Top Ten Tips for Securing Your Healthcare Enterprise Beyond HIPAA

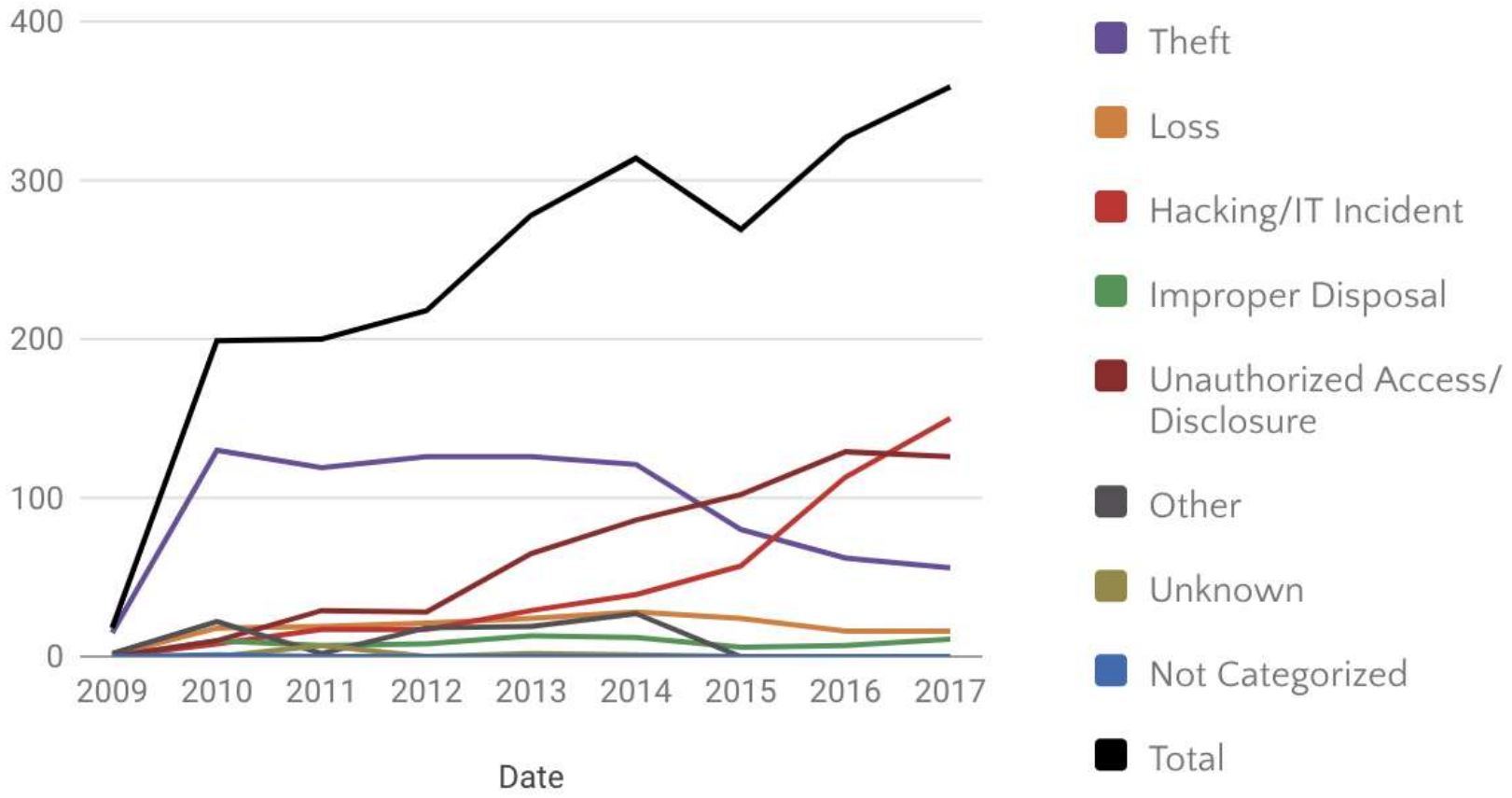
Jon Sternstein (Stern Security) and Noah Dermer (InstaMed)

October 9th, 2018

InstaMed®

Stern Security

Healthcare Breaches by Year



FILTERS APPLIED:

