CliftonLarsonAllen

# Information Security: What Could Go Wrong

May 2016

Investment advisory services are offered through CliftonLarsonAllen Wealth Advisors, LLC, an SEC-registered investment advisor. | ©2016 CliftonLarsonAllen LLP

WEALTH ADVISORY | OUTSOURCING | AUDIT, TAX, AND CONSULTING

# Learning Objectives

At the end of this session, you'll be able to:

- Identify common information security issues
- Describe the pitfalls of not being PCI compliant
- Learn about strategies to safeguard the information technology assets of your local government
- Understand the difference between a vulnerability scan and penetration test

# Overview – Threat landscape

“Information technology and business are becoming inextricably interwoven. I don’t think anybody can talk meaningfully about one without talking about the other.”

-Bill Gates

# Overview – Threat landscape

- Information Security Risks
  - Data loss
  - Data corruption
  - Data leakage
  - Loss of network privacy
  - Loss of network security
  - Loss of computing equipment

- How do we secure systems?

# Definition of a Secure System

"A secure system is one we can depend on to behave as we expect."

Source: "Web Security and Commerce"
by Simson Garfinkel with Gene Spafford

What we expect

- –Confidentiality
- –Integrity
- –Availability

# Illustration – CFO is not immune

- Could access personal email from work computer
- Had local admin access to work computer
- Firewall allowed any outbound traffic
- Active monitoring on internal network not in place
- Loss of data – unknown (possibly PII, PHI)

# Illustration – Is a safe….safe?

- Entity worked with PCI compliant payment processor
- Payments entered into "secure" website
- Indicated no storage of credit card data
- Panic - something from safe went missing
- Data loss – PII, cardholder data

# Illustration – POS hacked

- POS computer was physically accessible to public
- “Open” wireless network used for communication
- Entity self-assessed to PCI compliance
- Data loss – cardholder data

# PCI non-compliance pitfalls

**PCI DSS applies to every entity that stores, processes, or transmits credit card data**

1. Compensation costs
   - “Free” credit monitoring
   - Identity theft insurance
2. Legal action
   - Lawsuits
3. Bank fines
   - Passing along the costs
   - Increased transaction fees

# PCI non-compliance pitfalls

**PCI DSS applies to every entity that stores, processes, or transmits credit card data**

4. Federal audits
   - ➢ Federal Trade Commission
5. Remediation costs
   - ➢ Investigation – PCI forensic audit
   - ➢ Improvements to security
6. Lost revenue
7. Damaged reputation
   - ➢ Bad news travels fast

# 2015 Trustwave Global Security Report

574 data compromises across 15 countries

- 42% of breaches were of e-commerce breaches
- 40% were point-of-sale (POS) breaches
- 28% were a result of weak passwords
- 28% were from weak remote access security
- 49% of investigations involved the theft of personally identifiable information (PII) and cardholder data
- 81% of the victims did not detect the breach

# IT Security Strategy

- *Security is a **BUSINESS** issue, NOT a technical issue!!*
- Users who are more aware and savvy
- Computer systems that are resistant to malware
- Know the network

# Digital Dozen Toward Security

Build and maintain a secure networks and systems

1. Install and maintain a firewall to protect data

- Network diagram
- **Control of inbound and outbound network traffic**
- Local computer firewalls

# Digital Dozen Toward Security

Build and maintain a secure networks and systems

2. Do not use vendor-supplied for defaults for system passwords and other security parameters

  - ➢ http://www.cirt.net/passwords
  - ➢ www.google.com

◊ 2015 Trustwave report indicated that 28% of data breaches resulted from weak passwords

# Digital Dozen Toward Security

## Protect Data

3. Protect stored data

- Data encryption – laptops, flash drives, databases
- Data backup
- **USB ports – controlled**

# Digital Dozen Toward Security

## Protect Data

4. Encrypt data across open, public networks

   - **Wireless network security**
   - Disable SSL and early TLS

# Digital Dozen Toward Security

Maintain a vulnerability management program

5. Protect all systems against malware and regularly update anti-virus software or programs

   - **Not to be modified or disabled by end user**
   - Scheduled periodic scans
   - Alerts of potential malicious activity
   - Logging

# Digital Dozen Toward Security

## Maintain a vulnerability management program

6. Develop and maintain secure systems and applications

- **Process to identify security vulnerabilities**
    - **Microsoft patch Tuesday**
- Software development to include security
- System hardening checklists

# Digital Dozen Toward Security

## Implement strong access control measures

7. Restrict access to data by business need to know
   - **Principle of least privilege**

8. Identify and authenticate access to system components
   - Unique IDs – not shared
   - **Strong passwords**
   - Vendors

# Digital Dozen Toward Security

## Implement strong access control measures

9. Restrict physical access to data

- **Data center access**
- Video surveillance
- Visitor identification
- Vendors
- Filing cabinets

# Digital Dozen Toward Security

Regularly monitor and test networks

10. Track and monitor access to network resources and data

    - **Centralized event logging with alerts**
    - Network authentication
    - Server authentication
    - Remote access

- Trustwave report
    - 86 days: Median length to detection
    - 111 days: Median length from intrusions to containment

# Digital Dozen Toward Security

## Regularly monitor and test networks

11. Regularly test security systems and processes
    - IT audits
    - Vulnerability assessments
    - Penetration tests
    - **Testing to validate effectiveness**

# Vulnerability scan or Penetration test

## Vulnerability scan

A scan that is designed to check for common and known vulnerabilities as well as common misconfigurations over a variety of operating systems.

## Penetration test

A test that will use the same techniques that a black hat hacker would use to penetrate the network. Includes active attempts to exploit potential vulnerabilities and "hack" into systems.

## Internal/External tests

- Internal test is for all systems available on the inside network
- External is for the perimeter network or any system that is accessible from the internet.

# Digital Dozen Toward Security

## Maintain an information security policy

12. Maintain a policy that addresses information security for all personnel

- ➢ Incident response
- ➢ Forensic preparedness
- ➢ Security awareness training
- ➢ **BE PREPARED**

Jim Barton, CISA, PCI-QSA, CCSFP
Manager
Information Security Services
jim.barton@claconnect.com
863-680-5640