# Cybersecurity, Live Hacking demo, and PCI Compliance

## Protecting your organization from cyber threats

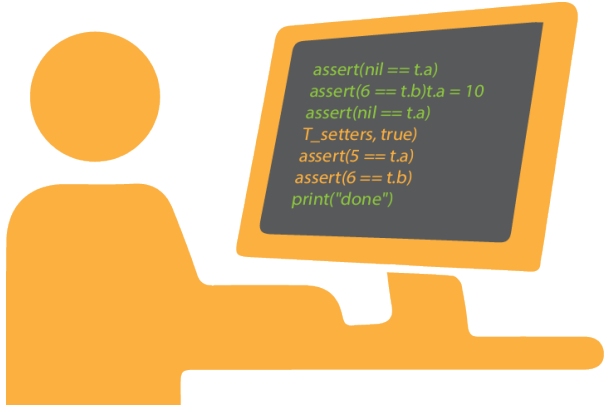
John Bartholomew, Sr. VP of Sales
Security Metrics

TD Bank
America's Most Convenient Bank®

securityMETRICS®

# Today's Hacking

- Malware
  - Stealing Credentials
  - Ransomware
- Remote Access
- X-site scripting (application vulnerabilities)
- Vulnerability exploitation (network services)
- …



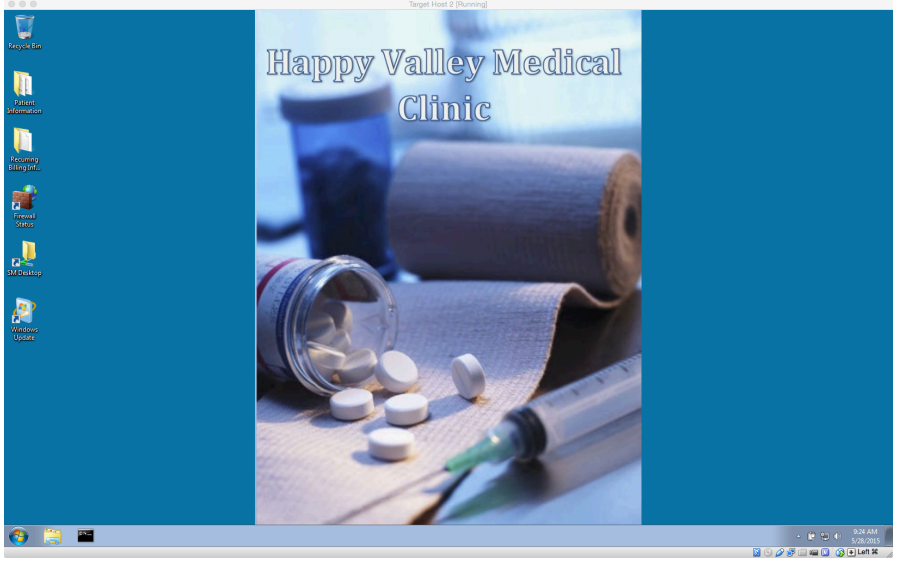
# Insecure Remote Access

- Compromise pathway of today's hackers
- Common applications
  - RDP (port 3389)
  - LogMeIn
  - RemotePC
  - pcAnywhere
  - GoToMyPC
  - VPN

# POS Malware Installation

- Commonly installed through “other” methods (not directly related to POS malware)
- Malware vectors
  - Inside job (USB)
  - Phishing/social engineering
  - Vulnerabilities exploitation
  - Weakly configured remote access

# Today's Hack

# Attack Fundamentals

Scan for port 3389 to identify potential targets


Dictionary/ brute force 3389 on potential targets

Test access (where credentials validated)

Go exploring

Install malware

# PCI DSS

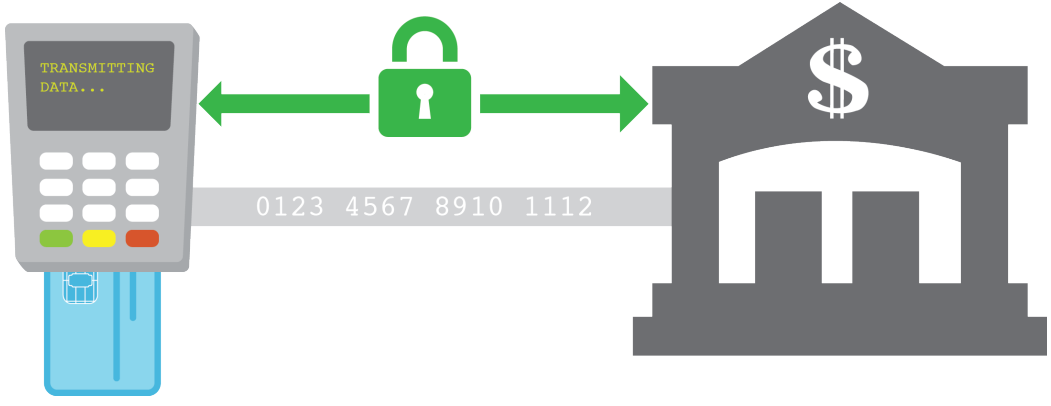
## Examples of Security Helpfulness

- Change Default Credentials (2.1)
- Lock Out Limits (8.1.6)
- Guest Account Removal (2.1)
- Multi-factor Authentication (8.3)
- VA Scanning (11.2)
- File Integrity Monitoring (11.5)
- Anti-virus (5)
- Penetration Testing (11.3)

# PCI DSS

## Secure Simplicity

- P2PE Certified
  (certified encryption solution)



# SecurityMetrics 2017 PCI Guide

http://info.securitymetrics.com/pci-guide

*"Whether it's to answer questions from your merchants, complete your own PCI compliance validation, or keep up with current data breach trends, this guide is a great resource."*

*-Jean Gerritsen, AVP Card Services, NCMIC Group, Inc.*

# Questions?

www.securitymetrics.com