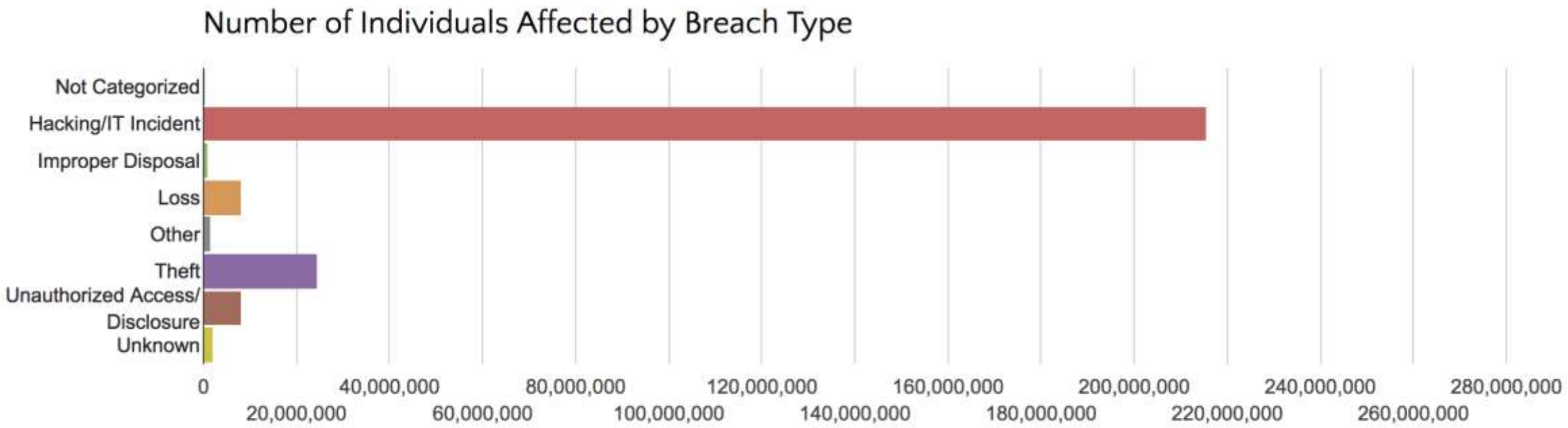
Date: From 2009-10-21 to 2017-12-31

Categories:'Theft','Loss','Hacking/IT Incident','Improper Disposal','Unauthorized Access/Disclosure','Other','Unknown',''

POWERED BY

Stern Security

Healthcarebreaches.com



FILTERS APPLIED:

Date: From 2009-10-21 to 2017-12-31

Categories:'Theft','Loss','Hacking/IT Incident','Improper Disposal','Unauthorized Access/Disclosure','Other','Unknown',''

