Who We Are

STRENGTH
MORE THAN 7,000 PROFESSIONALS

SAFETY
TOP 5% SAFETY RATING

EXCELLENCE
#10 TOP 500 DESIGN FIRMS

DEPTH
50+ OFFICES WORLDWIDE

COMMITMENT
100% EMPLOYEE-OWNED
Where We Are
Key Industries and Markets We Serve
Company Awards

FORTUNE 100 BEST COMPANIES TO WORK FOR®

ESOP COMPANY OF THE YEAR 2012
ESOP Association

PSMJ's PREMIER AWARD FOR CLIENT SATISFACTION
MISSION STATEMENT

Make Our Clients Successful
CIP & BCSI IN THE CLOUD
INTERACTIVE QUESTIONS
WHO USES CLOUD SERVICES?
WHO KNOWS ABOUT SOC2 REPORTS?

BURNS MCDONNELL
A THOUGHT FOR YOU ...
Of respondents have experienced a software supply chain attack.

66% of all security breaches originate in the supply chain.

50% of enterprises who view their third-party partners as a cybersecurity risk.

80% of all cyber breaches attributed to past supply partners.

45%

Crowdstrike, survey 2018

Help Net Security Survey Results, 2019

Bovens, SCRM@NIST 2016

THE BROKEN LINK: CYBER SECURITY IN THE SUPPLY CHAIN
WHAT IS BES CYBER SYSTEM INFORMATION?
BES CYBER SYSTEM INFORMATION (BCSI)

► Information about the BES Cyber System that could be used to gain unauthorized access or pose a security threat to the BES Cyber System.

► Examples
  • Security Procedures
  • Security Information
    ▪ EACMS
    ▪ PACS
  • Collection of network addresses
  • Network Topology

► Individual pieces of information by themselves do not pose a threat or could not be used to allow unauthorized access to BES Cyber Systems.

► Examples
  • Device Name
  • IP Address without context
  • Policy Statement
  • PSP Name
  • ESP Name
NERC CIP STANDARDS
CIP-011-2 — Cyber Security — Information Protection

**Purpose**
- To prevent unauthorized access to BES Cyber System Information (BCSI) by specifying information protection requirements in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the Bulk Electric System (BES).

<table>
<thead>
<tr>
<th>REQUIREMENT 1: INFORMATION PROTECTION PROGRAM</th>
<th>REQUIREMENT 2: BES CYBER ASSET REUSE &amp; DISPOSAL</th>
</tr>
</thead>
</table>

**Requirements**

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
</table>
| R1 | Each Responsible Entity (RE) shall implement one or more documented information protection program(s).
|   | - R1.1: Method(s) to identify information that meets the definition of BCSI.
|   | - R1.2: Procedure(s) for protecting and securely handling BCSI, including storage, transit, and use. |
| R2 | Each RE shall implement one or more documented process(es) that collectively include BES Cyber Asset Reuse and Disposal.
|   | - R2.1: Prior to the release for reuse of applicable Cyber Assets that contain BCSI (except for reuse within other systems identified in the “Applicable Systems” column), the RE shall take action to prevent the unauthorized retrieval of BCSI from the Cyber Asset data storage media.
|   | - R2.2: Prior to the disposal of applicable Cyber Assets that contain BCSI, the RE shall take action to prevent the unauthorized retrieval of BCSI from the Cyber Asset or destroy the data storage media. |
CIP-011-2 — Cyber Security — Information Protection

► Purpose
  • To prevent unauthorized access to BES Cyber System Information (BCSI) by specifying information protection requirements in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the Bulk Electric System (BES).

R1: INFORMATION PROTECTION PROGRAM

- **IDENTIFY R1.1**
- **PROTECT R1.2**

  - STORAGE
  - TRANSIT
  - IN USE

**REQUIREMENT 2: BES CYBER ASSET REUSE & DISPOSAL**

- **R2.1:** Prior to the release for reuse of applicable Cyber Assets that contain BCSI (except for reuse within other systems identified in the “Applicable Systems” column), the RE shall take action to prevent the unauthorized retrieval of BCSI from the Cyber Asset data storage media.
- **R2.2:** Prior to the disposal of applicable Cyber Assets that contain BCSI, the RE shall take action to prevent the unauthorized retrieval of BCSI from the Cyber Asset or destroy the data storage media.
Purpose

- To prevent unauthorized access to BES Cyber System Information (BCSI) by specifying information protection requirements in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the Bulk Electric System (BES).

R1: INFORMATION PROTECTION PROGRAM

- IDENTIFY
  - R1.1: Method(s) to identify information that meets the definition of BCSI.

- PROTECT
  - R1.2: Procedure(s) for protecting and securely handling BCSI, including storage, transit, and use.

