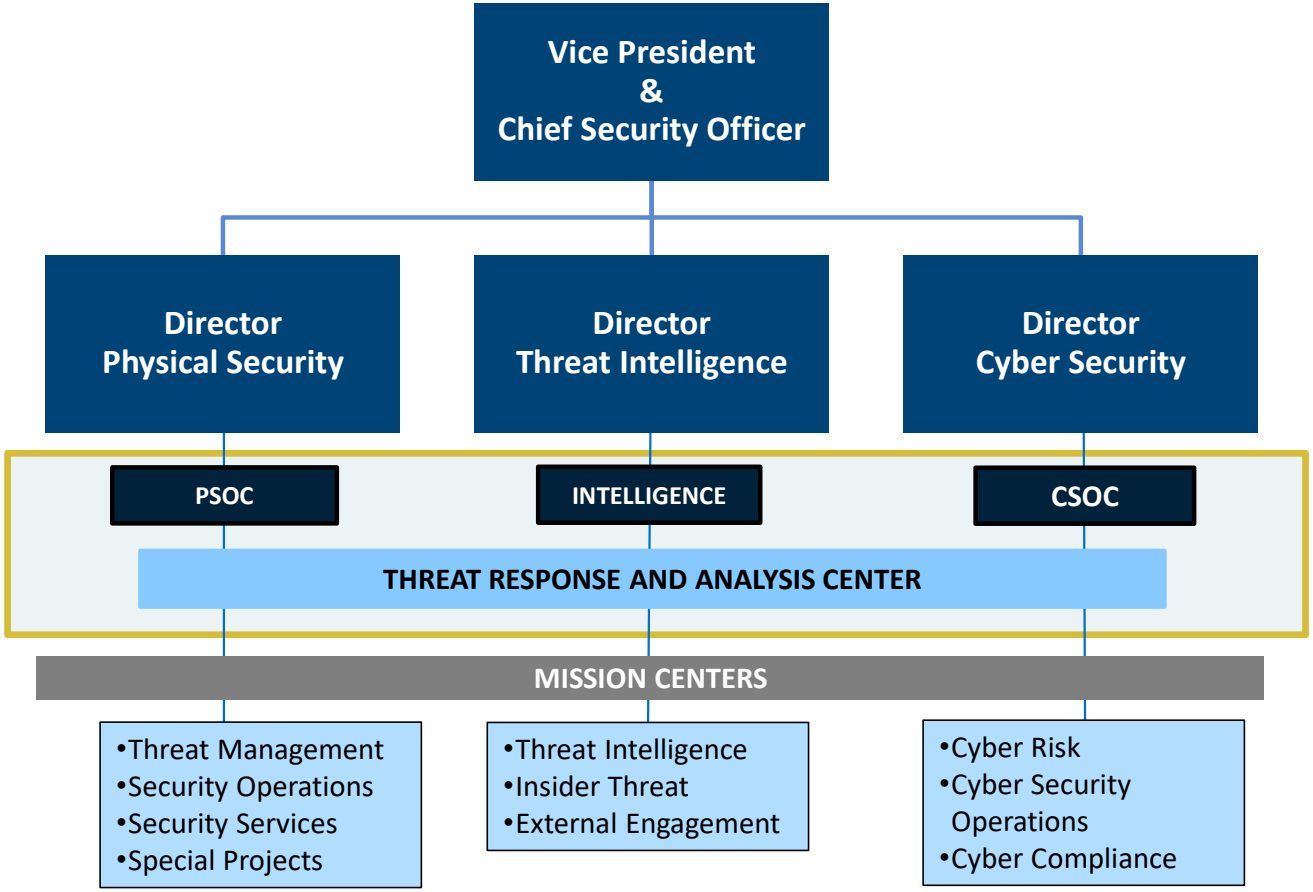
Jonathan Bransky

- Director Threat Intelligence
- Over 23 years in the energy sector and energy sector security
- Oversees threat intelligence and insider threat functions at Dominion Energy
- Dominion Energy industry and government security liaison
- Oil and Natural Gas Subsector Coordinating Council Chair (2021)