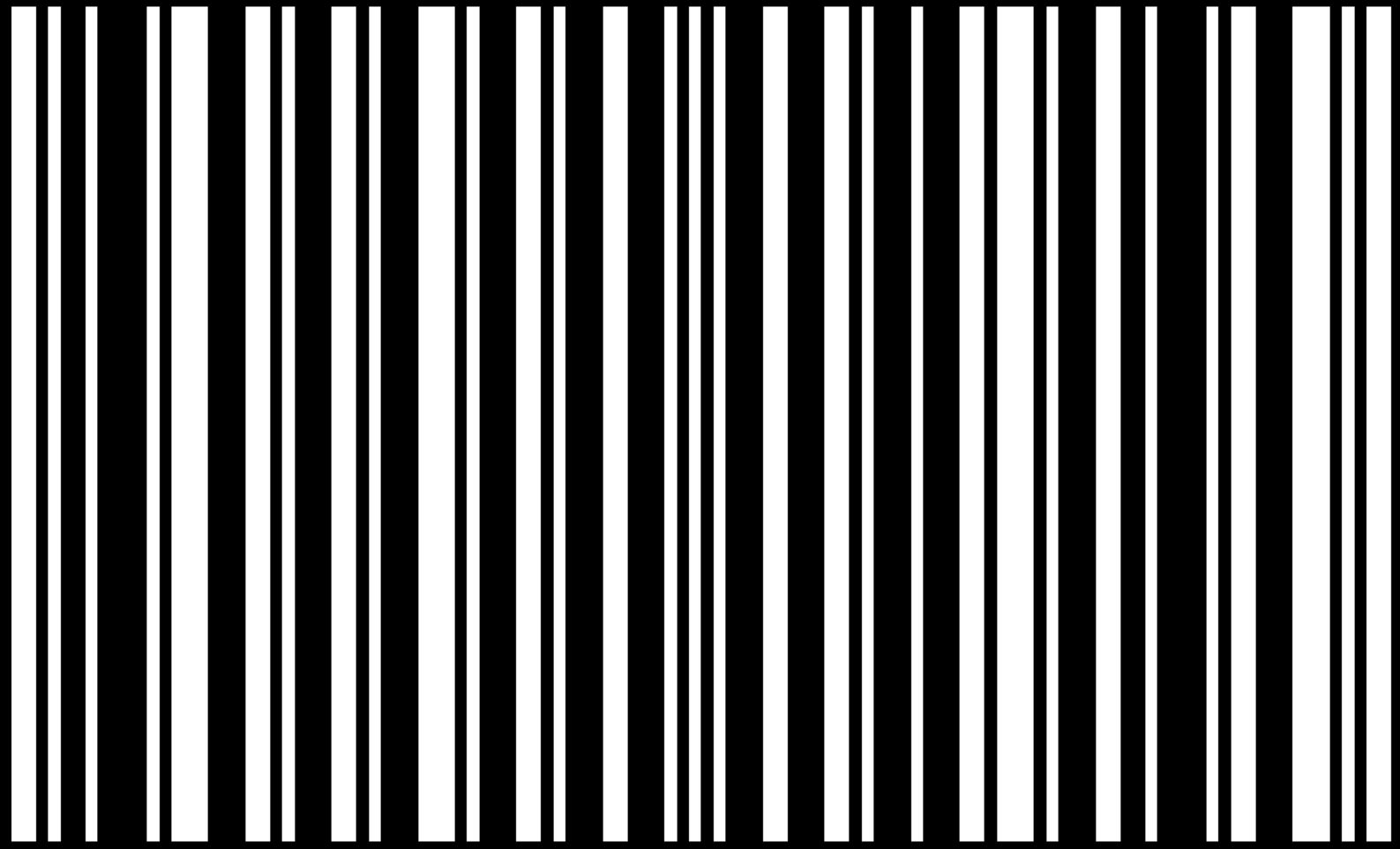
POWERED BY Stern Security

Tip #1

Security Strategy

Stern Security

Tip #2



ASSET INVENTORY

Stern Security

Tip #3

Minimize

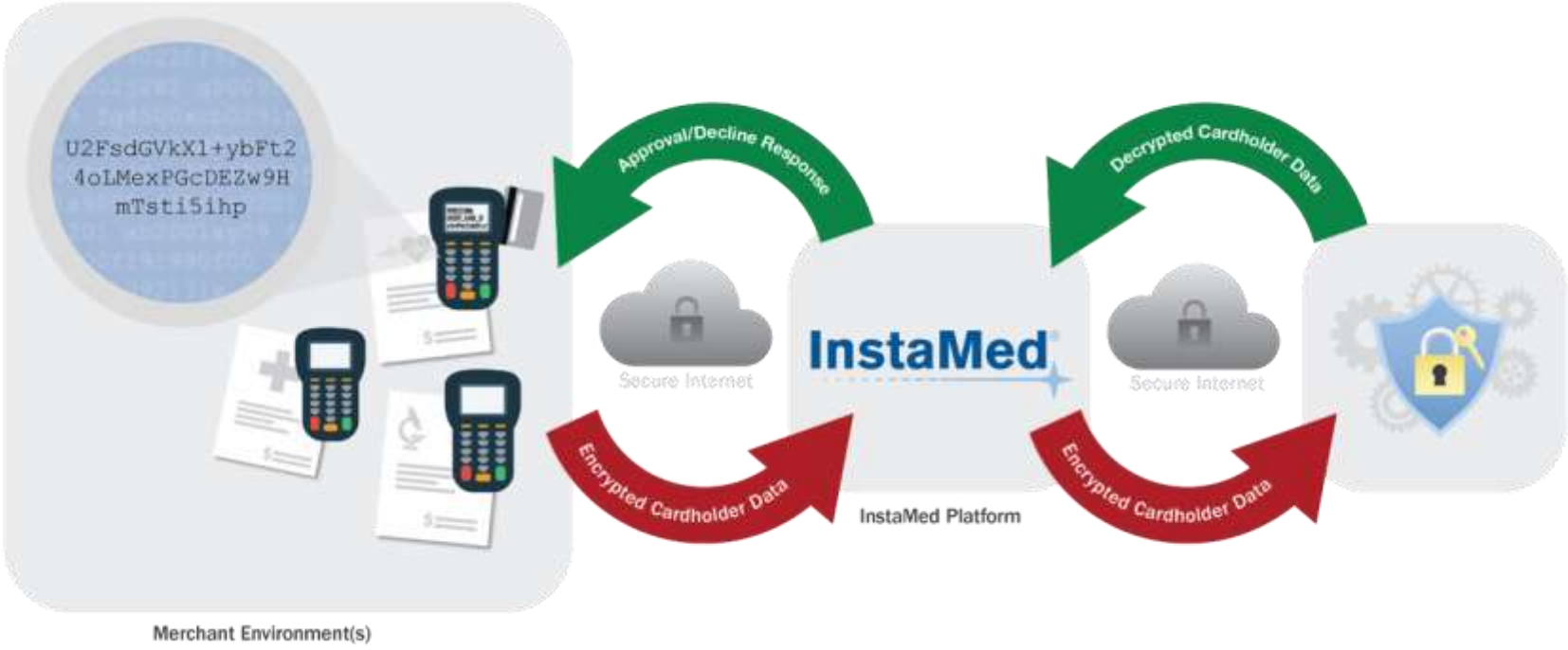
Data

Stern
Security

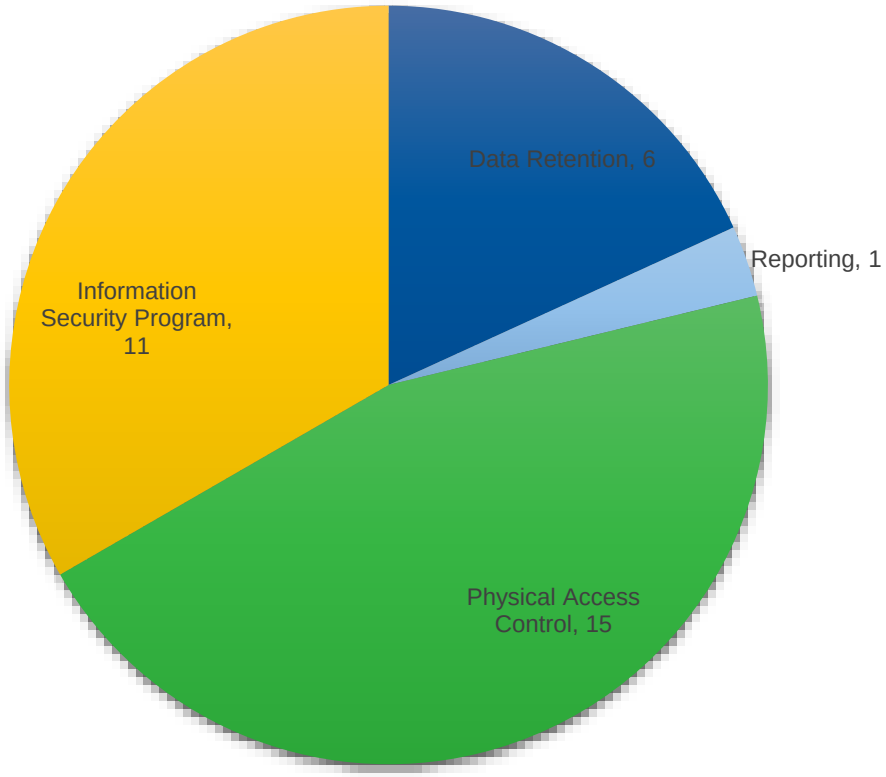
