

A Simple Approach to Infusing Business-Centricity into Your Security Program

One We Can All Implement



Omar Khawaja

April 6th, 2010

Why Business-Centric Security?

- Enables security organization to understand what's important
- Enables stronger communication with business owners

Security is a cost center – the Business pays the bills!



Security LeadersCare Most About...

Breach Prevention

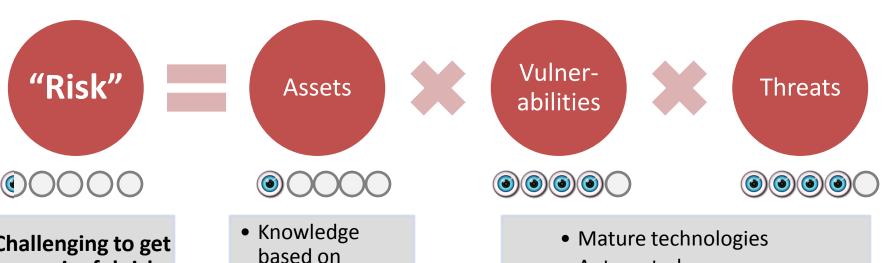
Compliance

Costs...

...the Business!



The Business cares about Risk Security is about Risk



Challenging to get meaningful risk picture w/o accurate valuation of assets

- Knowledge based on interviews and self-reporting
- Depends on context

- Automated
- Industry standards
- "Same" for everyone
- Can be normalized



Security LeadersCare Most About...

Breach Prevention

Requires preventing data from being breached

Compliance

 HIPAA, GLBA, PCI, State Breach Laws, etc. govern specific types of data

Costs...

- of securing data
- of maintaining compliance
- of enabling business in the **information** age

The Business Cares About Data!



The Business cares about Risk

Security is about Risk

Greatest opportunity for improvement!

- Knowledge based on self-reporting
- Depends on context

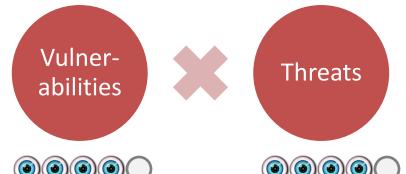






interviews and





- Mature technologies
- Automated
- Industry standards
- "Same" for everyone
- Can be normalized



"Risk"

Challenging to

get meaningful

risk picture w/o

accurate

valuation of

assets

What's Missing?

ISO 27002 Control Areas

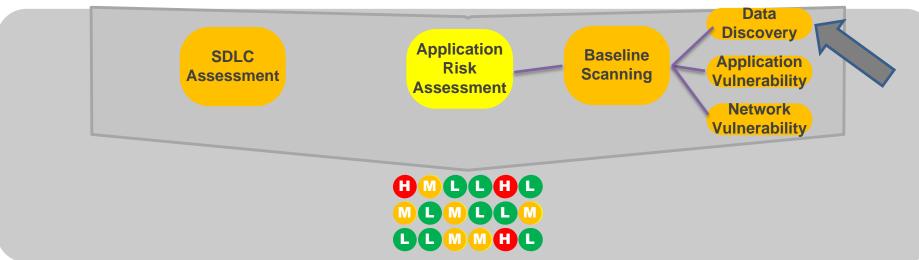


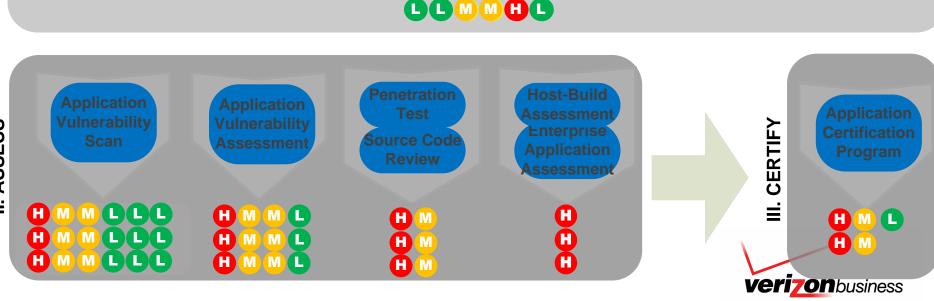




Data-Centric Approach

Application Security





Data-Centric Approach Vulnerability Management

Situation

- Too many "high" vulnerabilities identified
- Impact of each vulnerability is unclear



Challenge

• Which vulnerabilities should be addressed first?



Result

 Address vulnerabilities in order of system value



Remedy

 Assign value to each system based on associated data sets



Data-Centric Approach Security Operations

Situation

 Too many event logs, threats and alerts



Challenge

 Which should be addressed first?



Result

 Address event logs, threats and alerts in order of system value



Remedy

 Assign value to each system based on associated data sets



Data-Centric Approach Compliance

Situation

 Dealing with multiple compliance requirements is complex and costly



Challenge

- What systems need to be compliant?
- Are the required systems compliant?



Result

• Fewer systems within scope of compliance



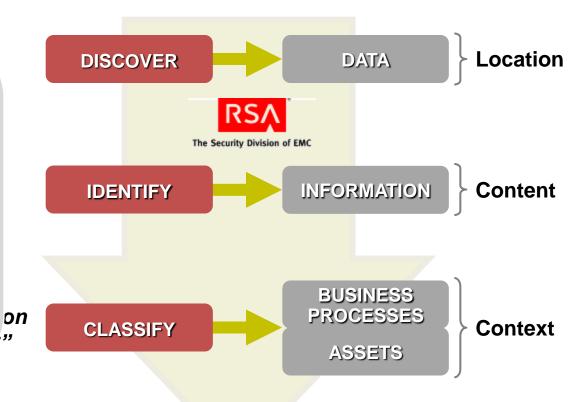
Remedy

- Establish compliance perimeter by discovering which systems store / process governed data types
- Validate data is being encrypted
- Understand how governed data flows through an enterprise



How do you get the data?

Two-thirds of 285
millions breached
records were not known
to be stored on the
systems prior to the
breach.





Source: Verizon 2009 Data Breach Investigations Report

Data Centric Approach

Addresses...

Breach Prevention

Staying out of the headlines

Compliance

Adhere to legal / contractual requirements

Costs

Minimizing total cost of effective security

...the Same Things the Business Cares About!



Finally...

A data-centric approach arms you with the necessary insights to do the right things... not just to do things right!

- Data-Centric is Business-Centric!
- Addresses CSOs' key concerns
- Can be applied to most components of an ISMS
- Security teams see the bigger picture
- Changes the conversation

