Realistic and Affordable Quantitative Information Security Risk Management

Effective risk management for small/medium businesses

Walter Williams 5/18/2013

Who am I

- Walt Williams, CISSP, SSCP, CEH, CPT, MCP
- Senior Manager of Security and Compliance at Lattice Engines
- Current member of BOD for NE ISSA Chapter
- Done everything from PKI, meta directory, LDAP, IAM, vulnerability assessment, penetration testing, risk analysis, security architecture and design, business continuity, disaster recovery, incident response……
- wwilliams@lattice-engines.com
- walt.williams@gmail.com
- @LESecurity
- https://infosecuritymetrics.wordpress.com
- **Security for Service Oriented Architectures CRC Press ISBN 978-1-4665-8402-0**

Thanks, many and manifold

- Dr. Mike Lloyd
- Jeff Bardin
- Donn Parker
- The folks at FAiR
- The Open Group
- Karen P. Stopford
- Matt Truenow
- Everyone at The Society of Information Risk Analysts
- Kevin Riggins
- ISSA
- And a special thanks to the good folks at l0pht who got me into this to begin with

What is Risk so we can measure it?

- First, information security risk is a subset of business risk
  - While important, it does not drive the business
  - It should inform business people in making business decisions
- There are many different definitions for information security risk

The ‘classic’ definition

- Classic definition (NIST): Risk = probability of an event * impact of same event
  - Trouble is that this method would classify SPAM
    - a high probability but negligible impact
  - as having the same risk as a bomb going off in the lobby,
    - a high impact, but negligible probability
  - What’s the problem with that?
    - Decision making based on this analysis would have the business continuity plan cost no more than the SPAM filtering used by an organization.
  - What good is an analysis that doesn’t help you make good decisions?

So, what is risk already?

- Risk is the potential that a given threat will exploit vulnerabilities of an asset or group of assets and thereby cause harm to the organization
  - Comes from ISO 27005
  - Implies a metric: Harm
- Thus to understand (measure) risk involves understanding:
  - Threat
  - Vulnerability
  - Asset
  - Impact/Harm

Assessing Risk

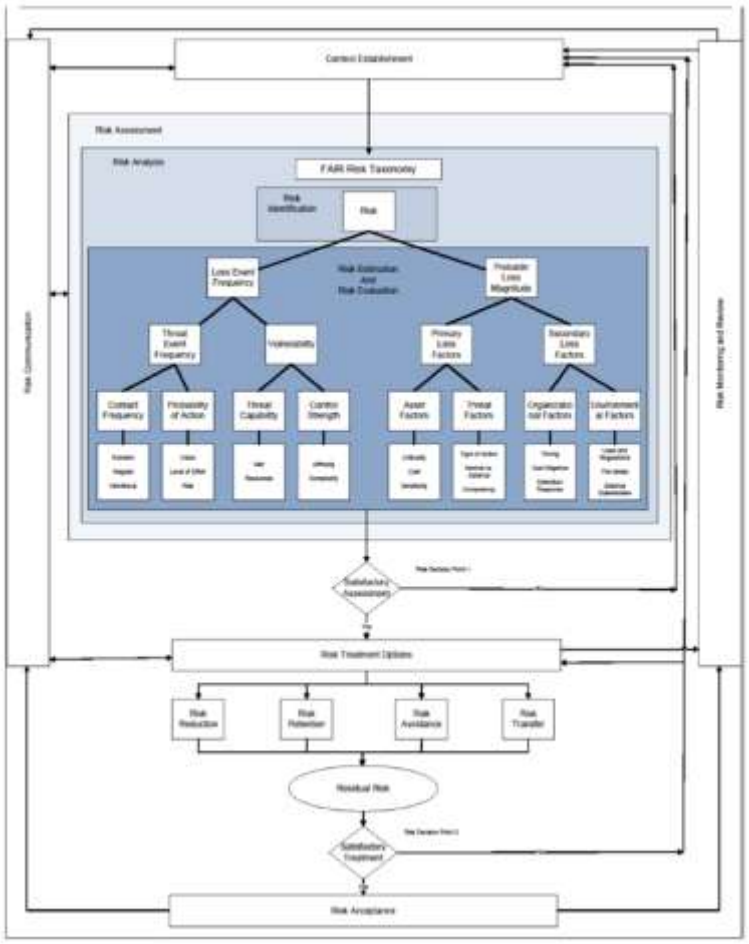
- Octave
  - Very customizable
- ISO 27005
  - Very customizable
- RiskIT
  - Good if you're using CobIT
- NIST SP 800-30
  - Uses classic definition of risk
- TARA
  - Looks at attack risk only

