Cybersecurity for Medical Devices Using MBSE Simulation

Prithviraj Mukherji PhD

Mukherji Consulting

January 31, 2015

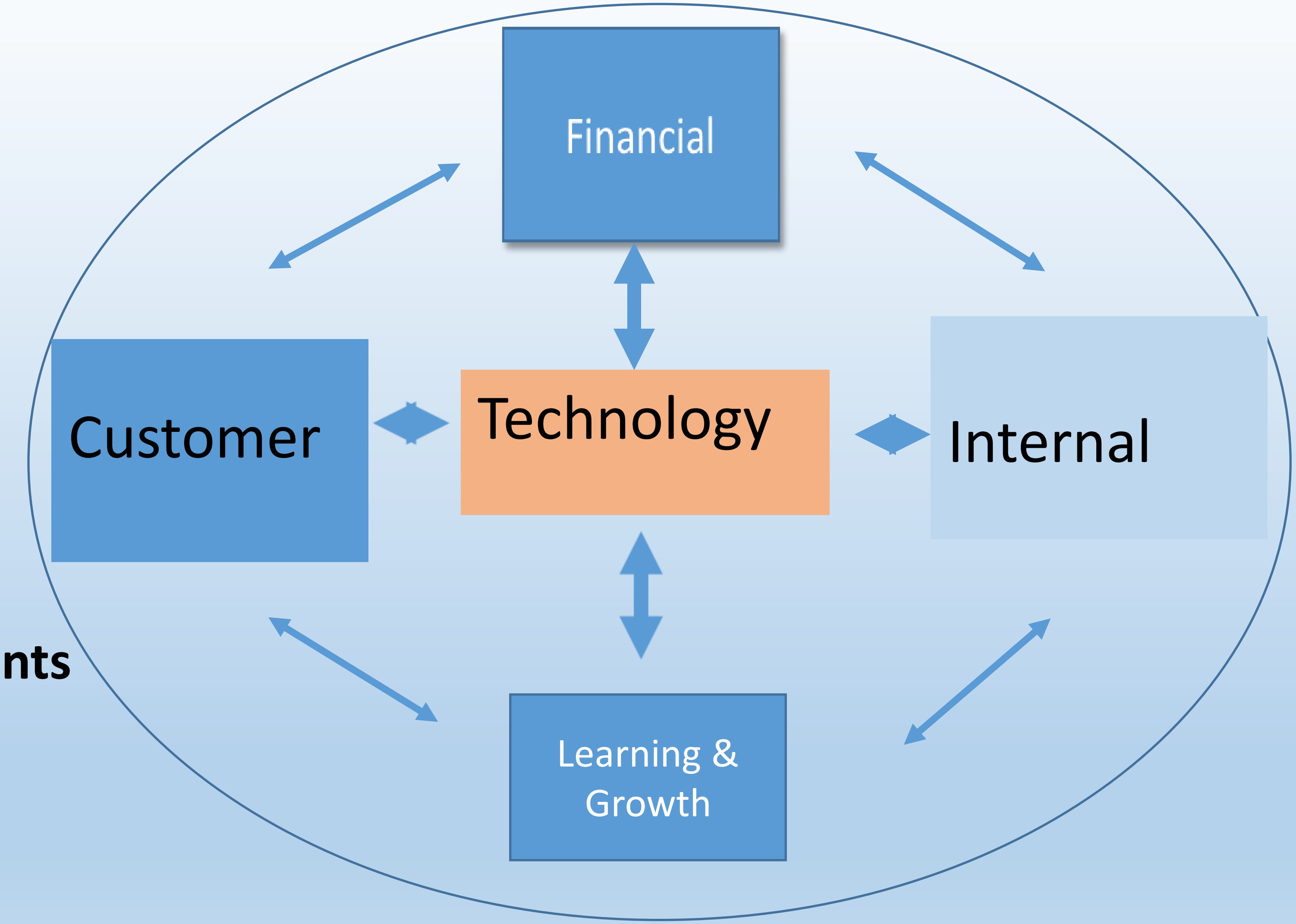
Assumptions

1. Capability and maturity of processes define probability of success
2. Security of operating systems, applications, and databases relies on the ability of software to enforce controls over storage and transfer of information in and between objects
3. State of any IT project can be simulated using a unit vector in Hilbert space
4. Hermitian matrices define probability amplitudes of clearly distinguishable (orthogonal) project states in 3-D Hilbert space

Mathematical Context for Simulation of Medical Devices in Emergency Department

- The last two bullets in slide 2 capture the mathematical basis for the simulation of capability/maturity of projects in Hilbert space.
- Slide 4 depicts the five dimensions of any clinical environment where medical devices are used. The five are: Financial, Internal Governance, Learning and Growth and Customer and Technology.
- The new feature in this simulation is that for mathematical purposes we allow these five dimensions to exist in a five dimensional Hilbert space where every object is described by a complex number. The set of objects in ordinary space is always considered for classical physics; however we use modern physics for this simulation and so every object is a complex number in Hilbert space.
- These same five dimensions are frequently used for strategic planning purposes, and so apply also to any attempt to tactically and strategically improve cyber operations in any networked environment made up of devices.

