Data Security

For non-technical yet accountable management

John “JB” Bartholomew
Sr. VP of Sales

TD Bank
America’s Most Convenient Bank®

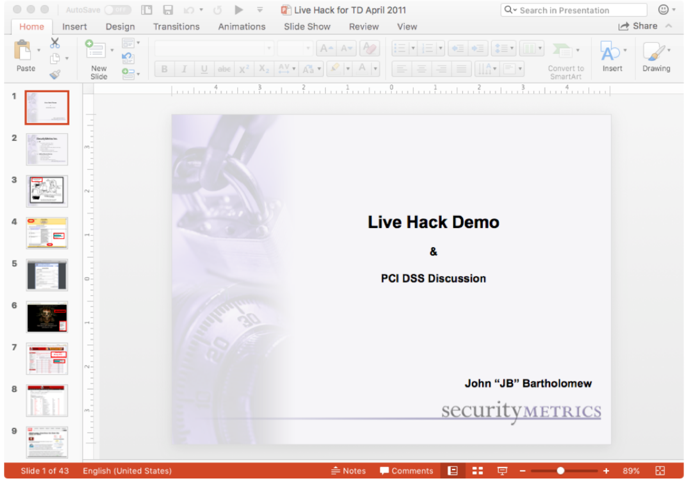
securityMETRICS®

Protect our Clients

- Security solutions
- Simplify compliance

TD and SecurityMetrics

- Collaborating since 2005



Live Hack Demo

&

PCI DSS Discussion

John "JB" Bartholomew

securityMETRICS

TD Bank
America's Most Convenient Bank®

securityMETRICS®

SecurityMetrics & PCI

PCI Involvement

Pre-PCI
- 1 of 5 original scan vendors
- CPP/Breach Pilot

Contributors for
- PCI Pen Testing Guide
- Shared hosting Appendix

PCI working groups or SIGs
- Encryption
- Mobile
- Cloud
- Scoping

PCI Task Forces
- Small Merchants
- Associate QSA program.

Compliance

PCI ASV

PCI Level 3 & 4 validation
- SAQ
- TIP
- SMB/DSE

PCI Programs
(Mass-compliance)

Security Tools

VA scans
Managed Firewall
Managed Security
Security Training
PANscan
PIIscan
Security Policies
Breach Warranty
...

Professional Services:

PCI ROC
PCI QSA SAQ
PCI PA DSS
PCI P2PE
PCI P2PE PA
PCI Forensics (PFI)
Penetration Testing

Live Hack

Attack Host [Running]
Hack Tools
Remote Desktop ...
Malware Tools
Windows Update
Files For Presenters
SM Desktop
Recycle Bin
9:21 AM
5/28/2015
Left ⌘

Target Host 2 [Running]
Recycle Bin
Patient Information
Recurring Billing Inf...
Firewall Status
SM Desktop
Windows Update
Happy Valley Medical Clinic
9:24 AM
5/28/2015
Left ⌘

Business/Financial Officer

- Finance, treasury, accounting, budgeting, money operations, expense tracking, investment management, etc...

- Buck(s) ... Here

- (Financial) Data Accountability

Common mistake #1

OOPS!

- Assign data security solely/primarily to IT 😟
  - Don’t know where all the data is 😳
  - Don’t understand all the relative sensitivities 😬
  - Don’t have authority to get needed cooperation 😕
  - Misplaced incentive for any needed IT corrections 😇😈

“Fundamentally, data security is not a tech problem,
but a business/organizational issue
with a tech component.”

Common mistake #2

Make it work first...

Then think about security

”Why is there never enough time to do it right the first time, but always enough time to do it over?”

Step 0 – The Security Committee

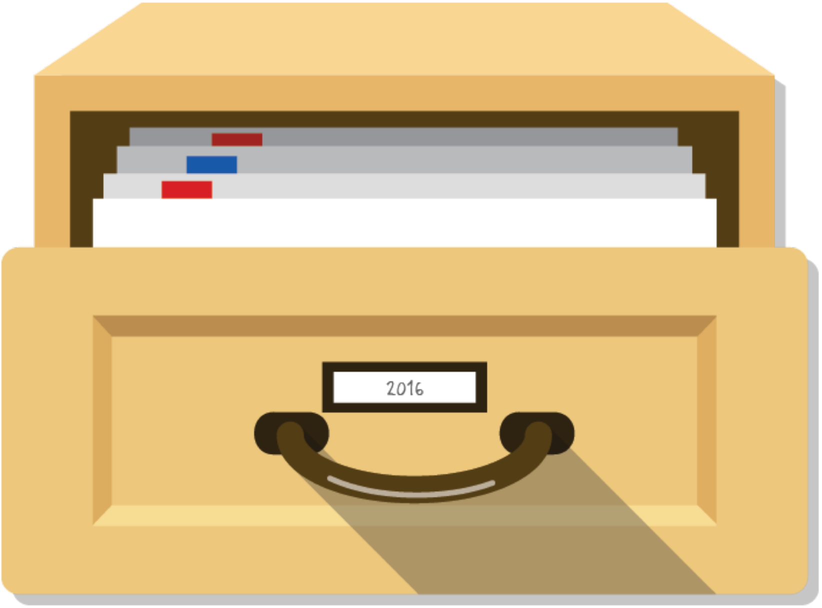
- Executive
- IT/Security
- Legal
- Public relations
- Other department heads

