RSAConference2016

San Francisco | February 29 – March 4 | Moscone Center

Connect to Protect

SESSION ID: PDAC-T09

Realities of Data Security

Scott Carlson

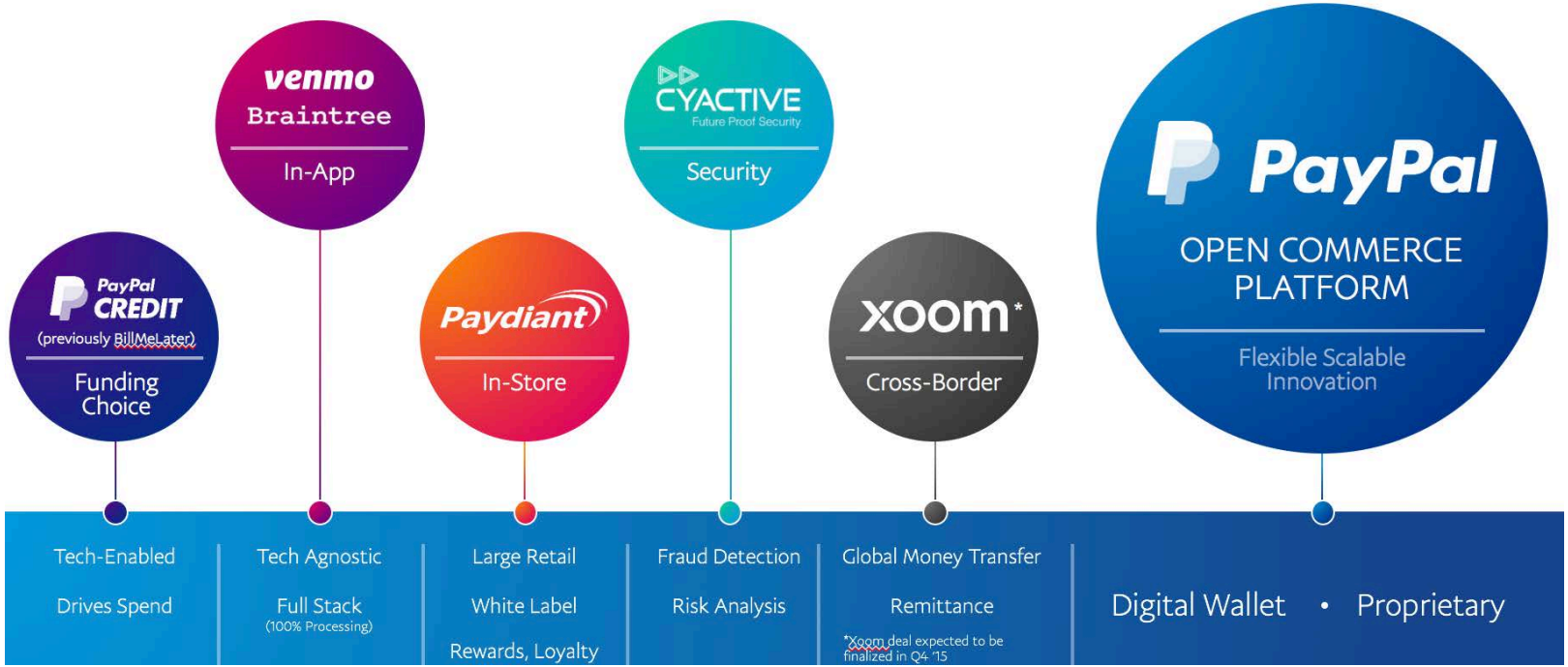
Director – Security Solutions

PayPal

@relaxed137

#RSAC

The Data Complexities



Why should we trust anyone with our Data?

