RSA CONFERENCE 2014
FEBRUARY 24 – 28 | MOSCONE CENTER | SAN FRANCISCO

Share.
Learn.
Secure.
Capitalizing on
Collective Intelligence

Achieving and Exceeding Compliance Through Open Source Solutions

SESSION ID: GRC-T09

Zack Fasel
Managing Partner
Urbane Security
@zfasel

Erin Jacobs
Managing Partner
Urbane Security
@SecBarbie

Urbane SECURITY

PCI - DSS

RED FLAG

GLBA

COBIT

FISMA

HIPAA

SOX

Did somebody say compliance?

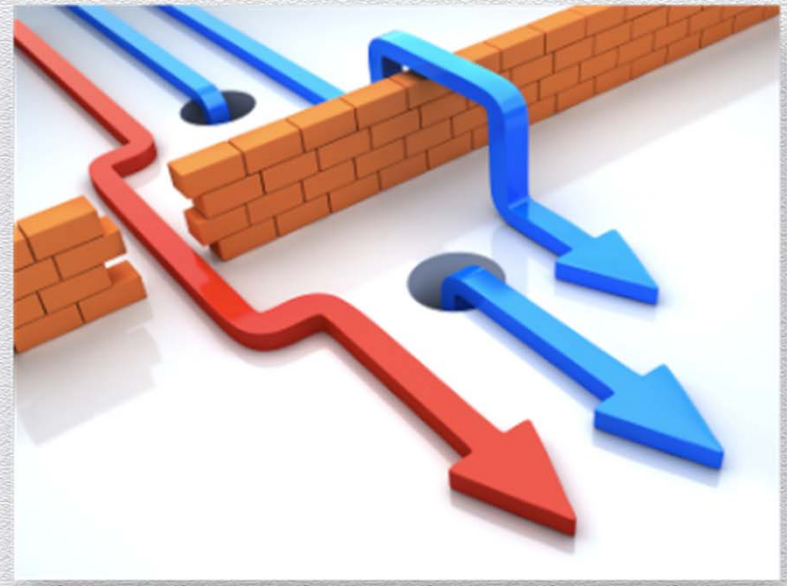
NERC/CIP

ISO/IEC 27002

COSO

HITRUST

Urbane SECURITY



…. But what about security?

It’s not getting fixed or even significantly better

- Weak or stolen credentials account for 76% of network intrusions, and over 50% use some form of hacking.

Source: Verizon 2013 Data Breach Investigations

- The average cost of a single, successful cyber-attack is $300K, and companies are attacked an average of 2 million times per week.

Source: IBM X-Force Trend and Risk Report

- 66% of breaches analyzed in 2013 took months to years to discover

Source: Verizon 2013 Data Breach Investigations

Stick around, this is going to be fun!

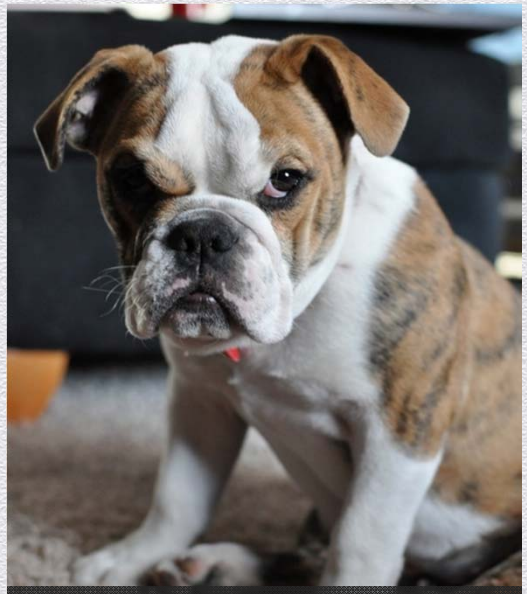
- Focusing on PCI-DSS as a starting model, but are present in multiple compliance requirements and controls
- Open Source vs. Free vs. Commercial Solutions
- Most common security control deficiencies that can be addressed
- Leveraging these controls to actually improve overall security (yay)
- Compliance strategies and ‘quick wins’
- Questions & Answers, beyond just this talk
- Technical and actionable recommendations

THE PCI DISCLAIMER:

While we're a QSAC/QSAs, we're not YOUR QSA.

Your mileage may vary based upon numerous factors, including environment, resources, controls, and QSA's intelligence level.

