RSAConference2015

San Francisco | April 20-24 | Moscone Center

CHANGE

Challenge today's security thinking

SESSION ID: GRC-F02

# Minimizing the PCI Footprint: Reduce Risk and Simplify Compliance


**Troy Leach**

CTO

PCI Security Standards Council

# Agenda

- Today’s Landscape
- Reducing the Card Holder Data Footprint
- How to Measure the Reduction
- 2015 Goals
- Get Involved

# Agenda

- Today's Landscape
- Reducing the Card Holder Data Footprint
- How to Measure the Reduction
- 2015 Goals
- Get Involved

# Where the Footprint Begins

***66% of data breaches, the organization didn't know the data was on the compromised system***

*VERIZON DATA BREACH INVESTIGATIONS REPORT*

Reducing the cardholder data footprint

More

Efficient security

Less

Complicated for PCI DSS

# *Ways to Reduce Footprint*

***Reduce the need or ability to store or transmit cardholder data***

- Business process
- Outsource
- Simplify
- Render Unreadable

# Approach to PCI DSS Simplicity

| Reduce the attack surface | **Continuous Awareness & Protection** | **Prevent New Types of Exposure** | Measure success and identify opportunity |
|---|---|---|---|

# Approach to PCI DSS Simplicity

Continuous Awareness & Protection

Prevent New Types of Exposure

# Common Misconceptions & Misunderstandings

I am “compliant” therefore I am secure

My data is out of scope because <insert “silver bullet” here>

I know where all my CHD is – it’s in my CDE

My vendors do my compliance for me

# Easier Said Than Done

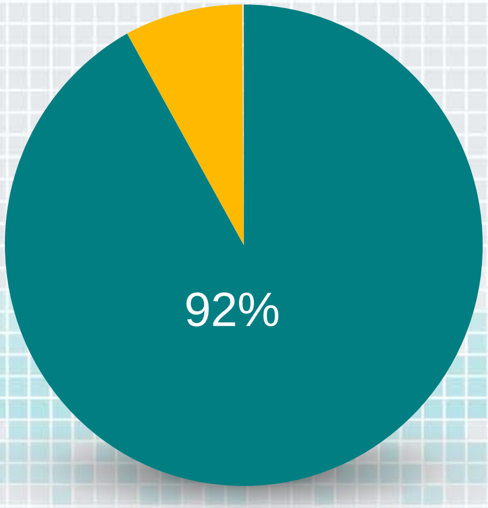
## Why we fail to maintain secure environments

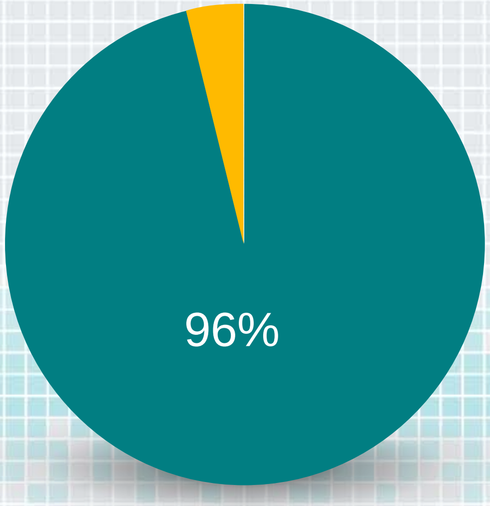
- Lack of awareness by IT practitioners
- Incentive to keep security a primary focus
- Quickly evolving technology landscape
- Rapid development and distribution of new solutions
- Still unnecessary exposure of CHD

# Eliminate the Simple

***92%*** of compromises were simple

***96%*** were avoidable through simple or intermediate controls




*Verizon Business Data Breach Investigations Report*

# Results from a Concentrated Focus on PCI

Concentrated focus on PCI can prevent one mistake leading to mass data compromise

# Reduce the Attack Surface

## Continually Identify the environment

- Maintain a CHD Dataflow Diagram
- Meet regularly with those able to create cardholder data pathways
- DLP Methodology

# Partner with Trusted Experts

- Verify claims of PCI DSS compliance
- Require agreements to maintain skillset
- Verify all third-party access

# Defining and Following Best Practices

## Are you asking the right questions?

- How does the cardholder data flow?
- Where is there storage of data?
- Where is there available connectivity?
- Is all cardholder data classified as such?
- What are our dependencies?
- What features are installed by default?

