Shoot First, Ask Questions Later

Using Bold and Immediate Action

Russ Scadden & Marcel Davidson
October 26, 2016

Protecting Data from Unauthorized Use

Trust or Distrust

Trusted employees who need access to the data to do their jobs

A Model of Distrust

- Because you cannot trust everyone…
  - You must protect as though you can trust no one ☹
- Fail to a “safe” state
  - For sensitive data: ***deny*** (by default)

Trust vs. Distrust

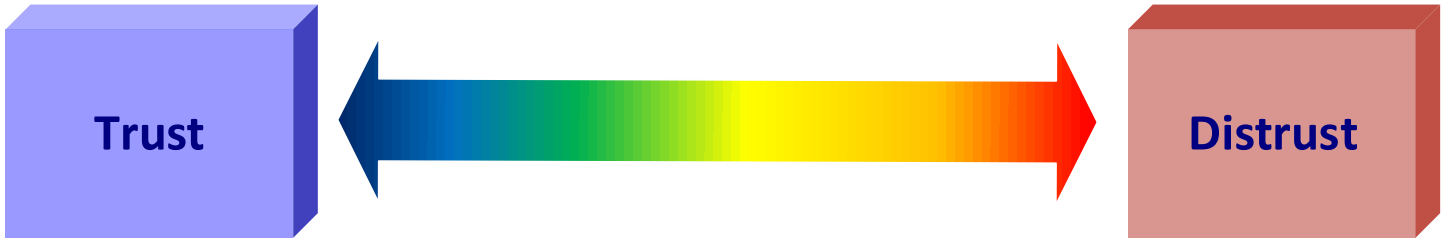
- Trust
  - ***Truster*** willing to be vulnerable to ***trustee*** based on expectations that ***trustee*** will perform as expected
  - Optimistic
- Distrust
  - ***Truster*** expects ***trustee*** to act in a manner contrary to ***truster's*** expectations
  - Pessimistic

- Which is "safer" in todays cyber climate?

Can Trust and Distrust Coexist?

- Assume: No
  - Unidimensional model
- Assume: Yes
  - Multidimensional model

Trust – Distrust Continuum



Confidence in trustee

Reduced fear
Reduced need to monitor

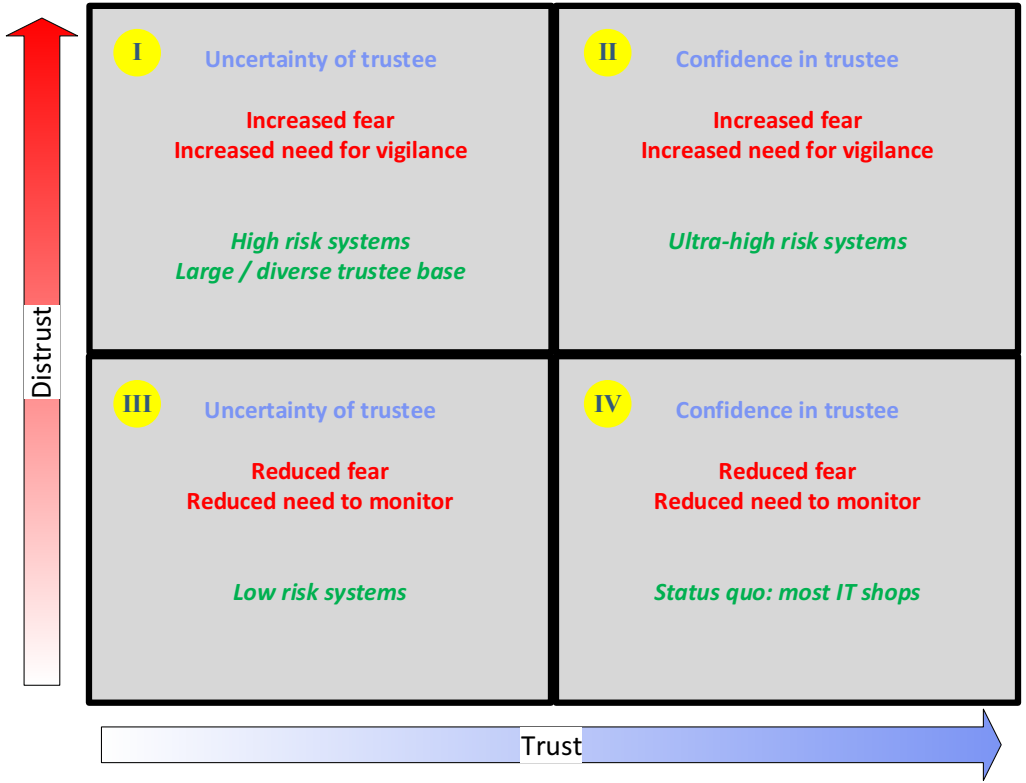
Status quo: most IT shops

Uncertainty of trustee

Increased fear
Increased need for vigilance

High risk systems
Large / diverse trustee base

Trust - Distrust Coexistence



Trust / Distrust Assertions

- Trust and distrust *can* coexist
- Trust: associated with ***user***
- Distrust: associated with ***environment***
- Safest security posture (quadrants I, II)
  - High trust user: Q II
  - Low trust user: Q I
- Assume: distrust towards environment

Anti-Virus Software

Blacklisting the bad things

Need to identify the person or process, and decide whether the intent is good or bad.

- Whitelist
  - Known good or acceptable
- Blacklist
  - Known bad or unacceptable

Security is based on how we use these lists.

About Whitelisting

- Only authorized activity allowed
  - *Explicit*: list of high trust users
- Any unspecified access is denied (by default)
  - *Implicit*: high level of distrust

Australian Govt.