The following information is based on our professional opinions and guidance. We make no claim that it is directly or indirectly endorsed by the PCI SSC or any other QSAs.



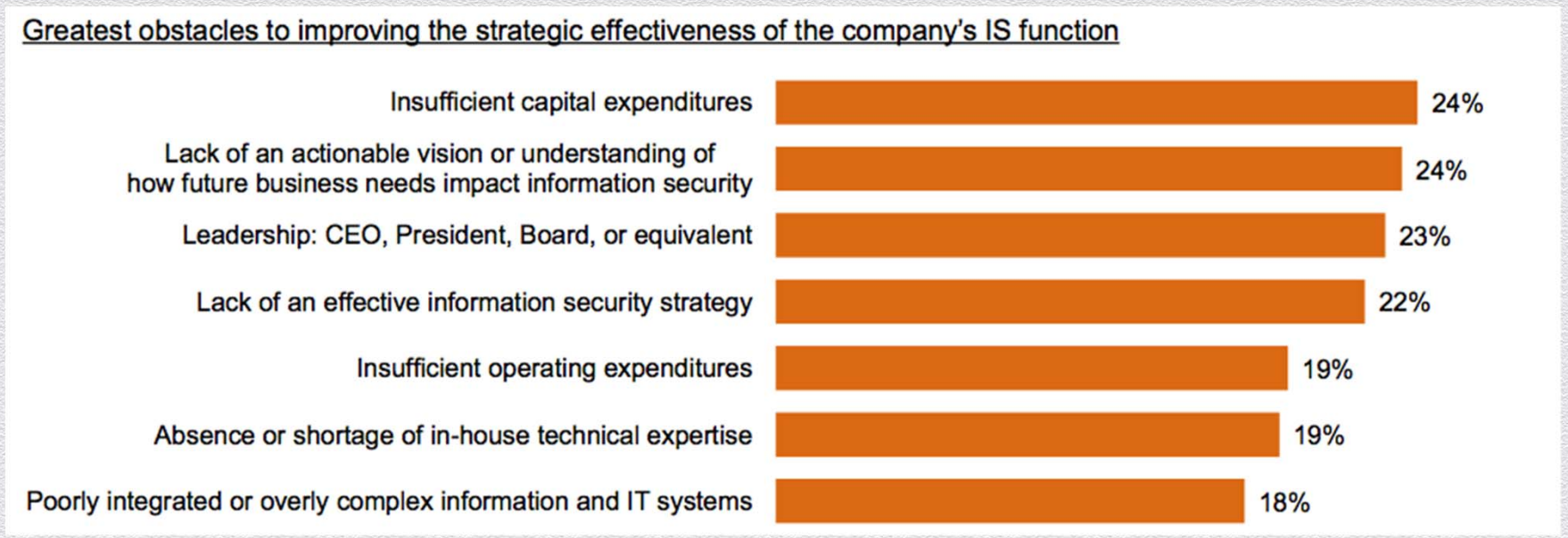
@AttiBull III, ESQUIRE
Chief Legal Council – U.S.
WILL PREPARE OPINIONS FOR BACON

Urbane SECURITY

How compliance is failing security!

- This isn't new – many talks have been given, but no progress made!
- Not a single compliance framework issue
- Cost + Difficulty / Resources
- More and more having to comply to numerous compliances