**Have Clear Asset Identification of Payment Account Data**

# Third Party SIG Guidance

PCI Security Standards Council®

**Standard:** PCI Data Security Standard (PCI DSS)

**Version:** 3.0

**Date:** August 2014

**Author:** Third-Party Security Assurance
Special Interest Group
PCI Security Standards Council

**Information Supplement:**

**Third-Party Security Assurance**

# How Old is Your Business Process?

# You Can't Attack What Isn't There

Confirm there is still need to retain

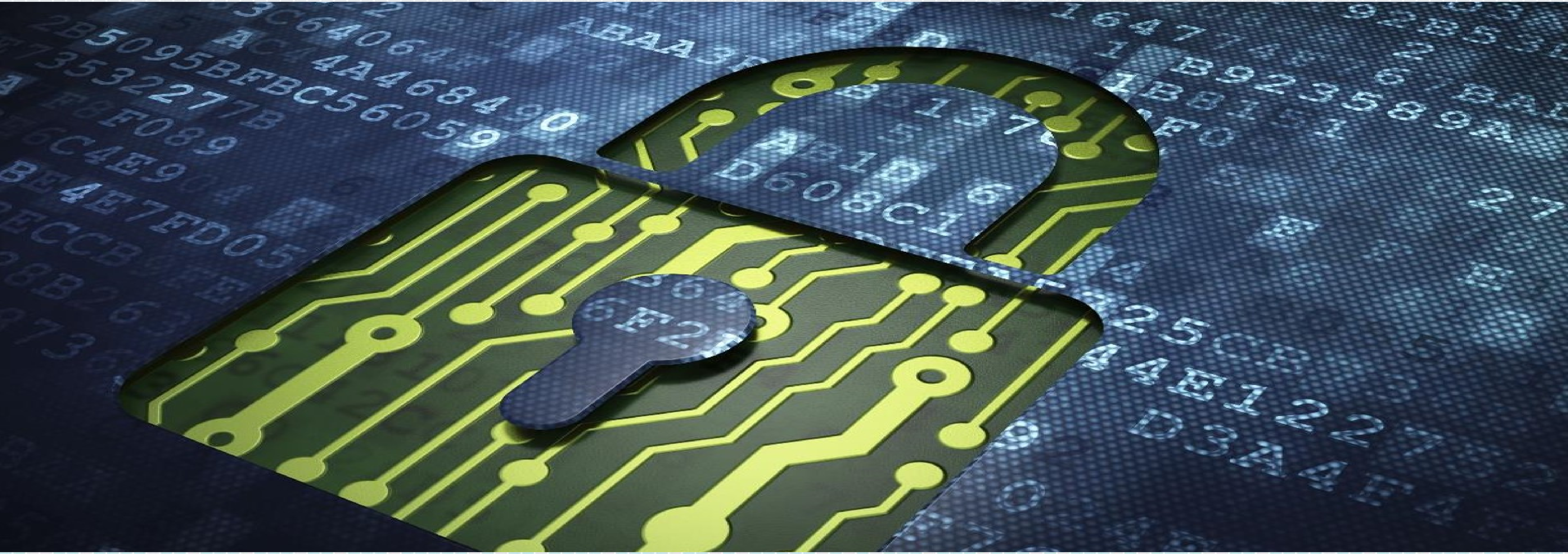
Verify with your financial partners

Evaluate opportunities to use surrogate values to replace PAN

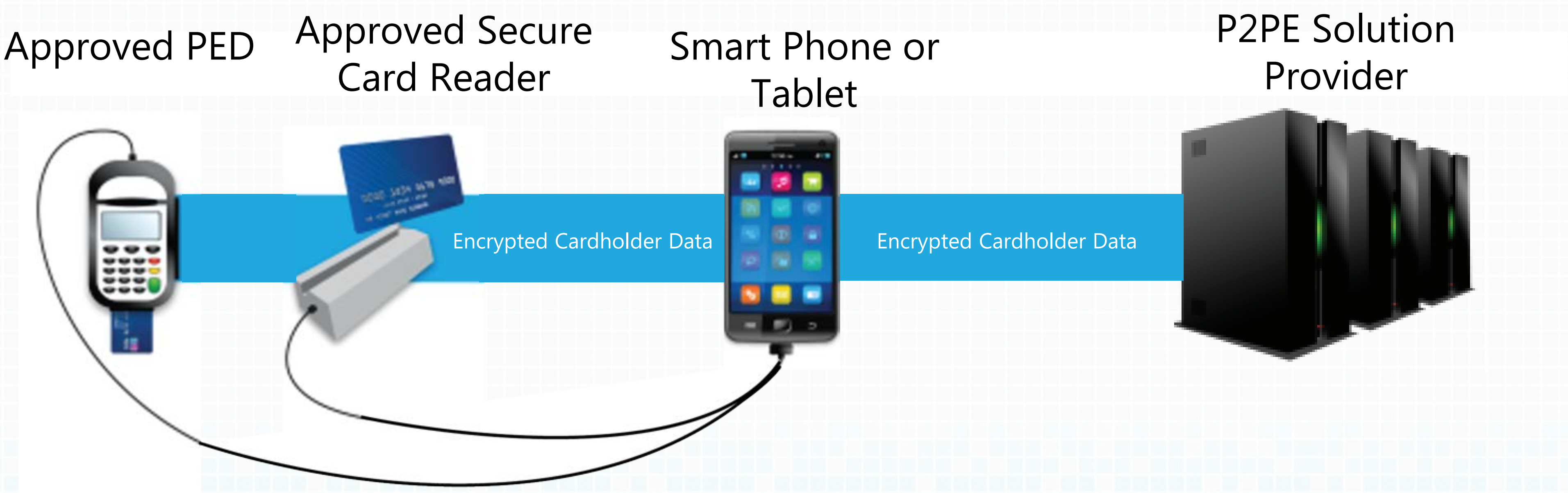
# Don’t Need It Don’t Store It

Is that Account Number worth more than a cheeseburger?