Strategic Plan for the Real World



Common Elements

Objectives

Metrics

Measurement

Status

Basic Hypothesis for Simulation

- The basic hypothesis is stated in assumption 1 in slide 2, namely, “Capability and maturity of processes define probability of success”.
- Slides 6- 18 provide historical “real world” data to support the basic hypothesis of bullet above.
- Historical data or “prior data” also known as “base rates” is important for Bayesian inference networks. Bayes theorem is used to extend the results of the estimated probabilities for operating at a desired state given an initial state to estimates for cost per story point (Agile) or function point (classical CMMI or waterfall methods).
- This simulation can be used to predict costs of developing medical device systems with given service level agreements for cyber security using Bayesian calibration of the simulator black box (Protracker).

High Cost of Low Performance

- Just 56% of strategic initiatives succeed
- In 2014, $109 million is lost for every $1 Billion invested in projects and programs
- Completion Rates:

High Performing organizations	89%
Low Performing organizations	36%
Projects aligned to org. strategy	71%
Projects misaligned to org. strategy	48%
Agile Org.	69%
Less Agile Org.	45%

Ref: PMI’s Pulse of the Profession: The High Cost of Low Performance, Feb. 2014

More Mature Entities Deliver More Value

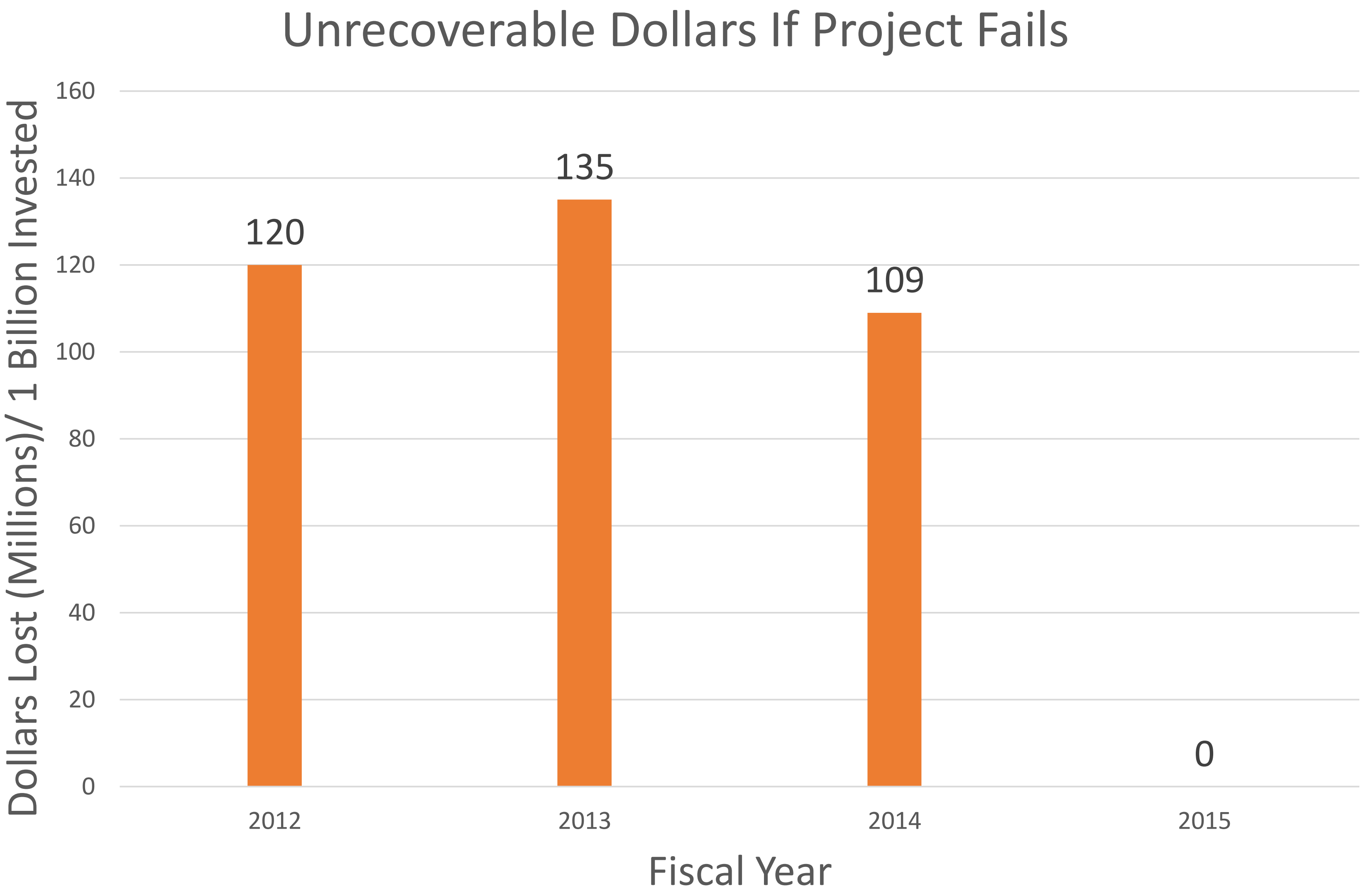
Research on 293 firms in the US, Europe, Central/South America Middle East/Africa and Asia confirms the hypothesis that when organizations improve their project management maturity, they experience

