RSA®CONFERENCE
CHINA 2012
RSA信息安全大会2012

THE GREAT CIPHER

MIGHTIER THAN THE SWORD

伟大的密码胜于利剑

Identifying, Valuing, and Protecting Informational Assets

Branden Williams & Jason Rader
RSA Security

RSACONFERENCE
CHINA 2012
RSA信息安全大会2012

How do we value information?

Bits vs Bits

- On one hand, we have bits of data

- On the other, we have MANY “bits” of money

What’s the Conversion Rate?

- 10 Bits = 10 RMS?
- 1 Gigabit = £1,000?
- 1 Byte = 2 bits?

- Where is this rate? How do I use it?
  - Doesn’t exist!
  - Too many factors affect it to map globally.

What about Information Classification?

IN
OUT
SSSH!
GOVT. SECRECY REPORT
THEY'VE GOT A HOLE!

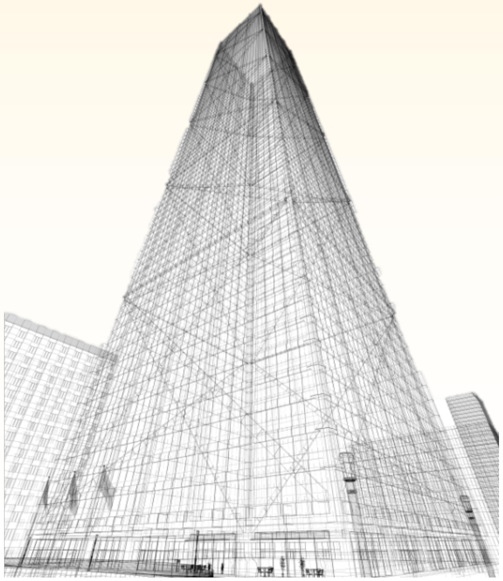
What about Information Classification?

- Typical classification systems are problematic
  - Lack definition (what constitutes info of this kind?)
  - And automation (teach systems to handle)
  - Don’t address individual data value (is a vault required?)

What about the math?

- Info Classification doesn't truly address the cost/benefit/risk
  - Let External Value = payoff * $\log_{10}$(number of actors)
  - Let Confidence = historical ability to calculate value
    - Number > 0 and ≤ 1
    - Low confidence throws protection costs higher
- $\$ \text{ spent on protection} \propto \dfrac{\text{External Value}}{\text{Confidence}}$
- Internal values must be considered!

We need a new model



- Minimum model requirements:
  - Group information by value
    - To ME
    - To Competitor/Military
    - Only if LOST
  - Address information value over time
    - Information changes in value over time
    - Usually depreciating, some more rapidly than others
  - Reflect # of actors and motivation
  - Reflect change in motivation based on payoff
    - Market forces can dramatically alter this
    - Large data stores are more attractive than small ones