# Render Cardholder Data Unreadable



# Render Cardholder Data Unreadable



# Render Cardholder Data Unreadable

# Agenda

- Today’s Landscape
- Reducing the Card Holder Data Footprint
- How to Measure the Reduction
- 2015 Goals
- Get Involved

# How Do We Measure Success?

# ROSI: It’s a Measurement Problem

Risk is hard to quantify

Data may not be easily available

Growing complexity of technology make metrics also complex

# Goal for Security Metrics

**To move from a culture of fear and uncertainty**

**to a culture of awareness and**

**then a culture of measurement**

*Security Metrics:*
*Removing Fear, Uncertainty and Doubt*
*by Andrew Jacquith*

# Goal for PCI Security Metrics

**To move from uncertainty of where cardholder data is**

**to a culture of awareness and**

**then a culture of measuring improvement**

*Security Metrics:*
*Removing Fear, Uncertainty and Doubt*
*by Andrew Jacquith*

# Bad Metrics

## Unclear

- Inconsistently measured

## Costly

- Does the metric improve cost of investment?

## Unusable

- Incomplete numbers

## Measure Success and Identify Opportunities

# Create Good Metrics

Consistently measured

Reasonable to gather

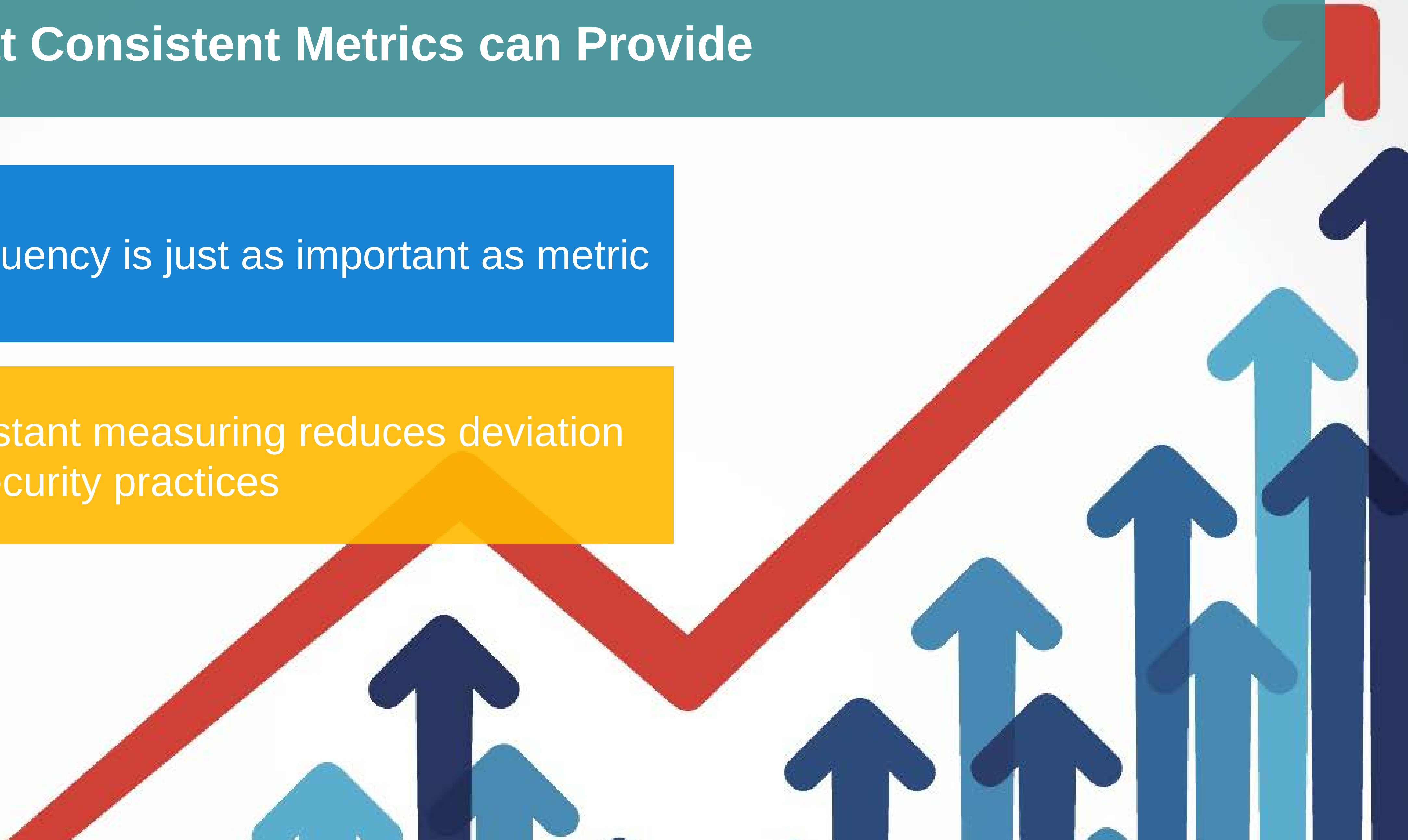
Quantitative

*NIST SP 800-55 – Must be relevant*

# What Consistent Metrics can Provide

Frequency is just as important as metric