The risk management cookbook

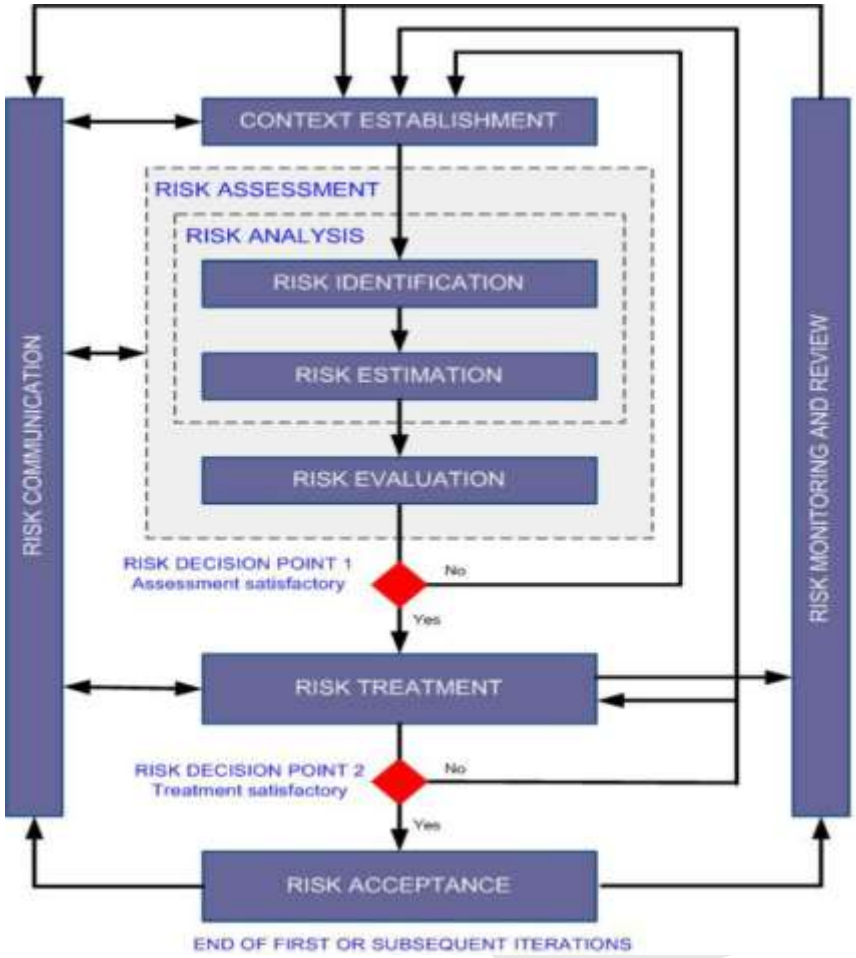
The OpenGroup took ISO 27005 & inserted FAIR into these assessment methodologies to provide metrics for risk estimation

The Risk Cookbook: https://www2.opengroup.org/ogsys/jsp/publications/PublicationDetails.jsp?catalogno=c103

The OpenGroup modified FAIR just enough to make it more useful



This gives us both a process and a means to measure risk



Identification of risks

- Define scope
- Identify the assets in scope
- Identify the threats
- Identify existing controls
- Identify vulnerabilities
- Identify consequences/impacts