What is P2PE Validated?

Point-to-Point Encryption Validated Solution

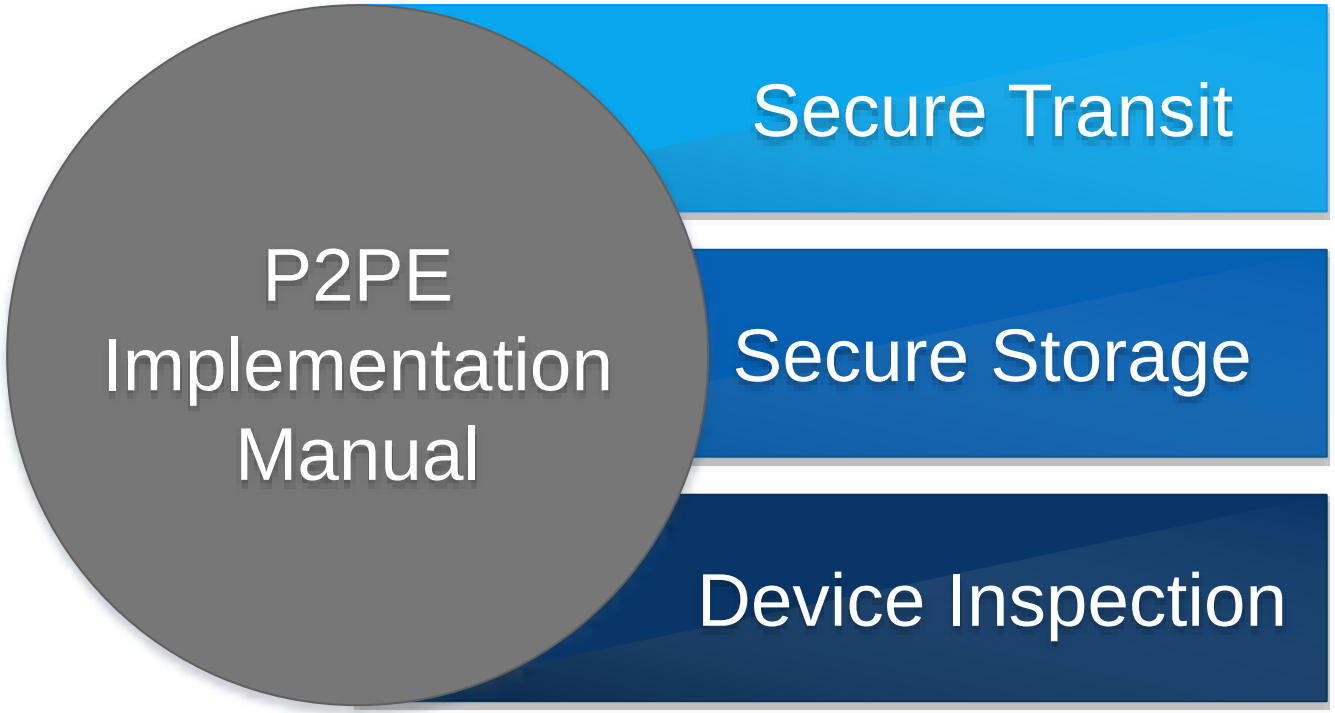
- Encrypt payment information from a device to a secure destination
- Applies to swiped, tapped, inserted and keyed transactions
- Listed o PCI Council Website