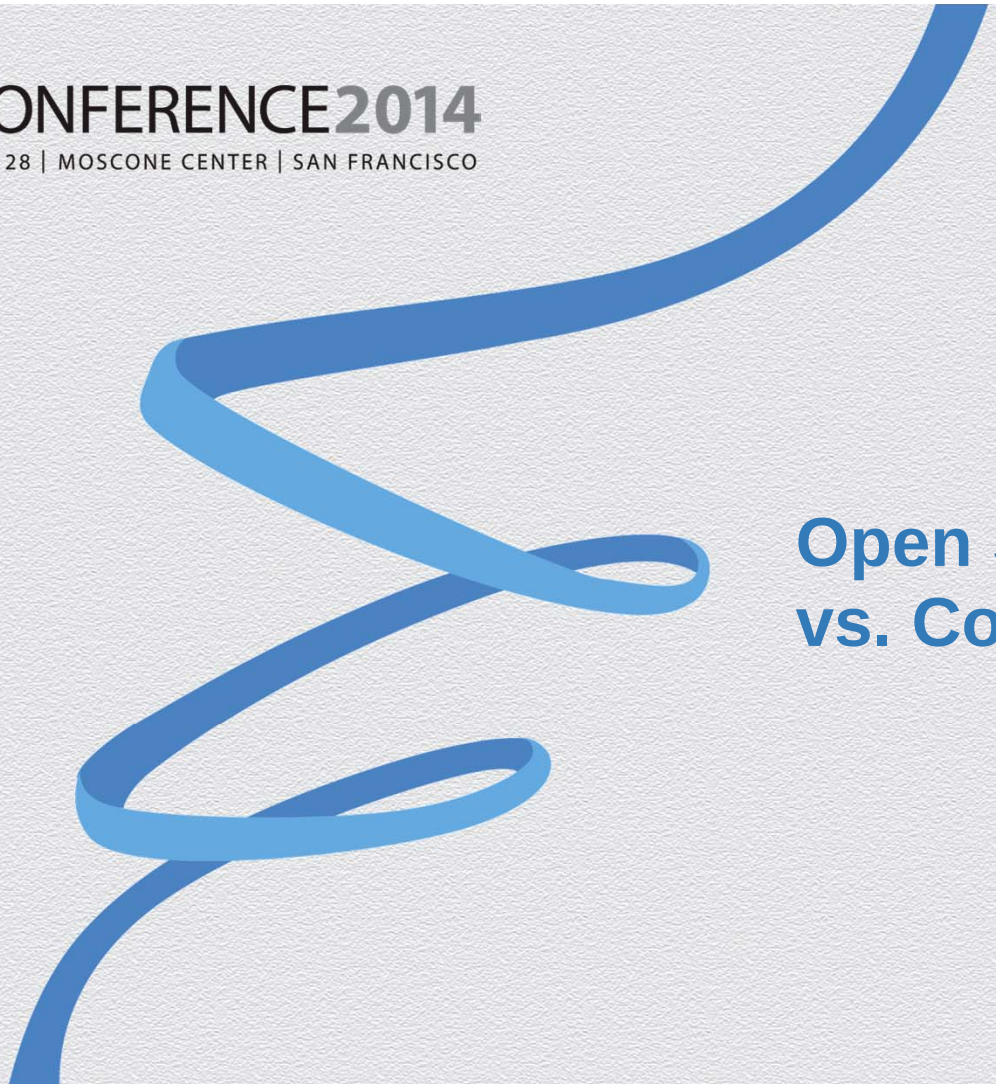
Let's spend smarter!



Source: PWC [The Global State of Information Security® Survey 2014]

RSA CONFERENCE 2014

FEBRUARY 24 – 28 | MOSCONE CENTER | SAN FRANCISCO



Open Source vs. Free vs. Commercial

Urbane SECURITY

Open Source still has a stigma

Benefits of open source solutions?

- Invest in people, not products, man
- Cost of 1 solution can obliterate an IT budget (log collection and system management costs how much?)
- Only one PCI-DSS requirement can't be met using OSS – External Vuln Scans
- Provides greater flexibility in design, customization, and growth
- Not locked in to a specific implementation.

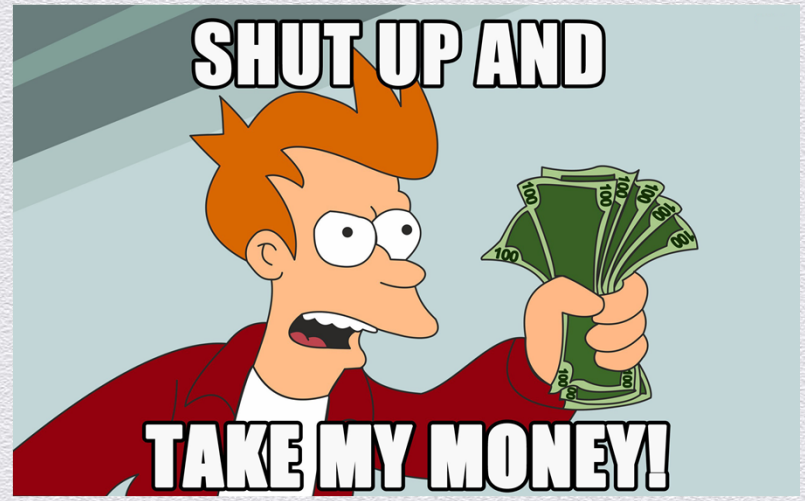
Urbane SECURITY

#RSAC

RSACONFERENCE2014

Why not an open source solution?