Constant measuring reduces deviation in security practices

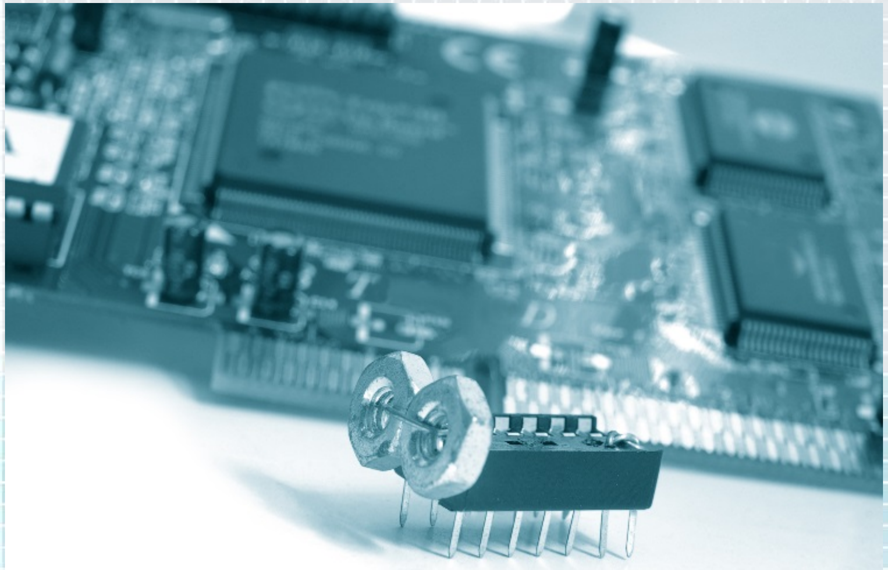


# PCI Security Metrics Should Help Reduce Attack Surface to Cardholder Data

**One of the main goals of building secure systems and applications is to minimize the *Attack surface*…**

The smaller the attack surface,
the more difficult it is for the attacker to leverage a vulnerability into a successful attack

Consider ways to quantify that



# Measure Success and Identify Opportunities

## Examples of PCI metrics

### Req 1

- Number of systems with direct connectivity to CDE
- % of connections to/from unauthorized hosts
- Mean time to complete configuration changes
- Average frequency of firewall review

### Req 2

### Req 3

# Measure Success and Identify Opportunities

## Examples of PCI metrics

### Req 1

- Number of systems with direct connectivity
- Ratio of attacks per e-commerce sessions

### Req 2

- Number of default passwords 6 months after ROC
- % of systems configured to system hardening standards

### Req 3

# Measure Success and Identify Opportunities

## Examples of PCI metrics

Opportunity to sell senior leadership on the idea of tokenization or P2PE by demonstrating numerically how many systems will no longer touch plaint-text CHD

connectivity

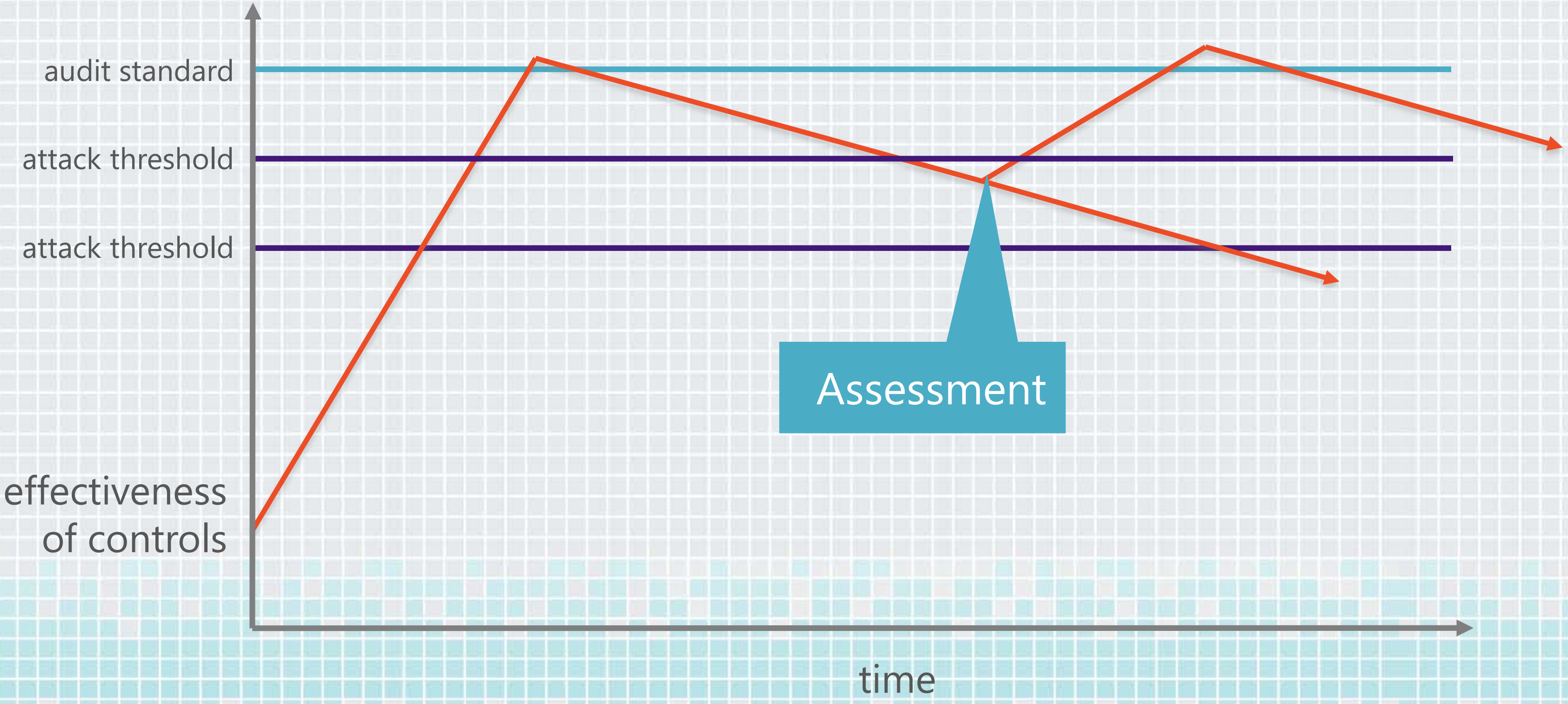
- Ratio of attacks per e-commerce sessions