P2PE Validated Requirements



P2PE Validated Requirements



Tip #4 - Healthcare Has an Unencrypted Data Problem

Nearly half of all providers **are not encrypting data** in transit

More than half of all healthcare breaches last year were a result of a **failure to encrypt data**

Source: HIMSS, California Data Breach Report

Tip #5 – Vendor Consolidation

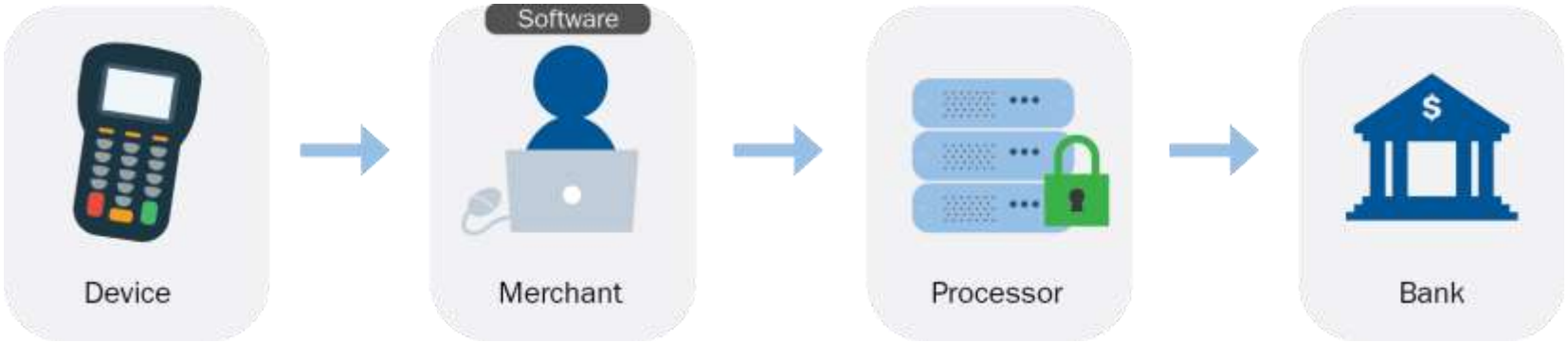
Eliminate Handoffs to Reduce Vulnerabilities

Benefits of Vendor Consolidation

- Eliminate handoffs that put data at risk
- Reduce vulnerabilities in your network
- Have more visibility into the end-to-end processes
- One less vendor to manage