- Support? Sometimes for a fee, sometimes non existent
- It doesn't usually "just work"
- Just shut-up and take my money!



RSA CONFERENCE 2014

FEBRUARY 24 – 28 | MOSCONE CENTER | SAN FRANCISCO

The issues and solutions?

Urbane SECURITY

The community issues

- No clear configuration guidelines
- Theoretical application
- Freemium solutions
- Focused on one OS but not others.

OpenPCIProject.com

Urbane SECURITY

The goal of the OpenPCI Project

- Guidelines on how to implement PCI and other security controls
  - Cross-Platform
  - Tried and Tested
  - Scalable but also Small Scale
  - Beyond compliance
  - Pros and Cons for each vs commercial alternative
- Specific walkthroughs on configuration of OSS
  - Simple Deployments
  - Ready to go Installs / VMs
  - Manageable

RSA CONFERENCE 2014

FEBRUARY 24 – 28 | MOSCONE CENTER | SAN FRANCISCO

Top issues facing organizations (and solutions!)

Urbane SECURITY

PCI DSS Control Areas

1. Implement Firewalls
2. Change Defaults
3. Protect CHD
4. Encrypt in Transit
5. Anti Virus
6. Secure System and Apps
7. Limit Access
8. Assign Unique IDs (+2FA)
9. Physical Controls
10. Logging
11. Penetration Testing / Scans
12. Policies

The Top PCI Issues Facing Most Organizations

1. Implement Firewalls
2. Change Defaults
3. Protect CHD
4. Encrypt in Transit
5. **Anti Virus**
6. **Secure System and Apps**
7. Limit Access
8. **Assign Unique IDs (+2FA)**
9. Physical Controls
10. **Logging**
11. **Penetration Testing / Scans***
12. **Policies***

Which would you say is #1?