Assets

- Different people have different definitions of assets
  - They are all right
- Assets have value
  - This is sometimes hard to determine
  - This value helps identify how much you want to spend preventing incidents
  - You don’t put all of your staplers in a bank vault to prevent their theft
- Most important asset: likely is your data

Value is more than just money

- This is where we find a meaningful metric for risk
  - What is Criticality of system?
  - What is Cost of System?
  - What is Sensitivity of System?
  - What is the loss of productivity?
  - What is the cost of incident response?
  - What fines will be incurred?
  - What is the impact to our reputation?
  - What is the impact to our investors?
- Many of these can be estimated using a monte carlo simulation. More on this later
- This provides us with Impact/Harm

Threats

- Many kinds of threats have the same impact
  - Bomb = earthquake = tornado = tsunami = etc.
  - Therefor you protect against the impact
  - Not the threat
- But not all threats with similar impacts have the same modus apparatus
  - Therefor you protect all points of egress for threats
  - If no threat can act on something, there is no need to protect it
  - It already is protected….

Basel I Threat Categories

- Originated with financial industry
  - Provided free tool for risk measurement
  - http://www.bits.org/publications/doc/bitskalculatorspreadsht.xls
- I have a modified version of this tool
- Reasonable categories
  - Internal Fraud
  - External Fraud
  - Employee Practices and Workplace Safety
  - Clients, Products and Business Practices
  - Damage to Physical Assets
  - Business Disruption and System Failures
  - Execution , Delivery and Process Management

The details

Airplane crash
Application software failure
Automobile crash
Biological agent attack
Bomb attacks
Bomb threats
Chemical spill
Civil disorder
Computer crime
CPU malfunction/failure
DDoS or DoS attacks
Discussing sensitive matters in open
DNS failure
Dumpster diving
Dust/sand
Embezzlement
Epidemic
Extortion
Fire
Floods
Gas leaks
Hardware failure
Hazardous waste exposure
Heat
High winds
Human error
Hurricane
HVAC failure
Lawsuits/ litigation
Leaving computer screen exposed or unlocked
Leaving doors unlocked
Leaving sensitive documents exposed
Lightning
Lost or stolen laptops
Malicious code
Network spoofing
Network/application backdoor
Network/application time bomb
Power failure
Power fluctuation
Radiation contamination
Robbery
Sabotage
Seismic activity
Shoulder surfing
Snow/ice storms
Social engineering
Software defects
Solar flares
System software failure
Tailgating to gain unauthorized access
Terrorist attack
Telecommunications failure
Tidal Wave
Tornados
Trojans
Typhoon
Unauthorized network or system access
Unauthorized scans
Unintentional DDoS
Unintentionally bad legislation
Vandalism
Virus hoaxes
Viruses
Volcanic eruption
War
War dialing
Web defacements
Work stoppage/ strike
Worms

Lattice

Controls

- You have to know what your controls are
  - You have to know why you have those controls
  - You have to know how effective are your controls
- How do you get to this knowledge?
  - Ask
  - Audit
  - Test

Control Categories

- I like to use the ISO 27002 catalog
  - Not perfect but more comprehensive than PCI
  - Leveraged in the BITS provided tool
  - Known and understood internationally
  - If you prefer, use CobIT
- Access Control
- Asset Classification & Control
- Business Continuity Management
- Communications & Operations Management
- Compliance
- Organizational Security
- Personnel Security
- Physical and Environmental Security
- Security Policy
- Systems Development

Vulnerability

- This is the method through with a threat can act on an asset.
- Or, a gap in a control.
  - Sometimes this is the same method through which authorized action takes place
  - Sometimes it is through a method that no one knew existed until it is found and used against you
  - You can only protect what you know.
  - Which is why we protect assets not protect against vulnerabilities

Impact

- This a statement of the harm done by the threat acting on the vulnerability to the asset
  - Not all impacts compromise the entire value of an asset
  - Some impacts will compromise the value of multiple assets.
  - The value of an asset is the aggregate of:
    - Loss of Productivity
    - Cost of Response
    - Cost of Replacement
    - Loss of Competitive Advantage
    - Fines/Judgments
    - Reputation
  - The value of the protection should always be less than the value of the asset
- Again a real metric we can estimate using a monte carlo scenario

Impact: The dilema

- How much is it really worth?
  - Your CEO says X
  - Your CFO says Y (next year Z)
  - Your CTO says A
  - How confident are you in any of their numbers?
- They're all correct! Aggregate!