How to Consolidate Vendors

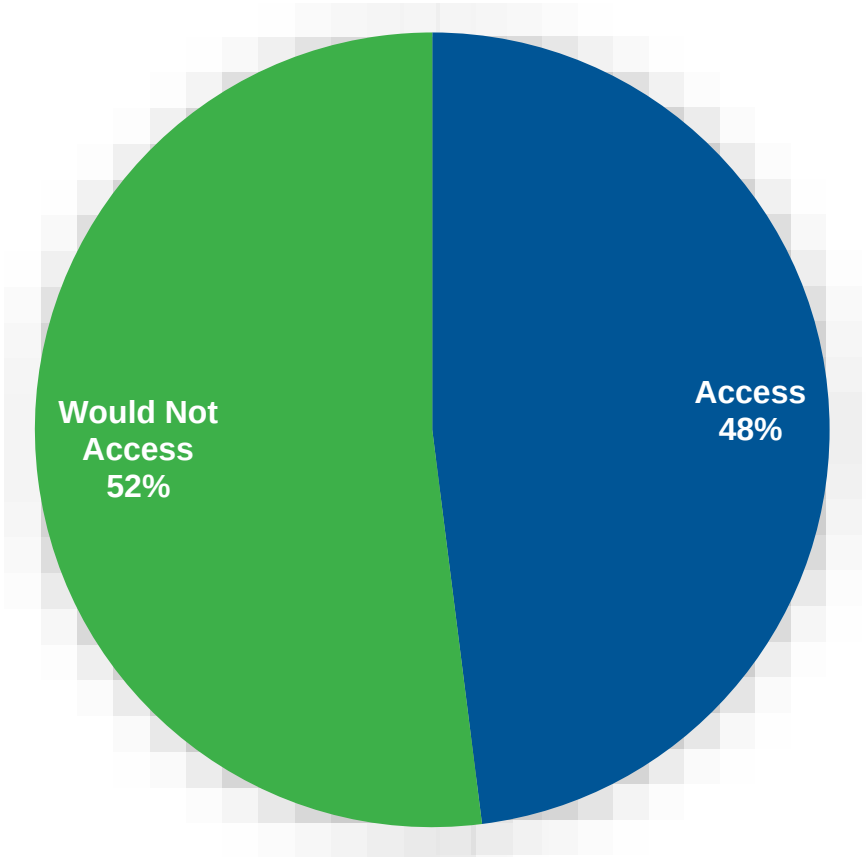
Handoffs Increase Your Security Risks




Tip #6
HIPAA Risk Analysis & Security Testing
Stern Security

Tip #7 – Train Your Staff

Employees Who Would Access Account After Termination?



http://www.sailpoint.com/blog/2016/03/2016-market-pulse-survey-weak-security-practices-leave-organizations-exposed/

Monitoring and Training

Staff has to understand where/how they are susceptible to risks

- Leaving laptops unlocked and unattended
- Saving data on flash drives
- Phishing and social engineering
- Writing sensitive information down on paper and not disposing of it properly

Tip #8 Patch Early, Patch Often

Time to Exploit Vulnerability

Passwords vulnerable after security flaw found

Michael Liedtke and Anick Jesdanun, Associated Press 7:32 a.m. EDT April 9, 2014

f 908 CONNECT TWEET in 31 LINKEDIN 10 COMMENT EMAIL MORE

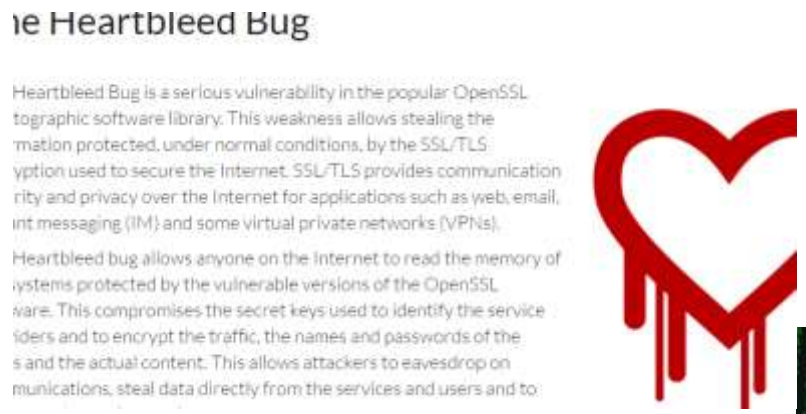
(Photo: Codenomicon)

SAN FRANCISCO (AP) — An alarming lapse in Internet security has exposed millions of passwords, credit card numbers and other sensitive bits of information to potential theft by computer hackers who may have been secretly exploiting the problem before its discovery.

The breakdown revealed this week affects the encryption technology that is supposed to protect online accounts for emails, instant messaging and a wide range of electronic commerce.

Security researchers who uncovered the threat, known as "Heartbleed," are particularly worried about the breach because it went undetected for more than two years.

USA Today – April 9, 2014



ıe Heartbleed Bug

Heartbleed Bug is a serious vulnerability in the popular OpenSSL
tographic software library. This weakness allows stealing the
'mation protected, under normal conditions, by the SSL/TLS
yption used to secure the Internet. SSL/TLS provides communication
rity and privacy over the Internet for applications such as web, email,
int messaging (IM) and some virtual private networks (VPNs).

Heartbleed bug allows anyone on the Internet to read the memory of
ystems protected by the vulnerable versions of the OpenSSL
ware. This compromises the secret keys used to identify the service
iders and to encrypt the traffic, the names and passwords of the
s and the actual content. This allows attackers to eavesdrop on
munications, steal data directly from the services and users and to