R2: BES CYBER ASSET REUSE & DISPOSAL

- REUSE
  - R2.1: Prior to the release for reuse of applicable Cyber Assets that contain BCSI (except for reuse within other systems identified in the “Applicable Systems” column), the RE shall take action to prevent the unauthorized retrieval of BCSI from the Cyber Asset data storage media.

- DISPOSAL
  - R2.2: Prior to the disposal of applicable Cyber Assets that contain BCSI, the RE shall take action to prevent the unauthorized retrieval of BCSI from the Cyber Asset or destroy the data storage media.
NERC CIP’s Tangled Web

OTHER MITIGATIONS FOR BCSI
OTHER MITIGATIONS FOR BCSI

- **CIP-004-6 R2.1.5**: Training on the handling of BCSI and its storage
- **CIP-004-6 R4.1.3**: Authorize Access to BCSI
- **CIP-004-6 R4.4**: Verify Access to BCSI every 15 calendar months
- **CIP-004-6 R5.3**: For Terminations, Revoke Access to BCSI by the end of the next day
WHAT ABOUT BCSI IN THE CLOUD?
ARE YOU STILL RESPONSIBLE?
Information Protection Program (IPP) must address and identify that BCSI is in the “Cloud”
BCSI IN THE CLOUD MITIGATIONS

R1: INFORMATION PROTECTION PROGRAM

**IDENTIFY**
- R1.1

**PROTECT**
- R1.2

BCSI

PROTECT BCSI IN THE CLOUD THROUGH ENCRYPTION

- STORAGE
- TRANSIT
- IN USE
BCSI IN THE CLOUD MITIGATIONS

R2: BES CYBER ASSET REUSE & DISPOSAL

VENDOR NEEDS TO PROVIDE EVIDENCE BCSI HAS BEEN DESTROYED

REUSE
R2.1

DISPOSAL
R2.2

UNAUTHORIZED RETRIEVAL OF BCSI

UNAUTHORIZED RETRIEVAL OF BCSI
# BCSI IN THE CLOUD MITIGATIONS

<table>
<thead>
<tr>
<th>CIP-004-6 R2.1.5</th>
<th>CIP-004-6 R4.1.3</th>
<th>CIP-004-6 R4.4</th>
<th>CIP-004-6 R5.3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Train Cloud Provider on the handling of BCSI and its storage</td>
<td>Authorize Cloud Provider Personnel with Access to BCSI</td>
<td>Verify Cloud Provider Personnel with Access to BCSI every 15 calendar months</td>
<td>For Terminations of Cloud Provider Personnel, Cloud Provider must Revoke Access to BCSI by the end of the next day</td>
</tr>
</tbody>
</table>
How do you ensure, enforce, and monitor your cloud provider on performance of these mitigations?
SOC 2 CERTIFICATION

- Privacy
  - Access control
  - Two-factor authentication
  - Encryption

- Security
  - Network/application firewalls
  - Two-factor authentication
  - Intrusion detection

- Availability
  - Performance monitoring
  - Disaster recovery
  - Security incident handling

- Confidentiality
  - Encryption
  - Access controls
  - Network/application firewalls

- Processing Integrity
  - Quality assurance
  - Processing monitoring
BCSI IN THE CLOUD

► PERFORMANCE
  • SOC2 REPORT (ATTESTATION)
  • THIRD-PARTY REVIEW
  • RE SPOT CHECK
  • TERMS & CONDITIONS

► ENCRYPTION
  • Business decision: What are the risks for encryption in storage, transit, and in use (memory, applications)?
  • Sufficient strength?
  • Logical key control and authentication
  • Acceptance Testing

► PERSONNEL
  • Systems Administrators and those who have physical access to the data center
  • Will they verify access every 15 months?
  • Revocation challenges
TOTAL COST OF OWNERSHIP
USE CASES OF BCSI IN THE CLOUD
CLOSING REMARKS
TROUBLING STATISTICS

Encryption controls vary widely among cloud providers

- 81.8% Encrypt data in transit
- 9.4% Encrypt data at rest
- 1.1% Customer-managed encryption keys

The cloud is home to sensitive data

- 21% of files uploaded to file-sharing services contain sensitive data
- 34% of users have uploaded sensitive data to a file-sharing service

Of all cyber breaches attributed to past supply partners.

45%

Of all security breaches originate in the supply chain.

80%

• BCSI MITIGATIONS REMAIN THE SAME
• ACCEPTANCE TESTING WHEN USING ENCRYPTION
• SOC2 REPORT IS AN ATTESTATION, STILL NEED TO VERIFY CONTROLS
• UTILIZE TCO AS A FACTOR
• CYBER SECURITY IN THE SUPPLY CHAIN
Questions?

Contact Information:
► Email: jbonventre@burnsmcd.com
► Website: www.burnsmcd.com
CREATE AMAZING.