Top 4 Mitigation Strategies

- *The Top 4 Strategies to Mitigate Targeted Cyber Intrusions (the Strategies) are the most effective security controls an organization can implement at this point in time based on the our current visibility of the cyber threat environment.*

- *The Australian Signals Directorate (ASD) assesses that* ***implementing the Top 4 will mitigate at least 85% of the intrusion techniques*** *that the Australian Cyber Security Centre responds to.*

Top 4 Mitigation Strategies

1. ***Whitelisting***
2. Patching (applications)
3. Patch (operating systems)
4. Minimize administrative privileges

Database Whitelisting

- Only authorized data consumers (applications, users, etc.) access data

Whitelisting: Pros

- High probability of true-positives (TPs):
  - I.e., most access likely to be authorized
- High probability of true-negatives (TNs):
  - I.e., most non-events appropriately dismissed

Whitelisting: Cons

- Vulnerability to false-negatives (FNs):
  - Risk: accidentally whitelisting unauthorized activity
  - “Dead wood” accumulates over time
- Vulnerability to false-positives (FPs):
  - Risk: accidentally blocking approved activity

Multifactor Whitelists

- More factors increase WL effectiveness
- Renders WL more difficult to “spoof”

Whitelist Example

Rule	Param 1	Value 1	Param 2	Value 2	Param 3	Value 3	Param 4	Value 4	Action	Comments
100	IP_ADDRESS	^10\.(10|20|30)\.							Kill	Disallow clients from these subnets
200	MODULE	^(app1\.exe|app2\.exe)$	IP_ADDRESS	^10\.199\.					Log	Log all activity by these applications
300	AUTHENTICATED_IDENTITY	^MYAPP$	OS_USER	^fred$	HOST	workstation1	IP_ADDRESS	^10\.200\.	Session	Session tracking for this user
400	AUTHENTICATED_IDENTITY	^MYAPP$	OS_USER	^wilma$	HOST	workstation2	IP_ADDRESS	^10\.200\.	Session	Session tracking for this user
500	AUTHENTICATED_IDENTITY	^MYAPP$	OS_USER	^service$	HOST	linux1	IP_ADDRESS	^10\.40\.50\.60$	Allow	Application server - full access
600	AUTHENTICATED_IDENTITY	BARNEY$							Kill	Black list rule for user: BARNEY
700	AUTHENTICATED_IDENTITY	^APP_MAIN$	OS_USER	^hrsvc$	HOST	windows1	IP_ADDRESS	^10\.45\.55\.66$	Allow	Application server - full access
800	AUTHENTICATED_IDENTITY	ADMIN	IP_ADDRESS	^10\.199\.	MODULE	:NULLVAL:	D,HH24	^[2-6],(0[7-9]|1[0-7])	Log	Log all other admin user activity (office hours)
999						-			Kill	Default rule: kill

Building the Whitelist

Identifying sensitive data and privileged accounts

- Identify Most Sensitive Data
  - Able to focus on columns versus entire table
- Identify Privileged Individuals
  - Application Accounts
  - Database Accounts
  - System Accounts

Terminating the Unknown

Deny access to unknown users and processes

- Learning mode
  - Source IP
  - Application Name
  - Connect ID
  - Before/After work hours
- Terminating the unknown
  - Before data is returned
  - Research after session is terminated
  - Alert to Security Operations
- Default rule: kill

Whitelist Considerations

- Requires monitoring (independent of access controls)
- Possible performance burden
  - Offset through caching the result
- Whitelist maintenance
  - “Drift” between WL rules and workload
  - False-positives
- Action
  - What to do about failures (default deny)?
  - What to do about “grey list”?

Protecting Data from Unauthorized Use

Management Commitment

Partnership

Management support working with Security Engineering

Working relationship between:

- Security Engineer
- Funding Manager
- Application Operations
- Data Steward
- Solution Manager
- Business Partners
- Auditors

Logistics

Putting it all together

- Weekly Meetings
- Ongoing maintenance
- Funding
- Priority
- Sec Ops
- App Ops

Sample Summary Report

DB Account	OS Account	Client Host Name	Client Type	Subnet	Client Trust Level	Hours	Client Program	Event Name	Schema	Table	Event Count
FRED	flintstonefj	freds-laptop	Workstation	10.200	Med	Office	TOAD	SELECT FGA	APP_SCHEMA	VENDOR	18
WILMA	slatewq	wilma-mac	Workstation	10.200	Med	Office	PL/SQL Developer	SELECT FGA	APP_SCHEMA	PAYMENT	4
BARNEY	rubblebb	rubble-pc	Workstation	10.200	Med	After	SQLl*Plus	SELECT FGA	APP_SCHEMA	LINE_ITEM	304
BARNEY	rubblebb	rubble-pc	Workstation	10.200	Med	Office	SQLl*Plus	SELECT FGA	APP_SCHEMA	PAYMENT	284
ABC	rpt-svc	Linux1	Server	10.50	High	After	oracle@db1	SELECT FGA	APP_SCHEMA	LEDGER	232
ABC	rpt-svc	Linux2	Server	10.50	High	Office	oracle@db2	SELECT FGA	APP_SCHEMA	CUSTOMER	112
XYZ	batch	windows1	Server	10.60	Low	Office	myapp.exe	SELECT FGA	APP_SCHEMA	PAYMENT	22

Case Incidents

- Low trust clients consuming “sensitive” data
- Unauthorized access channel to “sensitive” data
- Inappropriate use of credentials
- Inexperienced users accessing “sensitive” data
- Accidental misconfiguration by data consumer
- Violation of departmental policies by end user
- Downstream data loss / leakage
- Grey-listing of privileged user activity