Website and Details – April 7, 2014

First Known Exploit – April 8, 2014

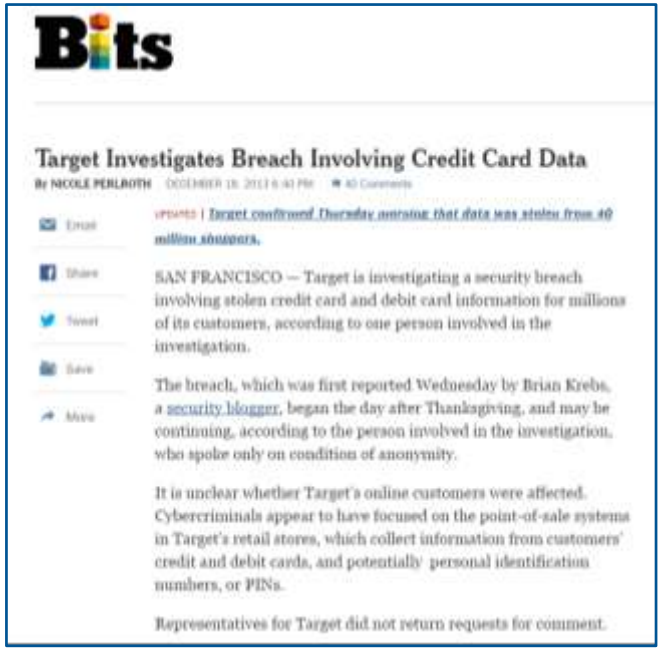

Tip #9
Security is a Goal,
Compliance is a Step
Stern
Security

Compliance vs. Security

PCI Compliant

September 2013 → October 2013 → November 2013 → December 2013

Hacked



Bits

Target Investigates Breach Involving Credit Card Data

By NICOLE PERLROTH DECEMBER 19, 2013 6:40 PM

UPDATED | Target confirmed Thursday morning that data was stolen from 40 million shoppers.

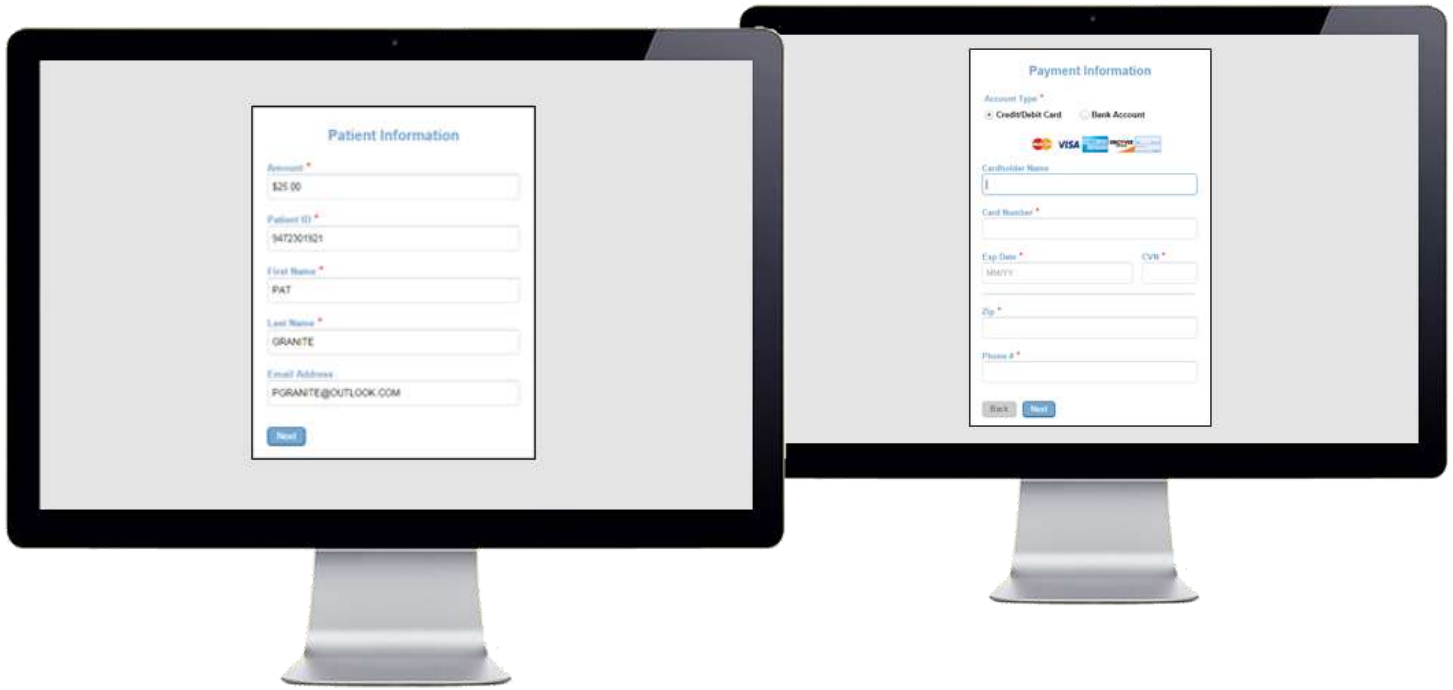
SAN FRANCISCO — Target is investigating a security breach involving stolen credit card and debit card information for millions of its customers, according to one person involved in the investigation.