Sean Stalzer

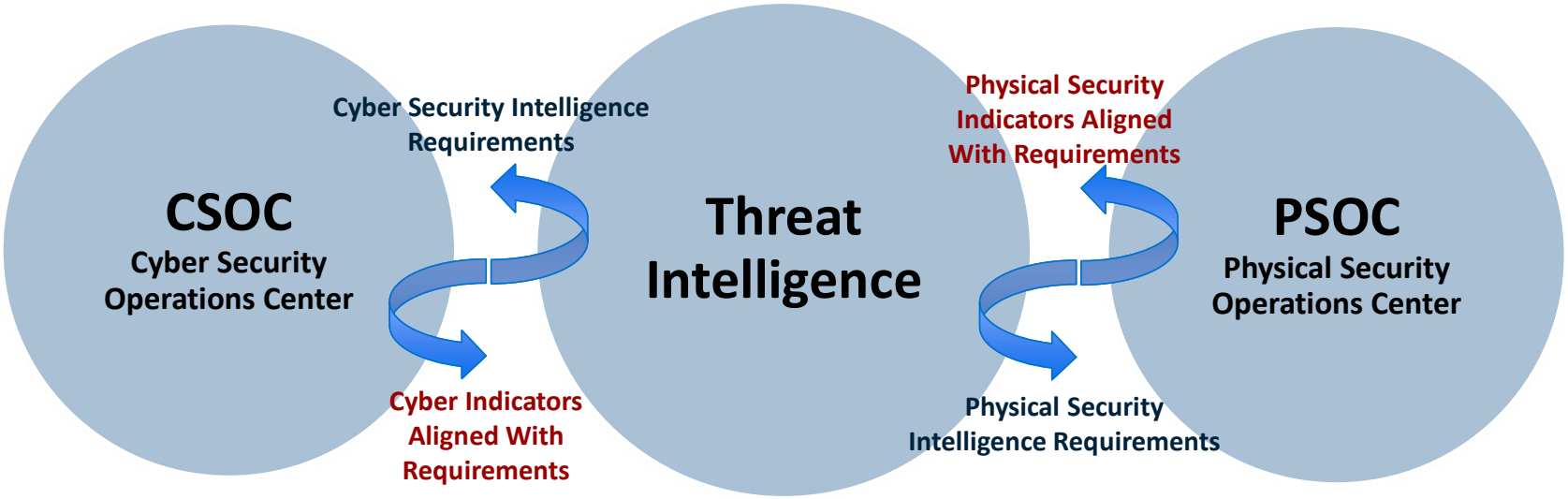
- Director Cyber Security
- Over 25 years at Dominion Energy
- Oversees the Cyber Security program for Dominion Energy across all states within which we operate.
- Includes: Monitoring, Penetration Testing, Vulnerability Testing, Third Party Risk Assessments, Security Awareness Training, Policy Creation, Cyber Regulatory Compliance Program Governance, Phishing Simulations etc..

Dominion Energy
Security Organization



One Security Organization

- Integrate Physical and Cyber Security Operations
- Provide timely threat intelligence



Active Engagement

Industry and Government

- Active in energy industry security communities, both natural gas and electric subsectors
  - American Gas Association Security Committee and Cyber Security Task Force
  - Edison Electric Institute Security and Security & Technology Policy Executive Advisory Committees

- Active engagement on both energy Sector Coordinating Councils and their security efforts
  - Oil and Natural Gas Subsector Coordinating Council
  - Electric Subsector Coordinating Council

- Participate in industry Information Sharing and Analysis Centers (ISACs): Downstream Natural Gas ISAC and Electricity ISAC

- Engage with state fusion and emergency response/preparedness organizations: Includes Utah Public-Private Partnership (UP3), Utah Division of Emergency Management, Utah Department of Public Safety

Active Senior Leader Engagement

Drives Company-wide Security Focus

- Quarterly update meetings with top senior leaders on cyber security, physical security and threat intelligence topics
- Multiple updates each year provided by the Chief Security Officer to the Finance & Risk Oversight Committee of the Board of Directors
- Strategic intelligence assessments provided on security related threats throughout the year
- Weekly threat intelligence briefs detailing industry and newsworthy cyber, physical and operational security threats

Cyber Threat Landscape

Areas of Concern

Ransomware	Double Extortion, Higher Ransom Demands, Impact to Industrial Control Systems (ICS)
Supply Chain	Software/Hardware Compromise, Third-Party Vendors
Advanced Persistent Threats	Common Activities, Targets, Energy Sector Examples
Data Breaches	Business Impacts, Reputational Threat

Cyber Threat Landscape – Ransomware

Double Extortion

- Data exfiltration
- Threat to expose data
- Collect two ransom payments:
  - To restore the network and
  - To recover stolen data

Higher Ransom Demands

- Average ransomware demand increased 100% from 2019 through Q1 2020
- Average ransomware payment rose from
  - $84,116 in 2019 to
  - $234,000 in Q3 2020

Impact to ICS

- In late-2019, Ryuk ransomware targeted Maritime Transportation Security Act (MTSA) regulated facility
- EKANS ransomware targets ICS
- Manufacturing ICS main target

Cyber Threat Landscape – Supply Chain

Software/Hardware Compromise

solarwinds

CCleaner

Third Party Vendors – Business Email Compromise

Figure 1 – Statistics from the FBI's Internet Crime Compliant Center (IC3)[1]

Cyber Threat Landscape – Advanced Persistent Threats (APT)

