LBMC INFORMATION SECURITY

LBMC Information Security Cybersecurity Sense Podcast Show Notes
Author: Bill Dean
Episode: 1
Date: July 28, 2017

The Value of Incident Response Tabletop Exercises

Topic #1

- Most week's we will cover 1-2 information security stories that have an impact on your organization.
- However, in this podcast, I want to discuss a low-cost approach method to determine how well you will respond to computer security incidents similar to those you are reading about in the news, as well as performing incident response tabletop exercises.

Topic #2

- Tabletop exercises are initially performed for compliance reasons, specifically PCI control X.
- We perform these often for AMLAW 50 law firms and top 10 hospital systems.
- Why perform tabletop exercises?
    - Designed to test response without lower stress
    - Does your incident response plan/policy work?
        - How do you know if you don't test it?
    - Identify strengths and weaknesses
    - Make the stressful decisions to be implanted when similar incidents occur
    - Visibility into how encompassing computer security incidents are (IT, executives, legal, HR, PR, service providers, vendors, etc.)
- Designing tabletop exercises:
    - Start with your goals and objectives
    - Be sure correct stakeholders are present
    - Leverage a "neutral" facilitator
    - Answers must be based on current capabilities (no "pixie" dust)

Bill Dean is a Senior Manager at LBMC Information Security. While involved in various aspects of LBMC's security services, he is also the practice lead for the organization's incident response, forensics, and litigation support practice.

References:

Incident Annual testing: https://www.sans.org/reading-room/whitepapers/incident/incident-handling-annual-testing-training-34565

Dept. of Homeland Security - Healthcare TTX: https://www.hsdl.org/?abstract&did=789781

State of Michigan; Utility Industry – H2O SCADA Exercise:
http://www.michigan.gov/documents/deq/deq-wb-wws-SSc3-0_271868_7.pdf

FDIC Community Bank Cyber Challenge:
https://www.fdic.gov/regulations/resources/director/technical/cyber/cyber.html

HITRUST Alliance CyberRx 2.0:
https://hitrustalliance.net/documents/cyber_intel/cyberrx/CyberRX2Playbook_LVLI.pdf