- Percentage of systems not patched within 30 days

### Req 3

- Percentage of systems containing cardholder data
- Number of business units with access to cardholder data

# Metrics Improve Behavior and Consistency



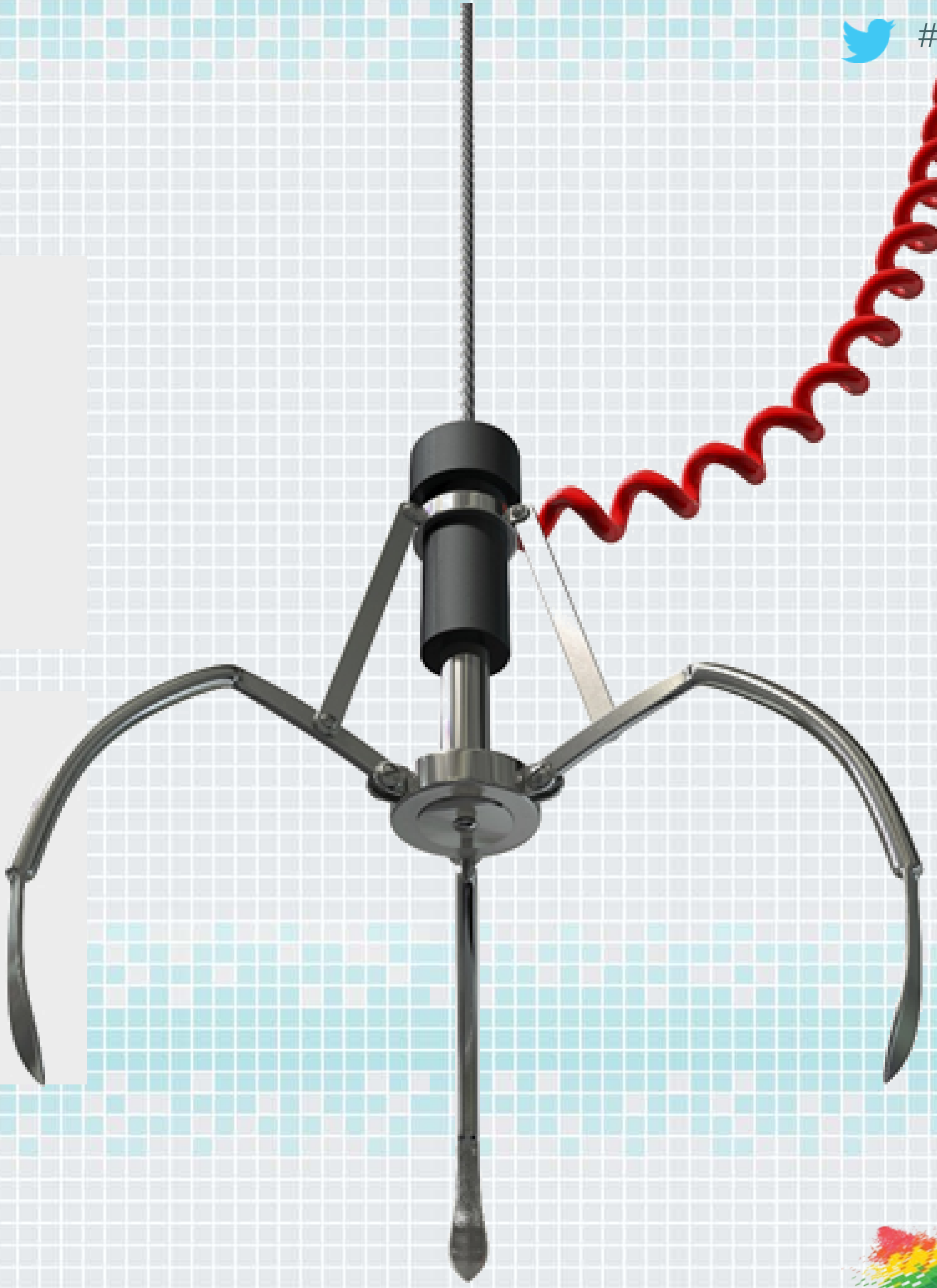
# Metrics are a Tradeoff

The maximal favorable result at minimal cost

# Reasonable Collection Methods

Manual collection is not only costly but higher likelihood of error and difficult to sustain

