ISE® Southeast Executive Forum and Awards

Nominee Showcase Presentation

The American Cancer Society
Achieving PCI Compliance with an Aggressive Timeline

Shaun Hunt
Vice President, IT Governance

Michelle Stewart
Senior Director, IT Security & Governance

Company Overview

- For 100 years, we have been leading the way to transform cancer from deadly to preventable.
- Helping people stay well, helping people get well, finding cures, fighting back
- About 6,400 employees, nationwide
- In late 2012, the Society becomes a single 501(c)(3) organization
- Corporate Center in Atlanta, GA
- 12 geographic divisions with regional offices
- More than 900 local offices

Presentation/Project Overview

- Planning begins for transformation of Society in 2010
- Focus on streamlining key processes, functions and capabilities
- Society organizational merger completed in late 2012
- IT Department restructured in 2012
- Combined organization had significant gaps in PCI Compliance
- Risk to Society deemed “Very High”
  - Nature of the gaps
  - Failed 2012 PCI on-site audit
- 2013 → “PCI Compliance Or Bust!!”

Overview of Business Challenge

Previous PCI Compliance - questionnaires

Process Discovery & Documentation

- System hardening & patching
- Donations (online)
- Call Centers
- Fundraising Events
- Product
- Partnerships / Outsourced functions

Application Architecture

- Efficient Security
- Reduce Exposure

Network Security

HURRY!!!

Project Scope/Goals

Process

- Standardize processes across Society

Application

- Segment donations from marketing websites
- Tokenize transaction workflows
- CHD redacted from scanned images (archive & ongoing)

Network Security

- Internal firewalls (segmentation & IPS)
- SIEM, DLP, NBA

PCI Compliance

- Successfully pass on-site audit in 2013

Project Results

- Standardized CHD Handling procedures across all divisions and functions
- Standardized system patching and hardening procedures across applications and locations
- Removed most stored CHD from Society
- Dramatically reduced PCI scoped assets
  - From >1000 servers & 1000s of endpoints to < 30 servers and < 200 endpoints
  - Removed some applications from scope entirely
- Centralized security monitoring of PCI environment (SIEM, DLP, NBA)

Focus on our Mission of Saving Lives!

Lessons Learned/Best Practices

DO:

1. Involve many people – increased awareness & improved results
2. Ask the same question 10 different ways
3. Collect/demonstrate proof of application & infrastructure compliance early
4. Compliance Calendar – tracks all ongoing tasks

DON'T:

1. Expect engineers to be PMs
2. RUSH