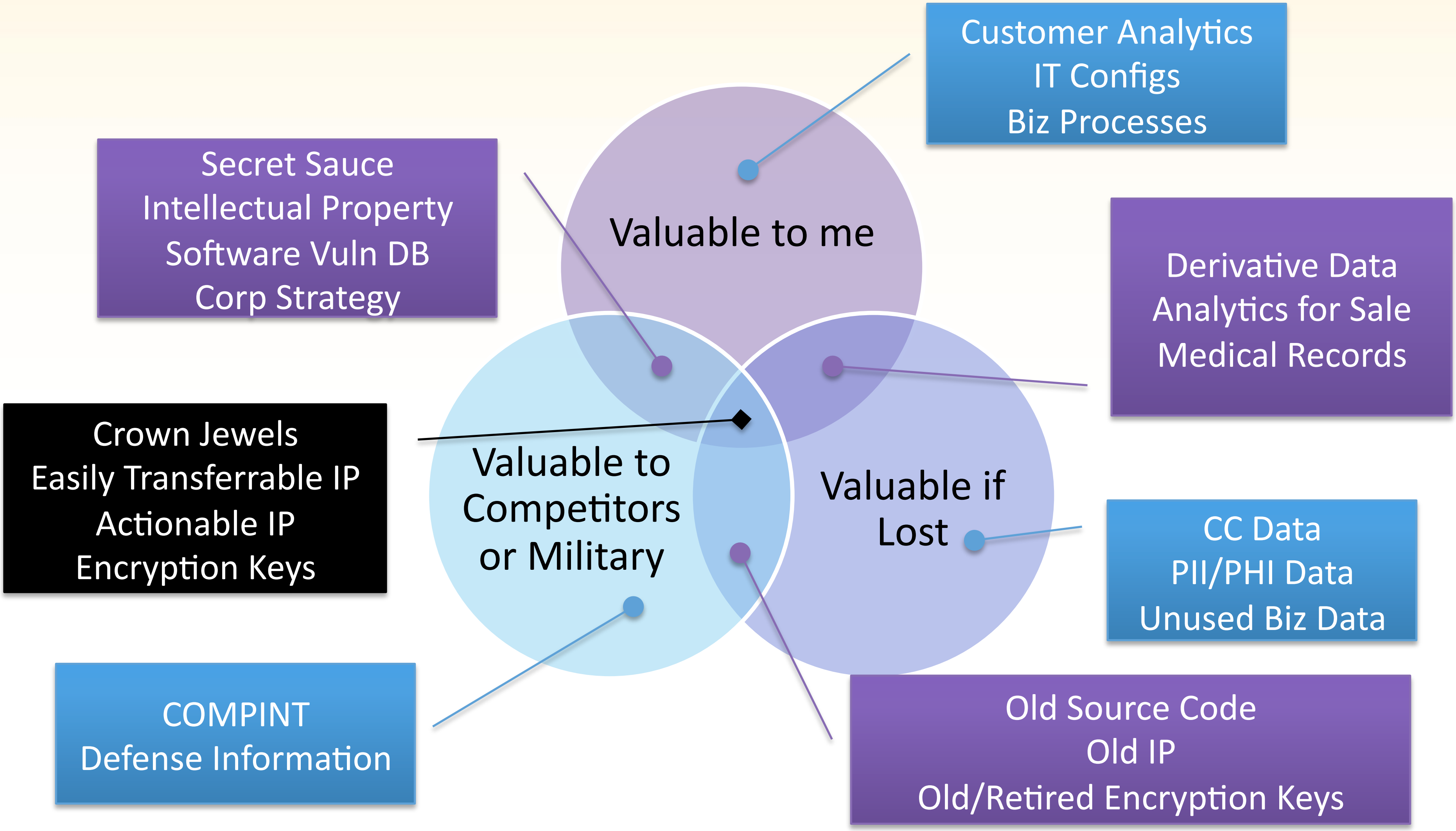
The model needs to be simple

- No industry jargon
- No dictionary required
- Not dozens of pages

Yet flexible

- Must be able to adjust with value changes
- Must rely on accurate inputs
  - Numbers of actors
  - Projected payoffs with data theft
  - Strength of perimeter defenses
  - Number of business processes using the data
  - Amount of data sprawl
  - Account for amount of data as a change in payoff
- Must be able to affect security posture