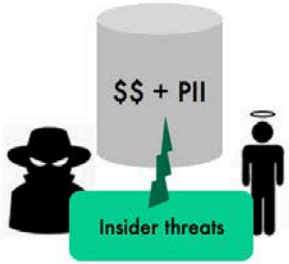
People actually need data to do their job

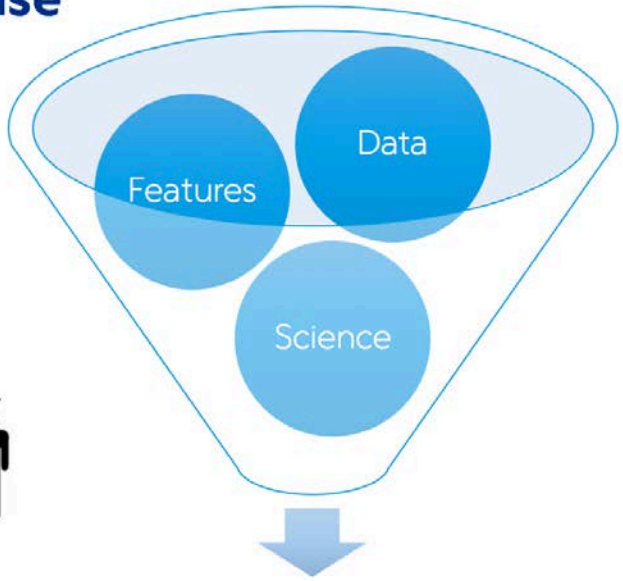
Email Marketing
Customer Support
Business Analytics
Financial Analyst
Marketing

Software Developer
Network Operations
Security Operations
HR / Payroll
Fraud Control

Wide-spread problems

Insider Misuse





55%

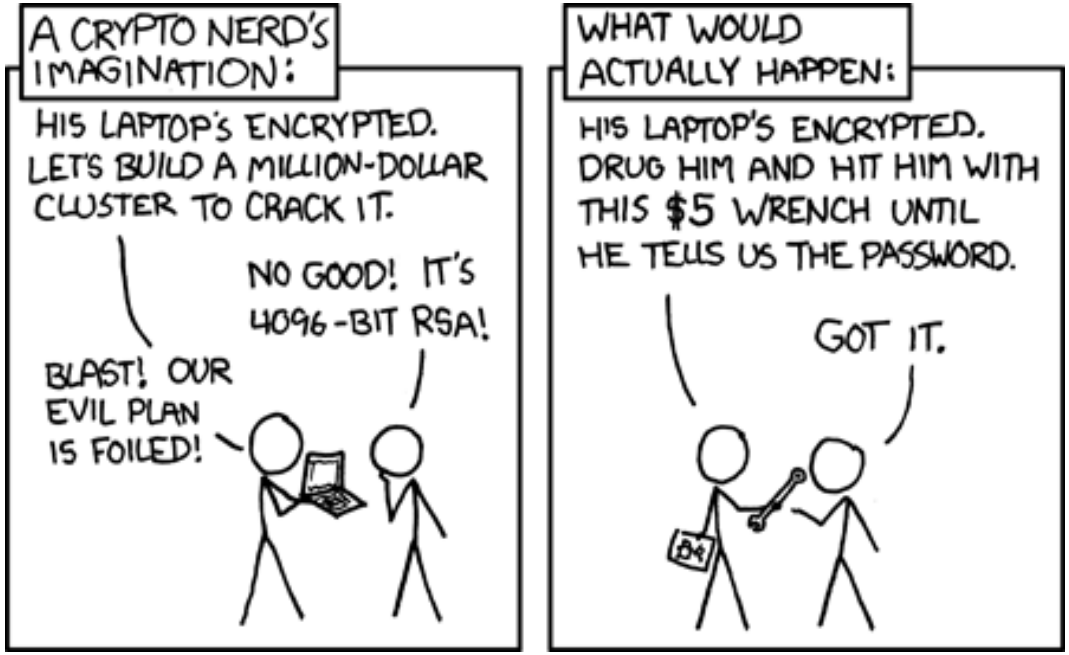
THE TOP ACTION WAS PRIVILEGE ABUSE—AT 55% OF INCIDENTS—WHERE INTERNAL ACTORS ABUSE THE ACCESS THEY HAVE BEEN ENTRUSTED WITH.

Source: Verizon 2015 DBIR

The People Problem

"Think of how stupid the average person is, and realize half of them are stupider than that."

-- George Carlin



So Now What ??