Automated tools can provide consistency to collection methods



# Tools to Help Collect

## Where to Find Measurement Data?

### *Tools:*

- Source code analyzers
- Dynamic application scanners
- Attack Surface Analyzer
- ASV scan report
- Threat Modeling Tool
- File Fuzzing Tools
- Regex Fuzzer
- Visual Studio Code Analysis

### *Locations:*

- System inventory
- Security vulnerability scans
- Logs
- Report of Compliance
- Other audit reporting
- IT bug tickets
- Incident Response

# Most Importantly:  Relevant

Contextually specific

Are meaningful to the user and relevant to the decision-making process

PCI Security Standards Council®

# Cost Effectiveness

$$CE = \frac{\text{COST}_{\text{new strategy}} - \text{COST}_{\text{current practice}}}{\text{BENEFIT}_{\text{new strategy}} - \text{BENEFIT}_{\text{current practice}}}$$

***CE < 1.0 ⇒ favorable***

# What is your TCO for PAN Retention?

- What is the cost to retain PAN?
- What is the value of retention?
- What is the liability for retention?

# A Single ROC is Simply a Measurement

## Measurement is just one point in time

Metrics compare at least two or more

Value in analytics to compare year-over-year?

Can support trends in progress for securing CHD

# PCI Security Score Per…

## PCI Security Compliance Scorecard

| Department | Identified Lead | Req 1 | Req 2 | Req 3 | Req 4 | Req 5 | Req 6 | Req 7 | Req 8 | Req 9 | Req 10 | Req 11 | Req 12 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Payment Services | Alice | | | | | | | | | | | | |
| Marketing | Bob | | | | | | | | | | | | |
| Sales | Bob | | | | | | | | | | | | |
| Human Resources | Alice | | | | | | | | | | | | |
| Unattended | Alice | | | | | | | | | | | | |

In Compliance | In Progress | Out of Compliance

# PCI Security Score Per…

## PCI Security Compliance Scorecard

| Department | Identified Lead | Req 1 | Req 2 | Req 3 | Req 4 | Req 5 | Req 6 | Req 7 | Req 8 | Req 9 | Req 10 | Req 11 | Req 12 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Payment Services | Alice | | | | | | | | | | | | |
| Marketing | Bob | | | | | | | | | | | | |
| Sales | Bob | | | | | | | | | | | | |
| Human Resources | Alice | | | | | | | | | | | | |
| Unattended | Alice | | | | | | | | | | | | |

In Compliance | In Progress | Out of Compliance

# PCI Security Score Per…

## PCI Security Compliance Scorecard

| Department | Identified Lead | Req 1 | Req 2 | Req 3 | Req 4 | Req 5 | Req 6 | Req 7 | Req 8 | Req 9 | Req 10 | Req 11 | Req 12 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Payment Services | Alice | | | | | | | | | | | | |
| Marketing | Bob | | | | | | | | | | | | |
| Sales | Bob | | | | | | | | | | | | |
| Human Resources | Alice | | | | | | | | | | | | |
| Unattended | Alice | | | | | | | | | | | | |

In Compliance
In Progress
Out of Compliance

# PCI Security Score Per…

## PCI Security Compliance Scorecard

| Department | Identified Lead | Req 1 | Req 2 | Req 3 | Req 4 | Req 5 | Req 6 | Req 7 | Req 8 | Req 9 | Req 10 | Req 11 | Req 12 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Payment Services | Alice | | | | | | | | | | | | |
| Marketing | Bob | | | | | | | | | | | | |
| Sales | Bob | | | | | | | | | | | | |
| Human Resources | Alice | | | | | | | | | | | | |
| Unattended | Alice | | | | | | | | | | | | |

In Compliance | In Progress | Out of Compliance

# PCI Security Score Per…

## PCI Security Compliance Scorecard

| Department | Identified Lead | Req 1 | Req 2 | Req 3 | Req 4 | Req 5 | Req 6 | Req 7 | Req 8 | Req 9 | Req 10 | Req 11 | Req 12 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Payment Services | Alice | | | | | | | | | | | | |
| Marketing | Bob | | | | | | | | | | | | |
| Sales | Bob | | | | | | | | | | | | |
| Human Resources | Alice | | | | | | | | | | | | |
| Unattended | Alice | | | | | | | | | | | | |