The breach, which was first reported Wednesday by Brian Krebs, a security blogger, began the day after Thanksgiving, and may be continuing, according to the person involved in the investigation, who spoke only on condition of anonymity.

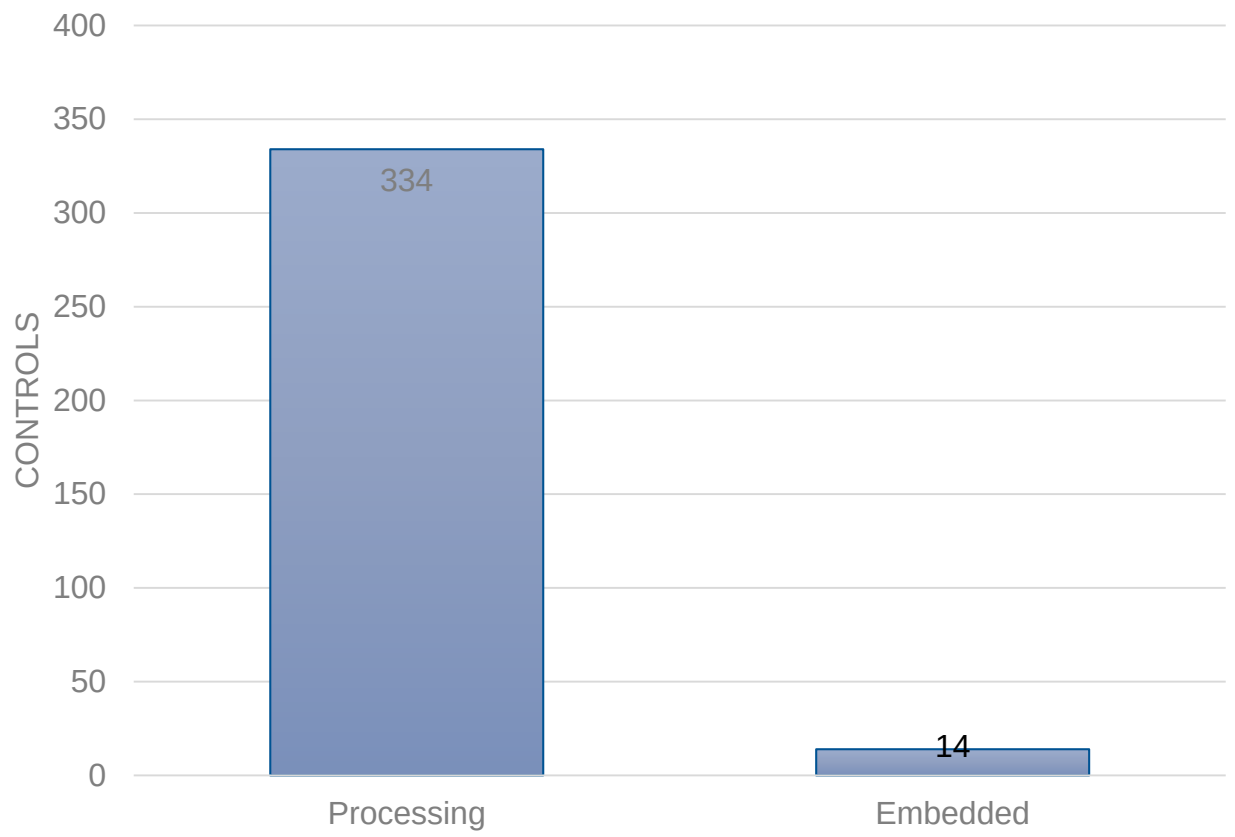
It is unclear whether Target's online customers were affected. Cybercriminals appear to have focused on the point-of-sale systems in Target's retail stores, which collect information from customers' credit and debit cards, and potentially personal identification numbers, or PINs.

Representatives for Target did not return requests for comment.

Payment Processing — Website

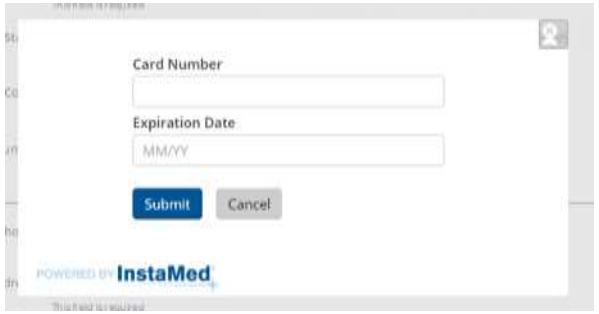


Processing vs. Secure Token



Secure Token

Consumer logs into portal and clicks Pay Now.



Consumer enters payment info into InstaMed embedded screen.

InstaMed creates 2 “tokens”

1. **Used to process payment**
2. **Used to enable digital wallet for future payments**


Tip #10
Join NCHICA
Stern
Security