When you are thinking about solving this dilemma, you cannot just worry only about the data itself

Data security should strive to

Find It

Data repositories with restricted/PII data
Business work flows & data flows
Identify owners, does data leave your network

Secure It

Delete or move into a secure network zone Encrypt data when it is found insecure
Create access rights controls & fix bad process

Monitor It

Ongoing monitoring with $tool – users & systems
Data scanning tools for compliance
Inbound/outbound flow monitoring
kill data streams & wall of shame

Find It

Ask

- Hey, where is our data?
- Where did this come from? Where is it going?
- Where Else could It be ?
- Are you caching anything ?
- How many copies are there?
- Has anyone taken it home?
- Did anyone stick it “in the cloud”

Validate

- Buy Stuff or Build Stuff
- Data tools haven’t caught up with data systems
- You cannot find everything with Tagging, sometimes you have to sniff it out
- Don’t forget your logging systems, file shares, and desktops
- To sample or not to sample

Secure It

Zones

- Build network zones in the right places to house the data where it needed
- Separate employee zones from customer zones from analytics zones
- If zones exist, uplift controls to match your new standard
- Build a common Bill of materials & definition of “Run the business”

Encrypt

- Deploy Hardware Security Modules (HSM) where required
- Make sure your tools can decrypt where appropriate
- Keys should be as unique as you need them to be
- once you encrypt the data, make sure that the data entry point is encrypted too

Monitor It

Logging

Build use cases

"Log all activity from DBA's and watch for select from application tables"

Log All the Things; keystroke log if required

positive & negative testing required for tools

tap, syslog, integrated, custom, modules, …

In-Line Detection

decrypt data if required

deploy at all ingress and egress points that matter

tap, DLP, proxies, email, …

Multi-Layer Trust Model

User Zone	Access Zone	Data Center Zone
Network	Bastion Host	Server
Desktop	Citrix Portal	Data Repository
Applications		Data
		Application

Controls required around Data

Centralized Logging	N, H, A
Vulnerability Scanning	N, H, A
Intrusion Detection	N
Patching Updates	N, H, A
Web Proxy	N
Anti-Malware	N, H
Time Synchronization	N

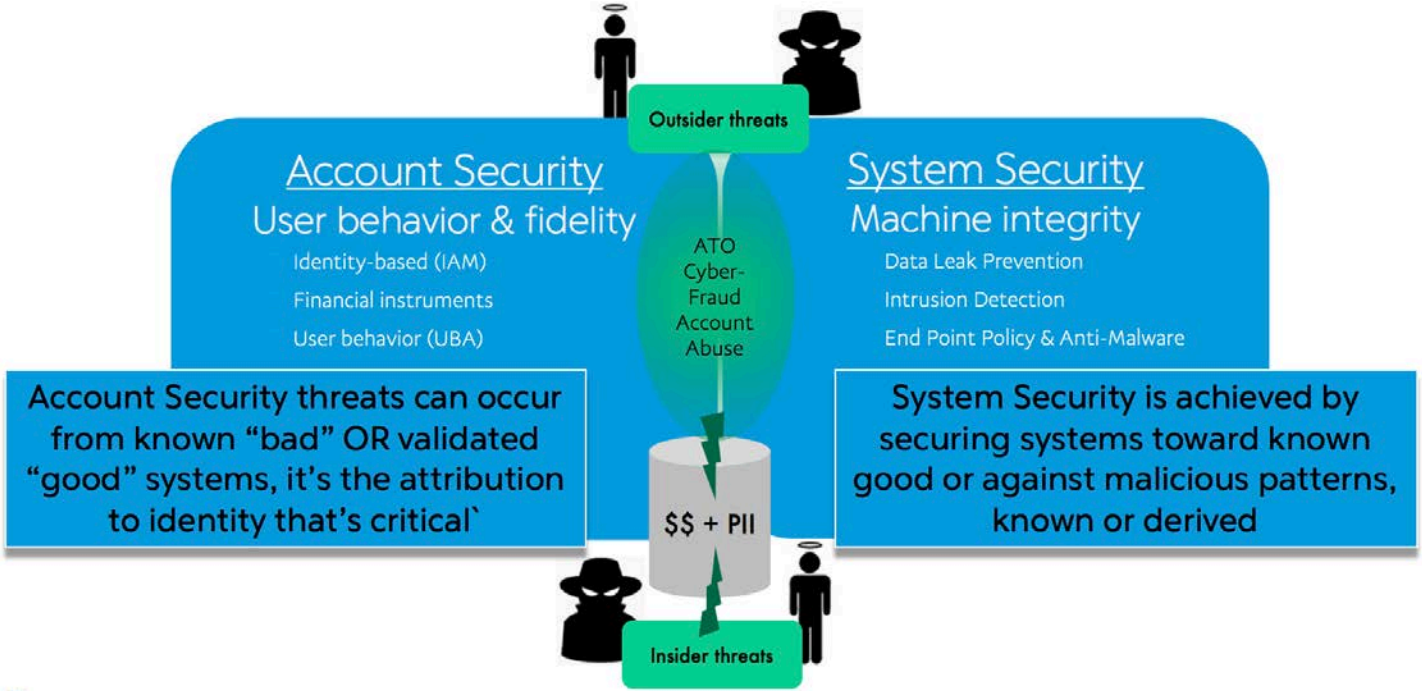
Data Loss Prevention	N
Firewalls	N
Role-Based Access	N, H, A
VDI / Citrix / Bastion	N
Packet Capture	N
File Integrity	H
Configuration Control	H