A Visual Depiction of the Model



Valuable to me

Valuable to Competitors or Military

Valuable if Lost

Customer Analytics
IT Configs
Biz Processes

Secret Sauce
Intellectual Property
Software Vuln DB
Corp Strategy

Derivative Data
Analytics for Sale
Medical Records

Crown Jewels
Easily Transferrable IP
Actionable IP
Encryption Keys

CC Data
PII/PHI Data
Unused Biz Data

COMPINT
Defense Information

Old Source Code
Old IP
Old/Retired Encryption Keys

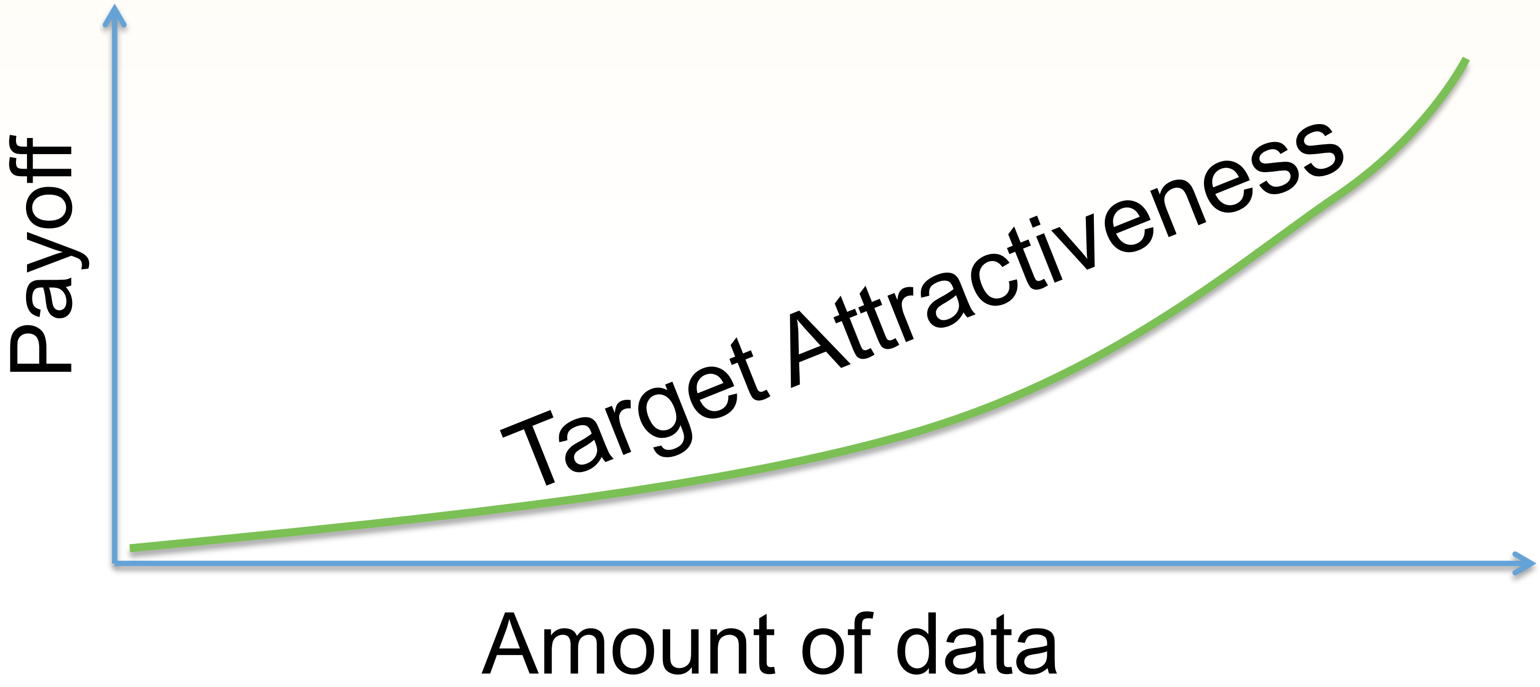
The Model

Value to You	Value to Comp.	Value if Lost	Examples	Breach Prob.	Biz Impact	ACTION
1	50	2.3B*	Number of Potential Actors			
Y	N	N	Customer Analytics IT Configs Business Processes	Low	A/I	Secured, but not vaulted
Y	Y	N	Intellectual Property Secret Sauce Software Vuln DB Corp Strategy	Med	C–Delayed Risk A/I Immediate	Protect (Vault)
N	Y	Y?	Old Source Code Old IP (where new IP is derived) Old encryption keys	Med	C/I	C: Destroy I: Secure Archive

The Model (part 2)

Value to You	Value to Comp.	Value if Lost	Examples	Breach Prob.	Biz Impact	ACTION
1	50	2.3B*	Number of Potential Actors			
N	N	Y	Credit Card Numbers PII/PHI Unused Biz Data	High (# Actors)	C	Outsource Destroy Obfuscate
Y	N	Y	Sec. Data Analytics (revenue) Medical Records High roller customers Proprietary Algorithms Financial Results	Low (High Impact)	C	Protect IP (Vault) Secure Data
Y	Y	Y	Crown Jewels Easily transferrable IP	High		Protect (Vault)

The Relevance of Data Mass



Combating Risk from Data Growth

- Reduce data stores
  - Truncation
  - De-value options (tokens)
  - DESTROY
- Reduce the effective size
  - 1M records / 10 keys = 100K recs!
  - Multiple algorithms

How to apply the model

- Look at the kinds of data your business controls
  - Try to define what it is, then relate it to the model
  - Be sure to find information NOT IN USE
  - Understand flow and sprawl of data
- Add values where you can
  - Valuing information is personal
  - Use your own data
  - Don’t rely on external sources to define data value
- Remember CONFIDENCE factor!
- Take Action Per the Model!

Contact:

- Branden R. Williams
  - Branden.williams@rsa.com
- Jason Rader
  - Jason.rader@rsa.com

Thank You

RSA CONFERENCE
CHINA 2012
RSA信息安全大会2012