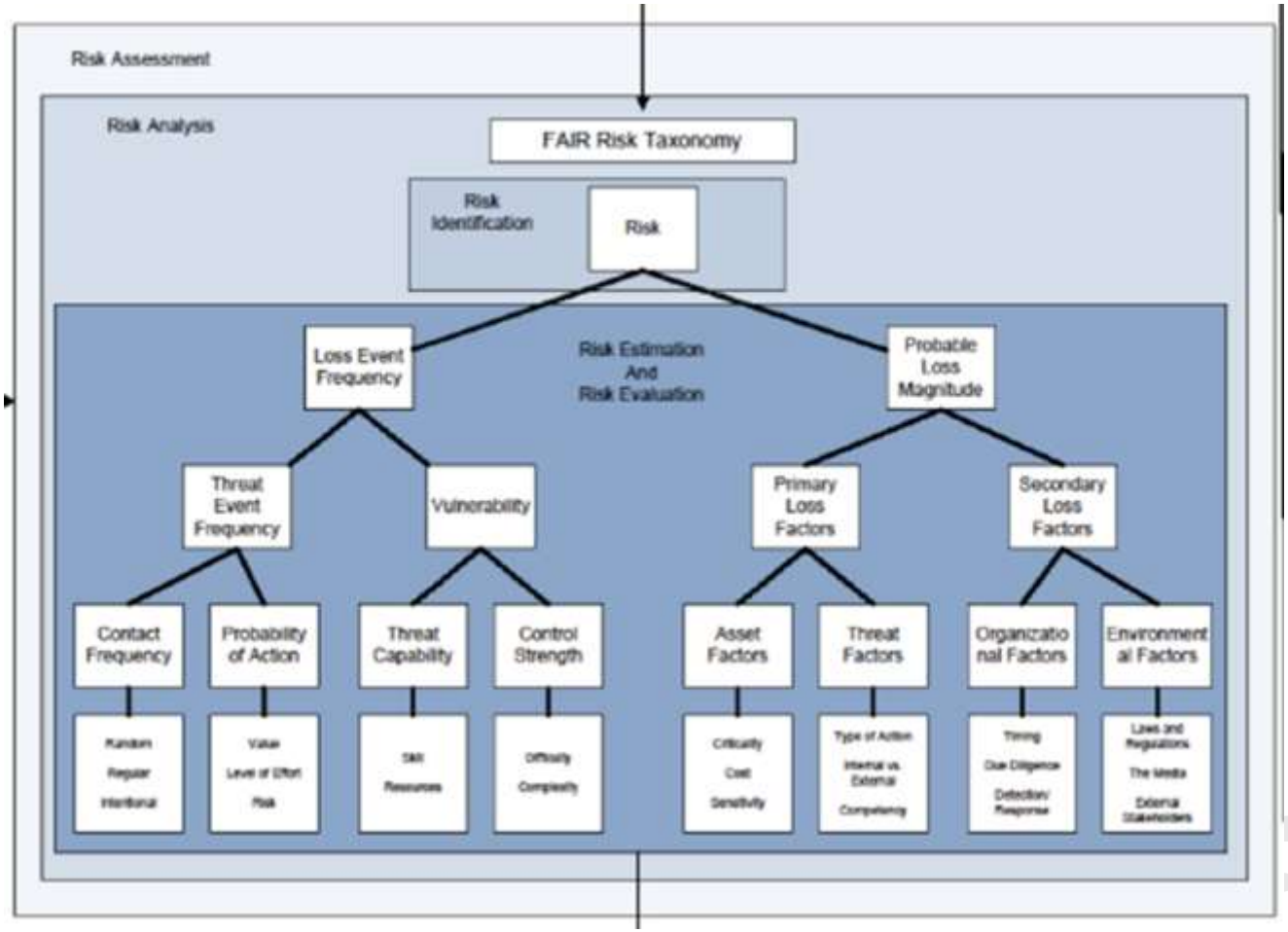
Getting towards analysis

- Understand the impact to each asset
  - Where multiple assets are impacted, aggregate the impacts
- Establish a scale
  - Scale should be proportional to impact
  - Scale should be proportional to the frequency of an event
  - Scale should be proportional to the capability of the threat agent
  - Scale should be proportional to the strength of existing controls
  - Scale should be proportional to the strength of existing vulnerabilities

Closer to Analysis

- In order to measure information security risk, one must first measure
  - Impact
  - Frequency
  - Capability of threat
  - Strength of controls
  - Degree of vulnerability
- Some of these measurements can inform others
  - Loss Event frequency can be expressed as a factor of Vulnerability and Threat Event Frequency
    - If it is hard to exploit, hard to come across, frequency of loss is low
    - If vulnerability is easy to exploit or easy to come across, frequency of loss is high
  - Loss Magnitude can be expressed as a factor of Asset, Threat, Organizational and Environmental issues

Some times you need to estimate



Estimation may be done at any point on the tree where no data below that point is available or reliable.

Vulnerability

- Vulnerability is a factor of
  - Threat capability
  - Or how knowledgeable do you have to be to exploit the vulnerability