In Compliance | In Progress | Out of Compliance

# Communicating Results

## Clear & Concise

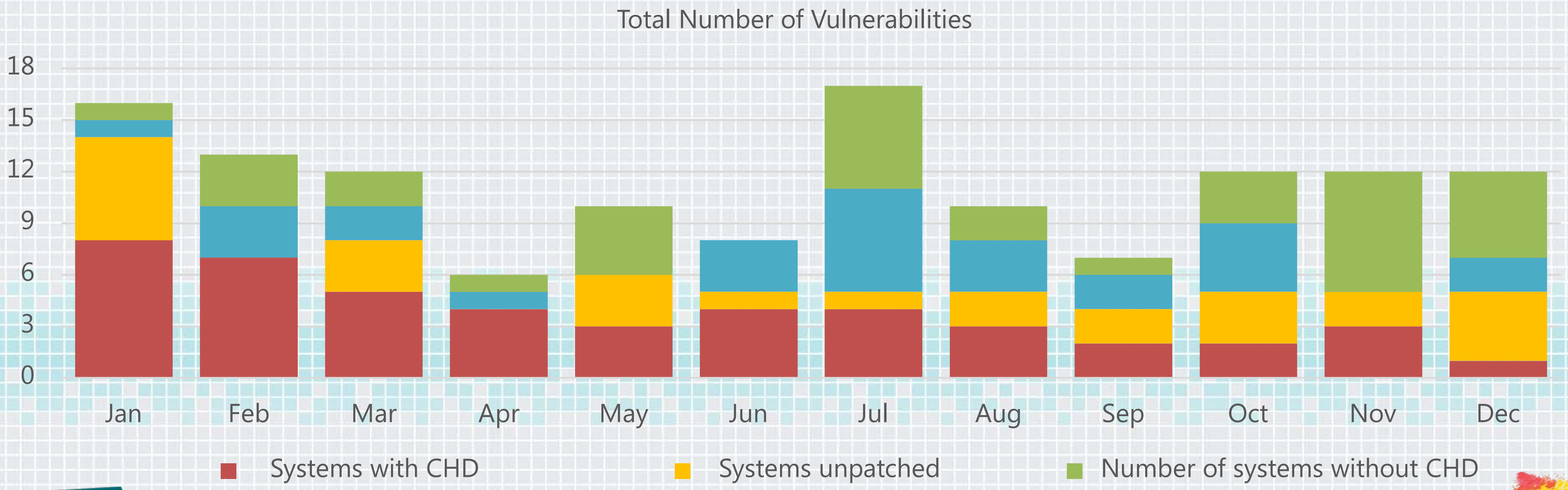
## Context

# Good Rules

Remove clutter

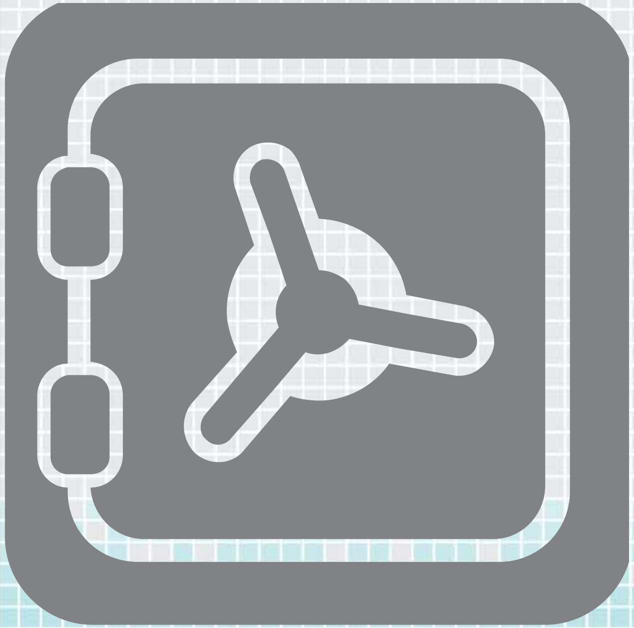
Emphasize one or two points

Put positive spin rather than negative



# Balanced PCI Scorecard

**What are the security versions of the four corners of a balanced scorecard:**



| | |
|---|---|
| Financial<br>*v* Security | Internal business processes<br>*v* Security |
| Learning and growth<br>*v* Security | Customer<br>*v* Security |

# Remember when using metrics

**Only use metrics that will be used to change behavior**

**Find ways to automate relevant metrics**

**Keep It Simple and remember your audience**

***You have to decide what works best for your organization***

# May discover ways to simplify the process

Any exposure of cardholder data beyond acceptance?

Reduce number of departments and individuals with direct access

# Simplify the environment

- ***Remove unnecessary systems***
- ***Use compliant service providers and partners***

# Simplify payment application development

- ***Development team aware of need to protect data***
- ***Lab Validated Applications***


- ***Installation consistently aligns with policy***
- ***Installed to specification by a qualified professional***

## Simplify the implementation

- *Lab Accredited Devices*
- *Aware of skimming attacks*

**Use of trusted devices**

# Agenda

- Today's Landscape
- Reducing the Card Holder Data Footprint
- How to Measure the Reduction
- 2015 Goals
- Get Involved

# 2015 Goals of the
# PCI Security Standards Council


# 2015 Goals – PCI DSS Revision

April 2015

# 2015 Goals – Designated Entities

# 2015 Goals – Token Service Providers (TSP)

# 2015 Goals - P2PE v.2.0 and Tokenization

Point-to-Point Encryption (P2PE)

Tokenization

Best Practices

***Enhanced Security***

# Overview of P2PE v2.0

- Simplified requirements and eliminated redundancy
- Refocused, function-specific domains
- New Domain 4 for merchant-managed solutions
- Simplified merchant PIM requirements
- Consolidated both P2PE standards into one
  - HW/HW and HW/Hybrid
- Increased alignment with PCI PIN standard
- New optional listings for P2PE “Component Providers”