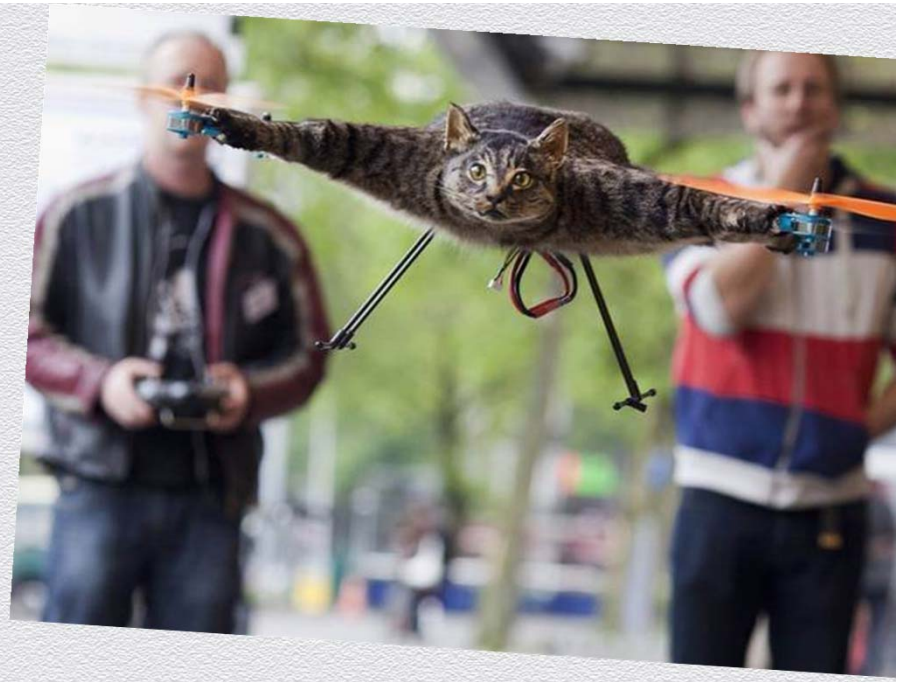
Urbane SECURITY

#RSAC

RSACONFERENCE2014

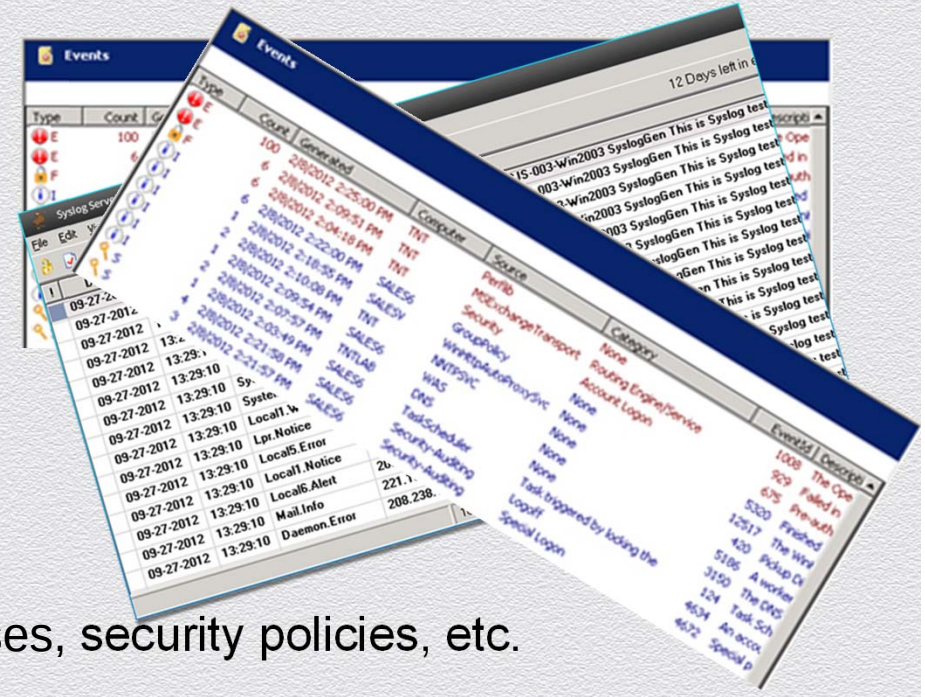
Logs Logs Logs…

- PCI-DSS Requirement 10
  - The mother of all requirements
- Considerations for logging:
  - Generation of events
  - Shipping logs to central location
  - Storage and processing of logs
  - Monitoring of logs
- Thousands of ways to skin a cat



Generation of events

- Is more better?
- What at a minimum?
  - Logins (Success and Failed)
  - All admin actions
  - Log access
  - Initialization / Clearing of logs
  - Addition / Deletion of users, databases, security policies, etc.



Shipping Logs to Central Location

- Linux / Mac / Network Gear / etc.
  - Syslog all the things
  - Agents? Depends on HIDS.
- Windows
  - Windows Event? Ugh.
  - Agents? Probably
  - Why not integrate with a HIDS?

Storage and Processing of Logs

- Easy storage/parsing? Just a syslog server
- Advanced? Oh let me count the ways
  - Fluentd
  - Logstash
  - Apache Flume
  - Facebook's Scribe
  - Graylog2
- Which one's right for you? Ugh…

Monitoring of Logs

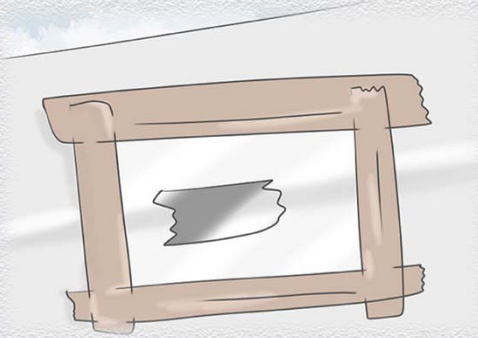
- What events to look for?
- What defines an anomaly requiring action?

File Integrity Monitoring

- What do I monitor?
- How do I monitor It?
  - OpenSource Tripwire
  - OSSEC
  - Samhain
  - Weekly Script + Hash + Diff
  - Built In Detection

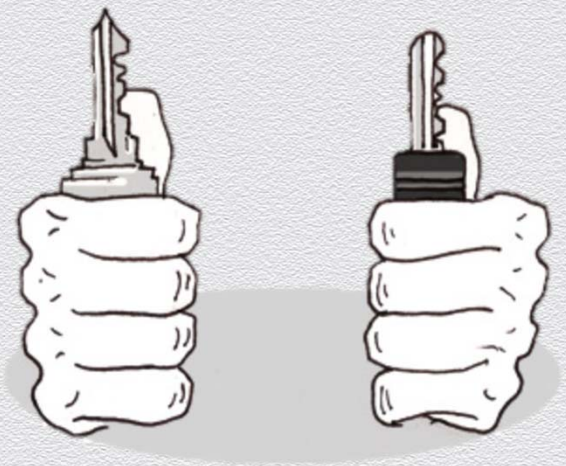
Patch Management

- What has to be patched?
- Linux – Cake
- Windows –WSUS + Custom Packages / WPKG
- Mac – Munki
- Puppet + Chef
- Definitely an area that needs more development.