- Control strength
  - If the vulnerability exists, but there is no way to get to that method of egress, the strength of the control may eliminate the threat
- CVSS 2.0 numbers provide a point of comparison
  - But ONLY if they are the complete CVSS 2.0 number

Completing CVSS

- CVSS provided with each vulnerability is a generic statement of vulnerability
- To complete:
- http://nvd.nist.gov/cvss.cfm?calculator&version=2
  - This completes the calculation by providing a relative measurement of vulnerability within the context of your environment

Why Probability is Useless

- You have a 100% chance of dying.
- But your chance of dying right now is much less than 1%
- This is why probability is not very useful
- Event frequency is the chance of something happening now

Frequency

- Event Frequency can be derived from historical data BUT
  - Past performance is no guarantee of future results
  - See Sony the day before the first compromise
- Event Frequency can be estimated as a factor of:
  - Contact Frequency
    - How easy is it to encounter the method of egress
  - Probability of Acting
    - How likely is it that some one would exploit the vulnerability
  - Both can be estimated using a BETA Pert distribution
  - This gets better when you calibrate

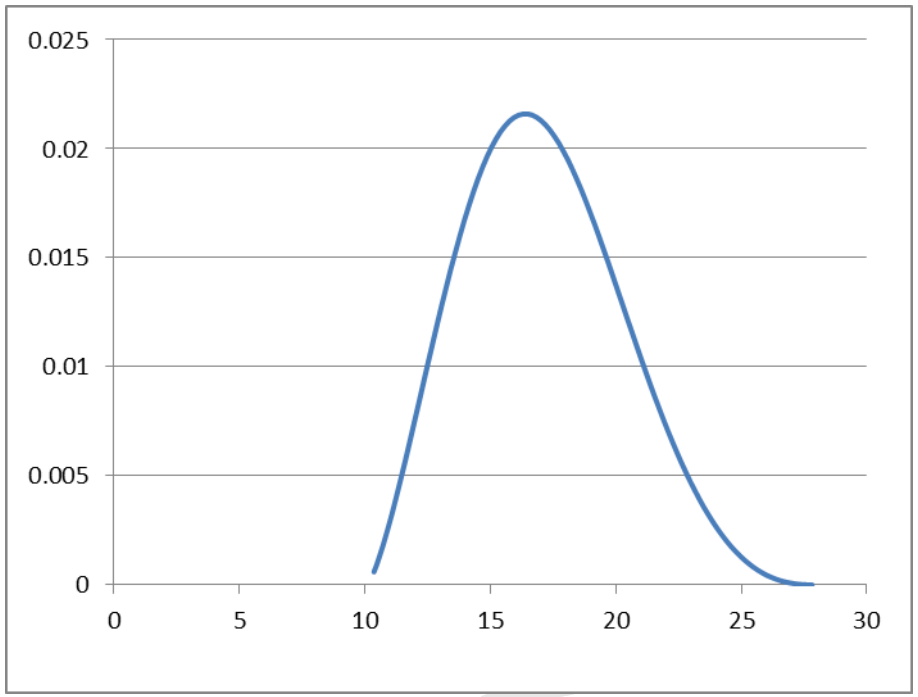
What do I mean by Calibrated?