1st Step – Data, data, who's got the data?

Identify:

- Data components/types

- Owners & users



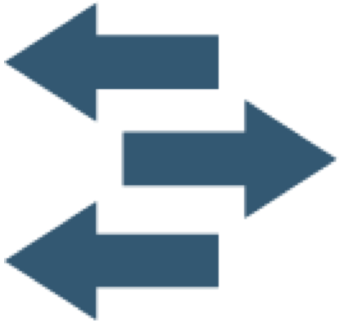
Step 1(b) – Data needed?

Review:

- Data flows, usage & business requirements
- Data sensitivities
- Retention/storage
- 3rd party exposure

What can be reduced or eliminated?

The sensitive data you handle determines the extent of your data security needs.



Sensitivity

Classification	Description
Sensitive	Data that is to have the most limited access and requires a high degree of integrity. This is typically data that will do the most damage to the organization should it be disclosed.
Confidential	Data that might be less restrictive within the company but might cause damage if disclosed.
Private	Private data is usually compartmental data that might not do the company damage but must be keep private for other reasons. Human resources data is one example of data that can be classified as private.
Proprietary	Proprietary data is data that is disclosed outside the company on a limited basis or contains information that could reduce the company's competitive advantage, such as the technical specifications of a new product.
Public	Public data is the least sensitive data used by the company and would cause the least harm if disclosed. This could be anything from data used for marketing to the number of employees in the company.

http://www.pearsonitcertification.com/articles/article.aspx?p=30287&seqNum=9

Step 1(c) – Schedule next data review?

“No plan ... is a plan to forget?”

Business/Organizations change!

Schedule your next data review.

Do not allow it to be
a check box meeting
where everyone says,
“nothing’s changed.”

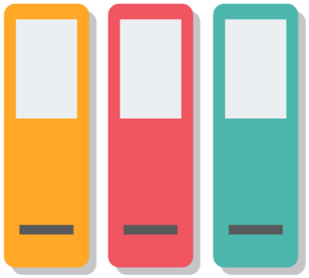
Step 2 –
Hand over project to IT & Security Operations

Wrong!

TD Bank
America's Most Convenient Bank®

securityMETRICS®

Step 2 – Define & Refine Guidelines



Jointly define/identify:

- **Policies** – guiding principles/objectives
- **Procedures** – approaches to accomplish policies
- **Controls** – specific instructions/parameters
- **Metrics/Verification/Frequency** – how to know that you know
  - i.e. checks and balances! ☺

Don't forget:
- continuity/recovery!
- third-party oversight!

Step 2(b) – Schedule your next review

Jointly review:

- Policies
  - Are these sufficiently definitive?
  - Adequately include continuity/recovery & 3rd party oversight?
- Procedures
  - Are the procedures adequate to achieve the policies?
- Controls
  - Are the controls specific enough to fulfill the procedures
- Metrics/Verification/Frequency
  - What don’t you know still?

Security Basics

The PLAN

- Risks
- Accountability
- Policies
- Processes
- Controls
- Metrics

PPCM Objectives

- Protect
- Detect
- Respond

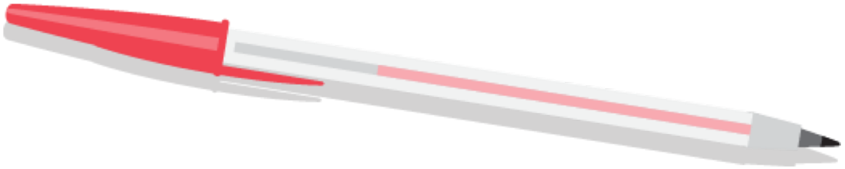
Execution by

- Technologies
- Processes & people

"You can understand and oversee data security!"

QUESTIONS?

www.securitymetrics.com



jb@securitymetrics.com

TD Bank
America's Most Convenient Bank®

securityMETRICS®