N=Network H=Host A=Application

Risks of Direct Data Controls

- No one can use the data if its always encrypted
- Tagging Data on Content? Good luck with that
- Tagging Data with Users? Easier, but still
- DLP is only as good as your Regex foo
- Be ready to customize for NoSQL Solutions
- Vendors design for “most common”... Know anyone like that ?

Monitor the human too



Threat Behavior Buckets

Never Anyone (Always Prohibit)

- No one should EVER do this
- No machine should EVER do this

Never This (Point Prohibit)

- This type of person should never do
- This type of machine should never do
- This type of data should never go

Never Seen (Watch and React)

- (Source Location)+(Source Machine)+ (Source Person)+(Target)+(Action)
- One of these items is irregular

Don’t say <u>NO</u>

Say <u>HOW</u>

Data Security is not a permanent state

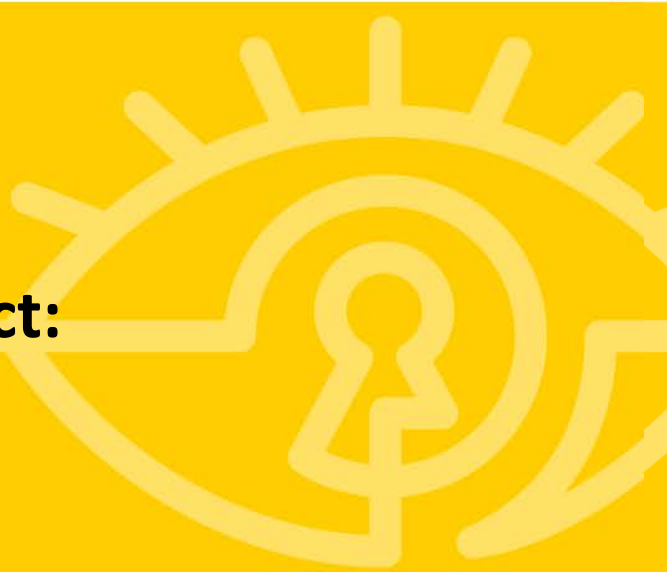
Data Security can not work effectively unless you have agility

(there's nothing static about data)

Pulling it all off

- Build technical and business standards related to use of data and control of data - “The Law”
- Build technical standards related to the controls expected of secure, restricted zones & related to the encryption / access to data – “The How”
- Find restricted data throughout the company, and scan for locations that should have NO data
- Identify method to protect the data once found – delete / relocate / protect / encrypt & execute
- Implement technical controls at the endpoint and network and repository
- Apply continuous monitoring controls to data & people

Build solutions and processes that outlast the people building them



For more information, please contact:
Scott Carlson
sccarlson@paypal.com
@relaxed137