- Calibration is a measure of what is your level of confidence in the numbers you provide
  - On what day was the Declaration of Independence voted on by Congress:
    - July 2, 1776
    - It was ratified on July 4, 1776
  - Experts often over estimate their level of confidence
    - Until they learn to calibrate
    - The best calibration comes from research
  - Event frequency data available
    - Verizon data breach report, Poneman data breach report, CSI Annual report, dataloss.org, etc.

BETA Pert Distribution

- Provides a reliable way to estimate probability
- Mean =(Optimistic Estimate + (g times Most Likely Estimate) + Pessimistic Estimate) divided by g+2 is the estimate of likelihood (where g=4)
- David Vose proposed that if you replaced g with a value indicating confidence, you could get a more realistic estimate of frequency:
  - Mean=(Optimistic + (Confidence * most likely) + Pessimistic) divided by confidence + 2
- This is very useful for gaging event frequency
- Does *not* need random number inputs (though some think it is improved with random numbers)

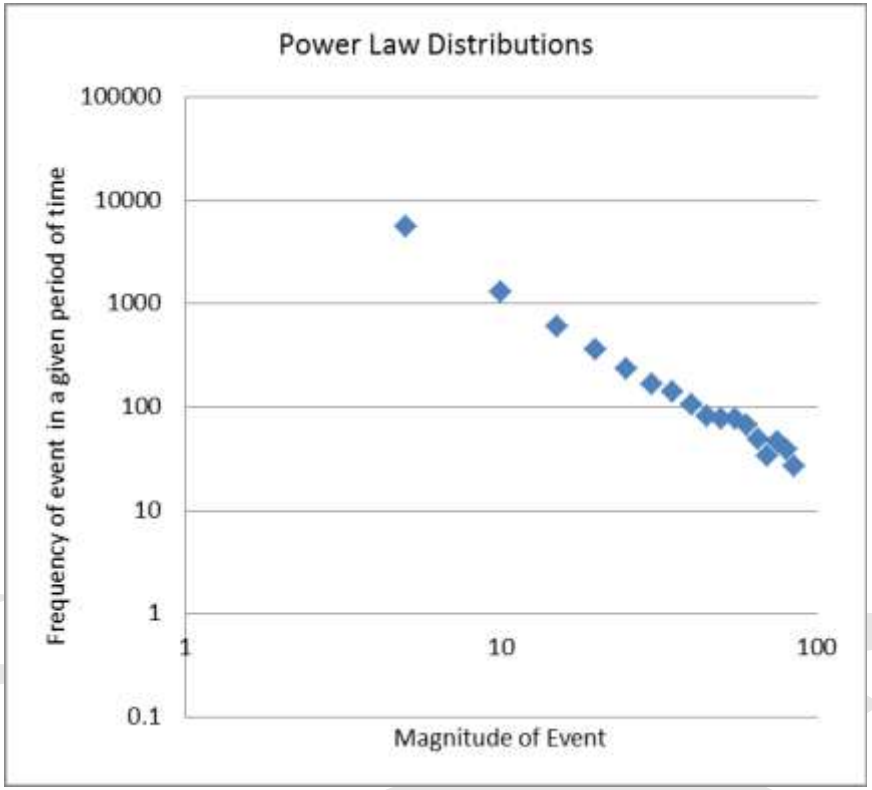
What a BETAPert distribution looks like



Alternative Models

- The Power law distribution has been shown to be rather useful to relate the frequency and magnitude of disasters

