CYBER SECURITY SUMMIT 2017

Compliance ≠ Security

(But, we're getting closer)

Rich Banta, Co-Owner & CISO, Lifeline Data Centers, LLC

LIFELINE
DATA CENTERS

LIFELINE DATA CENTERS

- FedRAMP-Ready
- HITRUST CSF Certified
- PCI DSS AoC/RoC
- SOC2
- IRS-1075

FedRAMP

HITRUST CSF Certified

AICPA Service Organization Control Reports
AICPA
SOC 2
Formerly SAS 70 Reports

Rich Banta

- CISSP
- CCSP
- CISA
- CRISC
- CFCP
- CDCDP
- CTIA
- CTDC

Compliance ≠ Security

Why does Compliance ≠ Security?

Compliance ≠ Security

Why does Compliance ≠ Security?

- Compliance is Checklist-Based

Compliance ≠ Security

Why does Compliance ≠ Security?

- Compliance is Checklist-Based
- Compliance depends on Audits

Compliance ≠ Security

Why does Compliance ≠ Security?

- Compliance is Checklist-Based
- Compliance depends on Audits
- Audits assess a point in time

Compliance ≠ Security

What efforts are being made to address the point-in-time shortcoming?

Compliance ≠ Security

What efforts are being made to address the point-in-time shortcoming?

- CMP: Continuous Monitoring Program

Compliance ≠ Security

CMP: FedRAMP's approach to Continuous Monitoring

Compliance ≠ Security

The FedRAMP Moderate Baseline contains 326 controls*.

*And an additional ~70 control enhancements

Compliance ≠ Security

The FedRAMP CMP calls for continuous ongoing monitoring and reporting on 58 of the 326 controls.

Compliance ≠ Security

NIST 800-53 R4 Control RA-5:

- Vulnerability Scanning

Compliance ≠ Security

NIST 800-53 R4 Control RA-5:

- Vulnerability Scanning
  - RA-5a: OS/infrastructure/web application/database scans
  - Scan results must be submitted in FedRAMP-specific dashboard format

Compliance ≠ Security

NIST 800-53 R4 Control RA-5:

- Vulnerability Scanning
  - RA-5d: Provide artifacts to ISSO showing high-risk vulnerabilities have been mitigated in 30 days and moderate risk-vulnerabilities within 90 days
  - POA&M

Compliance ≠ Security

NIST 800-53 R4 Control CM-7(1)a:

- Least Functionality
  - Identify and eliminate unnecessary functions, ports, protocols, and/or services
  - PPSM (Ports, Protocols, and Services Management)

Compliance ≠ Security

NIST 800-53 R4 Control CM-8(3)a:

- Information System Component Inventory
  - Automated detection of new assets
  - Reports submitted monthly
  - Vulnerability scan must = Inventory scan = PPSM = NAC, etc.

Compliance ≠ Security

Lifeline has no internal wireless networks.

(This includes the DMZ)

Compliance ≠ Security

This precludes having an IoT, or Internet of Things

Compliance ≠ Security

This precludes having an IoT, or ~~Internet~~ of Things

Idiocy

Compliance ≠ Security

This precludes having an IoT, or Internet of Things

CYBER SECURITY SUMMIT 2017

Compliance ≠ Security

(But, we're getting closer)

CYBER SECURITY SUMMIT 2017

LIFELINE DATA CENTERS

Questions?

Comments?

Rich Banta, Co-Owner & CISO, Lifeline Data Centers, LLC

CYBER SECURITY SUMMIT 2017

LIFELINE DATA CENTERS

Thank you for your time and interest!

Rich Banta, Co-Owner & CISO, Lifeline Data Centers, LLC