Activities

- Espionage
- Sabotage
- Crypto-mining
- Denial of service

Tactics

- Phishing
- Watering hole attacks
- Credential harvesting
- Targeting remote workers (VPN)
- Network scanning

Commonly Targeted Industries

- Healthcare
- Government
- Technology
- Research
- Defense
- Energy

Sophisticated Attacks Targeting the Energy Industry

Examples of historical attacks on energy sector targets

- Shamoon (2012)
  - Key victim was Saudi Aramco
  - Wiper virus which overwrote data on 30,000 computers

- Ukraine Power Grid Attacks (2015 & 2016)
  - First (and second) known successful cyber attack on a country's power grid
  - 2015 attack impacted 225,000 customers via the electric distribution system
  - 2016 attack impacted 225,000 customers via electric transmission and used custom created malware CRASHOVERRIDE

- TRITON/Trisis/HatMan (2017)
  - Malware targeted Schneider Electric's Triconex safety instrumented system (SIS)

Cyber Threat Landscape – Data Breaches

Target (2015)

- 41-70 million customers' PII and payment card information was stolen
- $57 million lost in class action lawsuits
- 11% decline in stock price
- $100 million in IT upgrades
- State legislation requiring notification of PII breaches

Office of Personnel Management (2015)

- 21.5 million individuals SSNs stolen
- Background investigation records of current, former, and prospective Federal employees and contractors
- Includes those who applied for security clearances
- Impacted 1.8 million non-applicants, primary spouses or co-habitants of applicants

Equifax (2017)

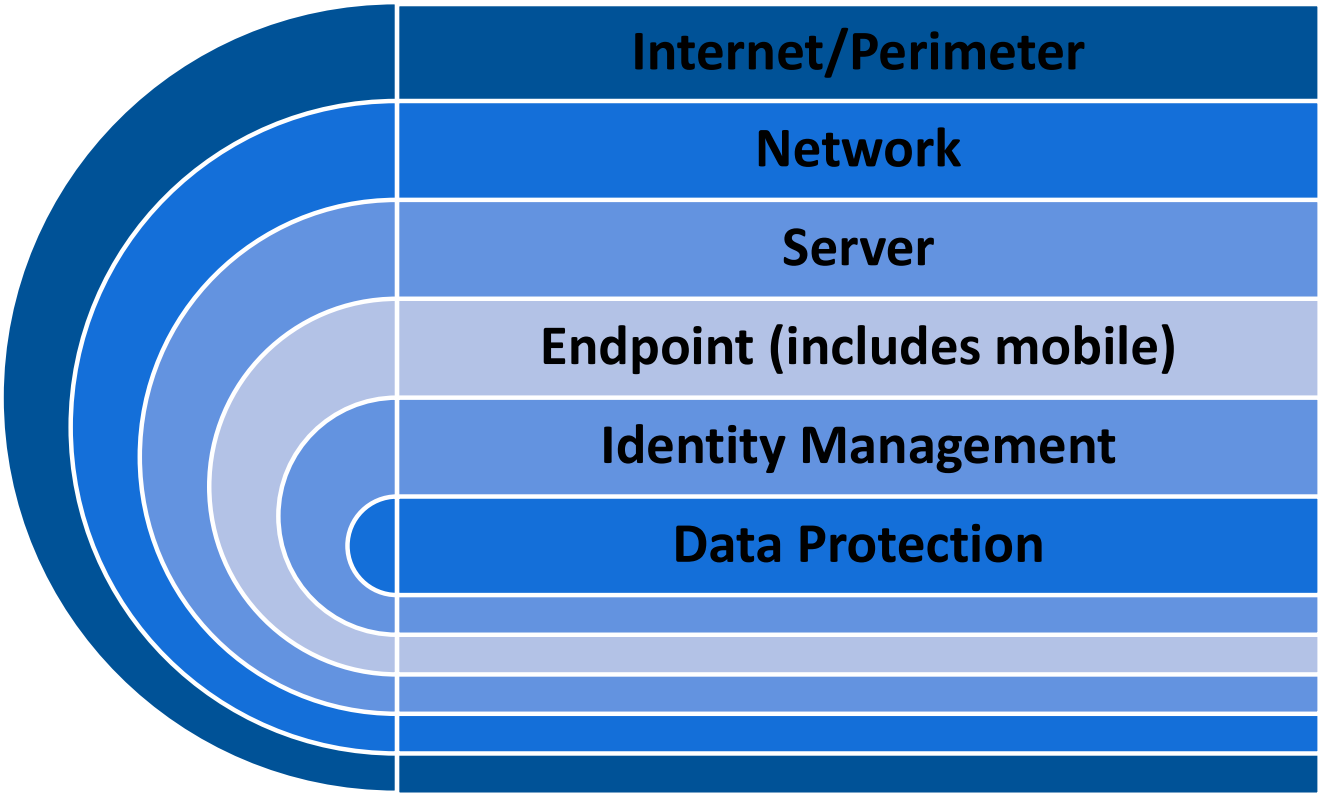
- 143 million customers' PII, payment card information and login credentials
- $26 million fine (2020)
- Various class action lawsuits ongoing