# PCI Listings for P2PE v2.0

## Current P2PE Listings

- P2PE Solutions
- P2PE Applications

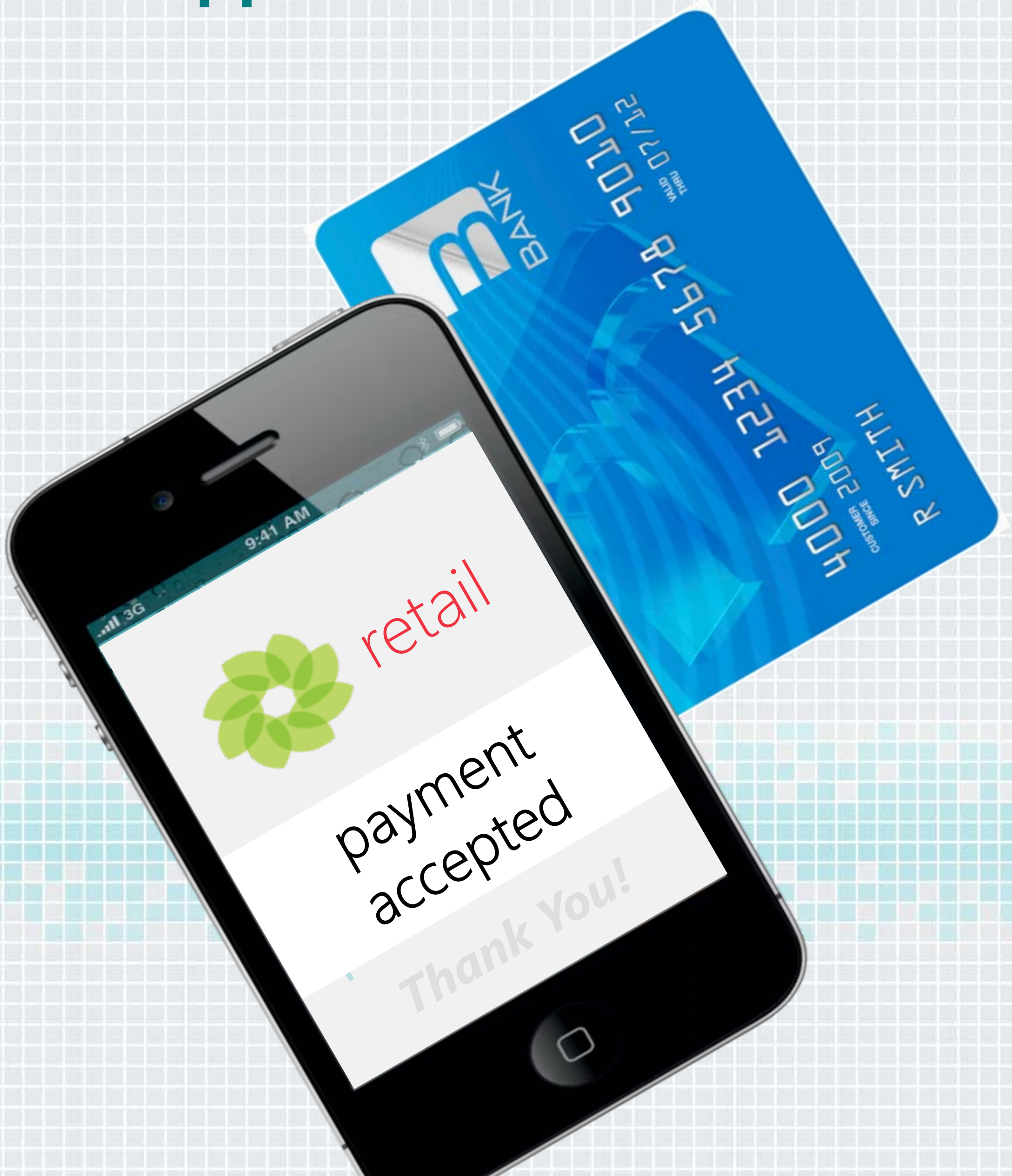
## P2PE v2.0 Listings

- P2PE Solutions
  - Solution assessed to all domains (excluding 4)

    *May use PCI-listed components*
- P2PE Applications (Domain 2)
- P2PE Components
  - Device management component providers (Domain 1 & 6 + Annex A)
  - Decryption management component providers (Domain 5 & 6 + Annex A)
  - KIF component providers (Annex B of Domain 6)
  - CA/RA component providers (Domain 6 + Annex A)

# 2015 Goals - SMB Taskforce

# 2015 Goals - Payment Application



# How to "Apply"

## Educate + Learn = Apply

- Industry Expertise
- Listen
- Examine and revamp your security efforts

# Apply What You Have Learned Today

- Next week you should:
  - Begin to consider how to minimize risk of exposing cardholder data in your environment
- In the first three months following this presentation you should:
  - Define strategies for minimizing your footprint of cardholder data
- Within six months you should:
  - Begin minimizing the security footprint and strengthen your organization
  - Have an approach to measure your effort and communicate effectively the results

**Please visit our website at**
**www.pcisecuritystandards.org**