2 Factor Authentication

- Certificate Based
  - VPN
  - Jump Box
- SMS Based
  - Roll your Own
- OATH Based
  - Hardware - Yubikey
  - Software – Lots
- Other – Wikid or Authenticator - Radius or Custom Plugin?



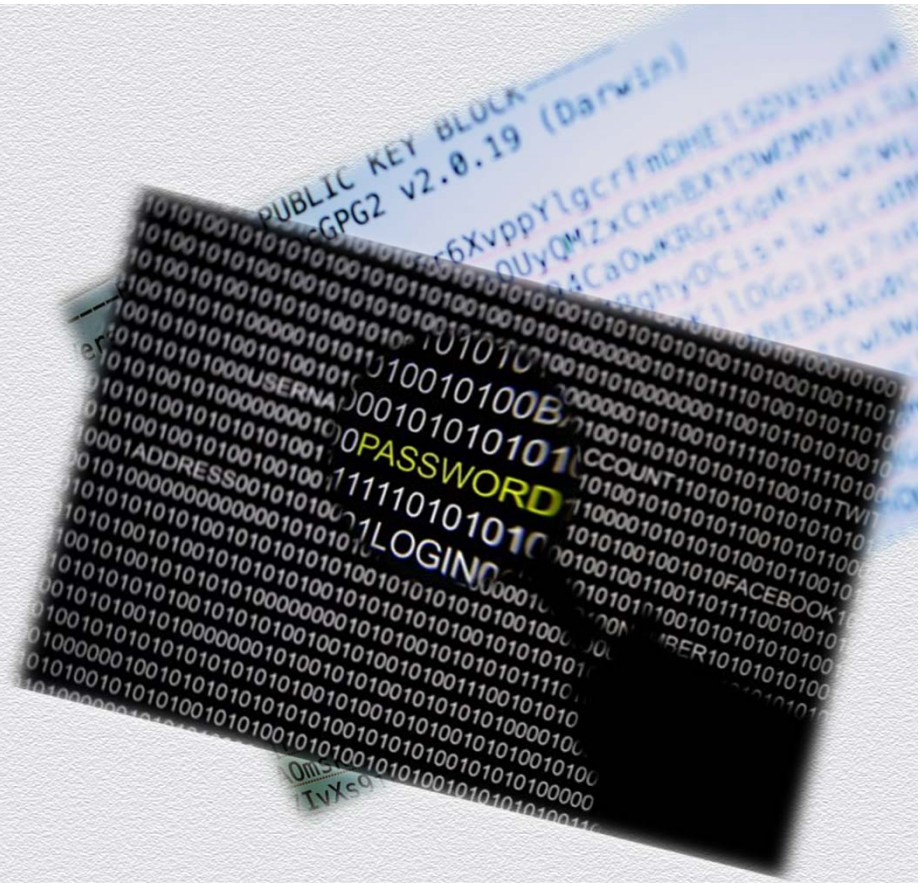
Anti Virus

"PCI DSS Requirement 5.1: Deploy anti-virus software on all systems commonly affected by malicious software (particularly personal computers and servers)."

- Depending on situation, Anti-Virus does not need to be signature detection based and can be application whitelisting based.
- Home grown solutions may also work (i.e. check for and kill rogue processes + FIM)
- Or, It can be ClamAV based

Cryptography

- Key Management
  - Dual control + split knowledge
  - Secure key generation
  - Storage and protection of keys
- SSL certificates often overlooked
- Built-In database encryption



RSA CONFERENCE 2014

FEBRUARY 24 – 28 | MOSCONE CENTER | SAN FRANCISCO

Summing It Up

Urbane SECURITY

RSA CONFERENCE 2014
FEBRUARY 24 – 28 | MOSCONE CENTER | SAN FRANCISCO

Questions & Answers

info [at] UrbaneSecurity.com
Twitter: @UrbaneSec

Urbane SECURITY