To calculate, you need the slope and intercept, a random generator, size of the event, and event frequency



Tools

- Free
  - http://code.google.com/p/openpert/
    - Requires Excel
- Commercial Tools
  - http://www.vosesoftware.com
  - http://www.riskamp.com/library/pertdistribution.php
  - Excel

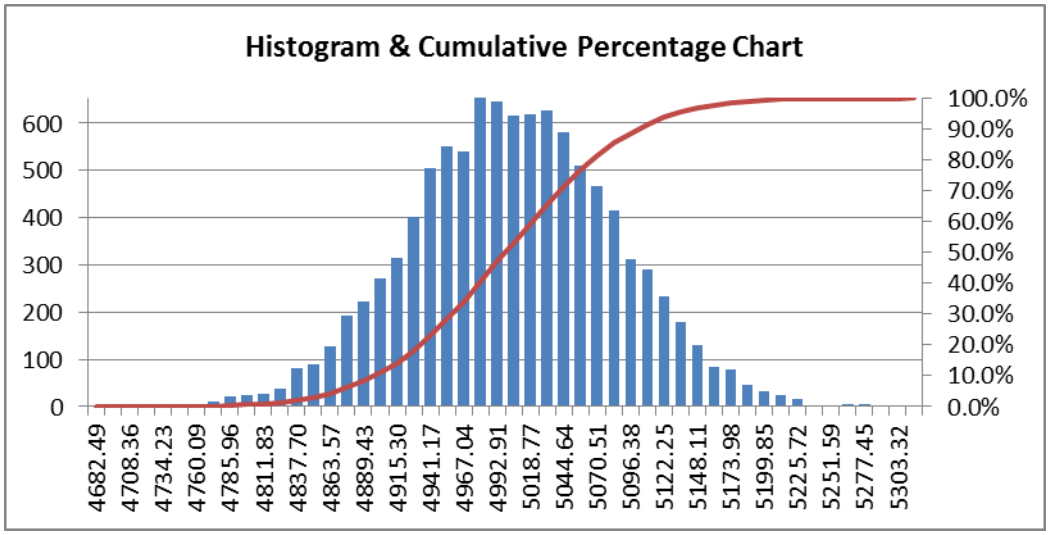
Calculating Risk

- Asset Catalog
  - Derived from interviews
  - Impact to organization from event by a threat regarding asset is key metric
  - This considers the vulnerability and controls context of your organization
- Threat Catalog
  - BITS or other
- Controls Catalog
  - ISO 27002, CobIT or other
- Vulnerability/Gap analysis
  - Your CVSS numbers can help here IF put in context using environmentally calibrated CVSS 2 scoring
- Frequency Estimation and Calibration
  - Frequency is best used to determine priority between two different risks of the same impact to the same asset
- Impact
  - Your best metric

Monte Carlo Simulation

- Simply put, this is a methodology of estimating reality
  - Used by the Manhattan Project
  - You need domain of possible inputs
  - Generate them randomly from a probability distribution over the domain
    - good use for beta-pert
    - Need uniform distribution with large number of inputs
  - Perform a deterministic computation
  - Aggregate the results
    - Determine probability of each result
  - Perfect tool to estimate impact (DEMO)
  - Provides a good metric

Graph of Monte Carlo simulation results



After the Analysis

- Complete Gap analysis through performing vulnerability assessment
- Determine Scale
- Document and communicate risk
- Determine how to manage
  - Remediate, Transfer, Avoid, Accept
- Determine what is residual risk from management strategy
- Implement risk management strategy

Questions?

- wwilliams@lattice-engines.com
- walt.williams@gmail.com
- @LESecurity