Inspirational Therapy Center (ITC) XXI – 2017 IT Security Case for

Security Posture Assessment and Mitigation of Information System Environment

Written by: Dr. Brandon R. Brown

Background Information

The Inspiration Therapy Center (ITC) is a privately held physical, occupational and speech therapy practice in Los Angeles, CA.

ITC is a regional provider of therapy services with major contracts from national and regional healthcare insurers such as Kaiser Permanente, United Health Group, IEHP, and public insurers such as MediCAL, Medicaid, and Covered California. ITC was formed twelve years ago Ms. Barbara Thompson, a caring and charismatic woman who inspires her staff of twenty therapists, and office workers. The annual revenue of ITC is roughly $2.7 million for FY 2016 and has been expanding comfortably by 5-7% since its inception

Recently, with the explosion of news stories related to ransomware, HIPAA violations by hospitals, and an increase in hacking against small medical facilities, Ms. Thompson decided to initiate a risk management strategy focused on Cyber Security. Her goal is to have a complete audit of the establishments to include its written documentation as well as its current information system security posture. Her ultimate success would be to pass both PCI-DSS 3.2 and HIPAA guidelines via an external audit.

As a first step in this direction. Ms. Thompson wants to ensure that the organization's Information Systems and IT infrastructure are sound, secure, and resilient. She has a firm grasp on day to day operations, and her husband, a former military member has a good grasp on physical security for the facility. The below scope of work is ONLY for address of the infrastructure in question and all matter of items not described below are OUT OF SCOPE for this engagement.

Problem Statement

ITC is pursuing an initiative that will allow it to meet both HIPAA and PCI compliance standards in 2017. This initiative is beneficial in that when ITC is certified compliant, it can expand within the marketplace via current and new contracts with insurers.

To accomplish this goal, ITC must undergo a rigorous pre-audit regimen to include assessment and mitigation of risks associated with its Information Systems and Network Infrastructure. Since this is a "pre-audit", the combination of assessment and mitigation by the same vendor is acceptable as said vendor will not participate in the external audit and certification process.

There will be several deliverables for this engagement to include an executive de-brief / lessons learned session. In this session, the assessment team will outline their audit steps, rationale, findings, and mitigation to said findings.

The final deliverable document will contain proof of all findings, their proposed mitigations, and further proposal(s) for ANY improvements that may be out of scope / budget for this engagement.

Scope of Work:

The Inspirational Therapy Center (ITC) is requesting a comprehensive assessment of its Information Systems and Infrastructure. This will be broken down into three phases.

Phase 1:

An external, blind penetration test against the enterprise's publicly accessible address(s).

Phase 1 will include an external vulnerability assessment with detailed explanations of any findings. Any findings rated as "High" (Equal to or above 7.5 according to the National Vulnerability Database (NVDB)) will be "Run to Ground" and either confirmed through manual penetration testing or deemed as a "False Positive"

Any vulnerability found and exploited will be proven via screenshot or video capture for proof of exploit.

Use of additional tools for assessment, test, and breech are authorized.

*(You can't just find an exploit and say it's bad without "Proving" it is a risk through exploitation and therefore proof that you CAN exploit the vulnerability)

Phase 2:

An internal, blind penetration test against the enterprise's private address space. Same rules apply as with Phase 1.

* (If by now you have not breached the systems. (ALL systems). You may request credentials from Dr. Brown (brbrown@cpp.edu). He will note the request and inform the judging panel.

Phase 3:

Mitigation and Reporting Phase:

> Step 1: Complete your assessment / findings report. Include in it any vulnerability assessment(s)

Step 2: Complete a mitigation report detailing the steps your team took to correct your findings. Please include proof of changes to include a change log and any pertinent roll back information (I.E. include both old and new configuration files for routers, switches, firewalls, web servers etc….)

Step 3: (Optional) Include any improvements that would run “out-of-scope” for this engagement. (For Example, purchase of new equipment, software, resources etc.)

Step 4: Assemble your final presentation, report, and materials for an executive briefing with consultants who will be taking the next step in the audit process.

The consulting board are very busy professionals with multiple clients and will not tolerate a meeting longer than 30 minutes. Therefore, Your Consulting Team will be given 20 minutes to deliver your final presentation. The final 10 minutes will be used for a question and answer session to clarify any gaps. In order for the board to properly understand and evaluate your assessment, it will be very important for the entire oral presentation to be completed within the 20-minute presentation period.

The ITC Network:

- Visio Diagram of ITC environment

Submission of Reports and Presentation Materials

It is the policy of the Inspirational Therapy Center to accept reports and materials in electronic form only (Adobe Acrobat .pdf format with highlighting and notation permissions enabled, Microsoft Power Point, and any simulation in MP4). Your team is responsible for ensuring their proposals are received by ITC by the date and time indicated below. Completed reports shall be emailed to itc2017@calpolymissa.org and any simulation material (I.E. MP4s) will first be zipped and compressed. You will receive a verification e-mail once the documentation is successfully received.

Important Dates

Prospective consulting teams should be aware of the following important dates. Failure to complete submissions or attendance at these dates will result in disqualification from being considered for final ranking:

- **April 21st, 2017 – Proposals in electronic form due to LI by 5:00 P.M. Pacific Time**
- **April 29th, 2017 – Oral Presentation and Interview to LI’s Consultant Selection Committee**

ITC’s consulting board is looking forward to receiving your proposal and attending your oral presentation.