Capitol One (2019)

- 100 million customers' PII and bank information
- $100-150 million in total estimated cost
- 6% decline in stock price
- Chief Information Security Officer demoted

Cybersecurity Approach

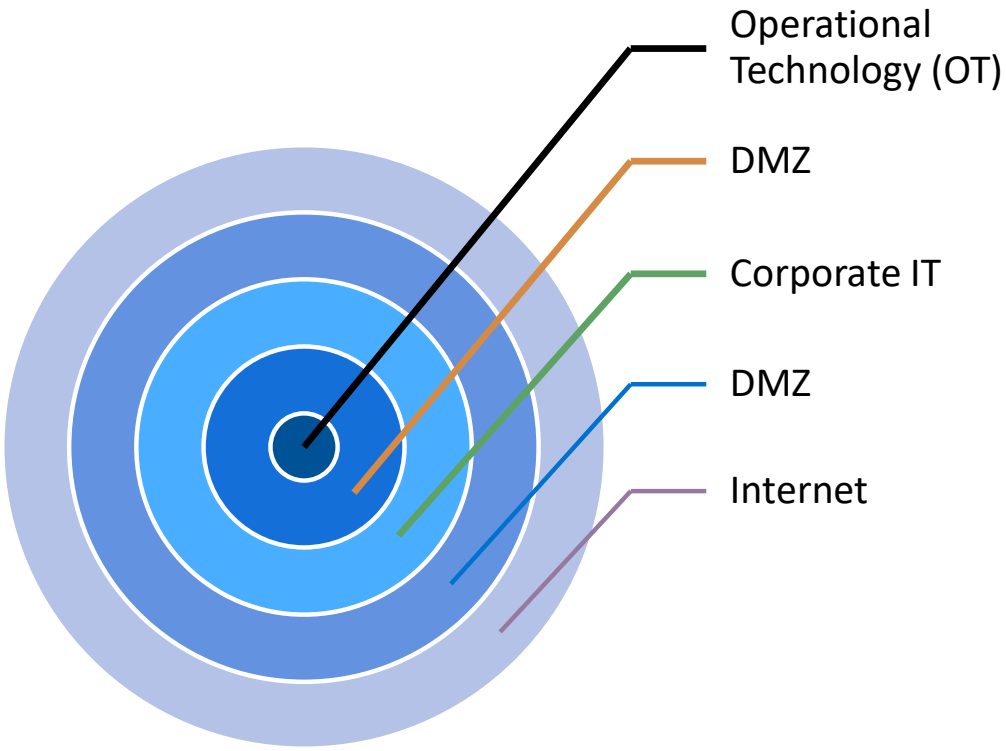
Layers of Protection



Dominion Energy®

Cybersecurity Approach

Secure all zones



Dominion Energy

Cybersecurity Incident Response

- Documented incident response plan covers key stages of an incident
  - Incident Detection, Assessment and Classification
  - Containment, Remediation and Investigation
  - Post Incident Analysis

- The Cybersecurity Incident Response Plan:
  - Details roles and responsibilities
  - Includes key external notifications which may be required
  - Describes external communications coordination
  - Maintains a list of key internal and external contacts

- Cybersecurity Incident Response Plan is reviewed annually;
  Key internal and external contacts are reviewed and updated quarterly

- Tested annually

Cybersecurity Incidents External to Dominion Energy

Evaluate and Adjust Dominion Energy security posture

- Dominion Energy reviews tactics, techniques and procedures used in non-Dominion Energy incidents
  - Conduct What-if analyses
  - Review cybersecurity capabilities to mitigate the approaches used by the threat actors
  - Evaluate residual risk to determine if investment in technology, procedures, or configuration changes are warranted

- Example events analyzed
  - Saudi Aramco
  - Sony Pictures
  - Ukraine 2015 and 2016
  - Monthly FBI bulletins of recent attacks and techniques
  - Anthem
  - Recent DDOS attacks
  - Recent Business Email Compromise schemes

Participate in Industry and Government Exercises and Activities

- Active participant in biannual Grid Ex security incident response exercise
  - Participated in Grid Ex V, November 2019
  - Plan to participate in Grid Ex VI, November 2021
- Observer at December 2020 US Department of Energy Cybersecurity Incident Response Tabletop Exercise
- Though not cybersecurity incident response, Dominion Energy was a planner and player in US Department of Energy Clear Path VIII exercise focused on the Salt Lake City and surrounding areas (Fall 2020)
- Support and participate in industry cyber mutual assistance efforts

Actions Speak Louder