- corresponding gains in project management performance.
- they also show improved organizational performance.

- High Performing Maturity Level: 3.4 Cost Savings: 26%
- Low Performing Maturity Level: 1.7 Cost Savings: 6%

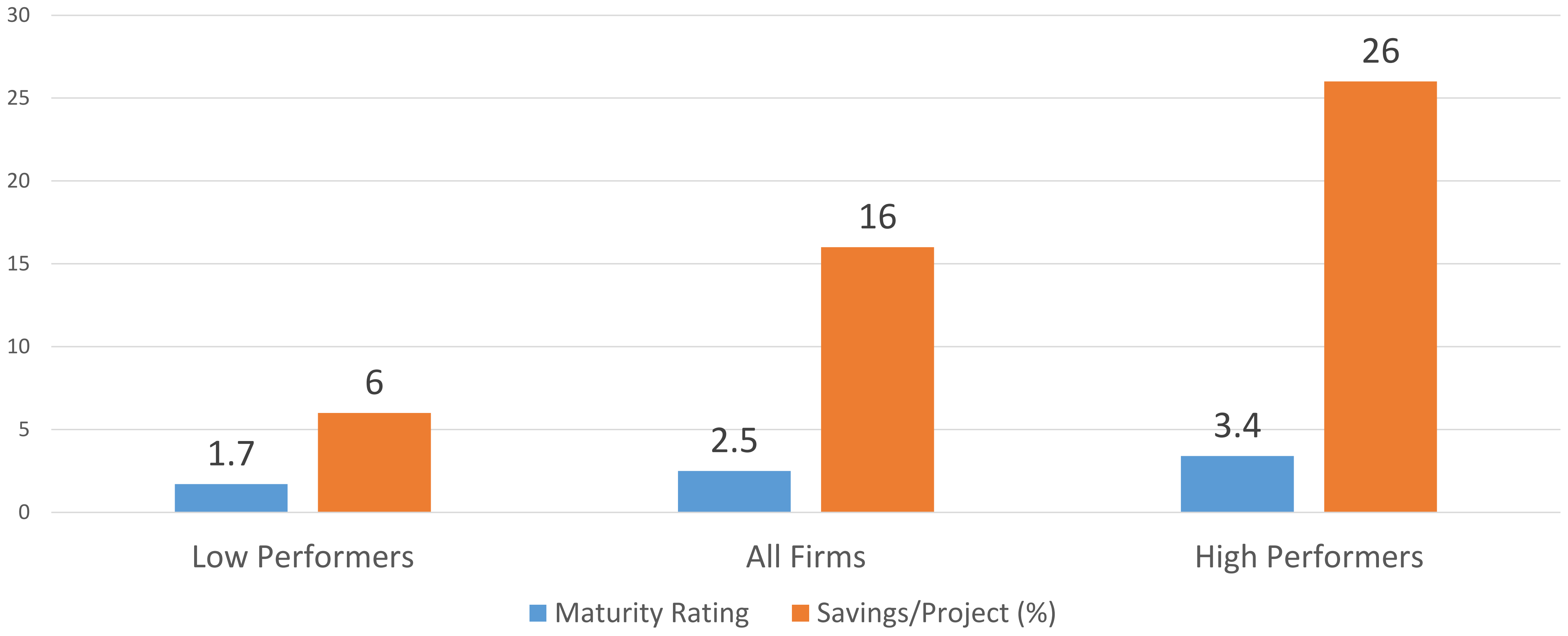
- 11% of 293 were healthcare firms and 5 % in pharmaceuticals

Ref: Project Management Maturity & Value Benchmark, 2014 (PM Solutions Research)



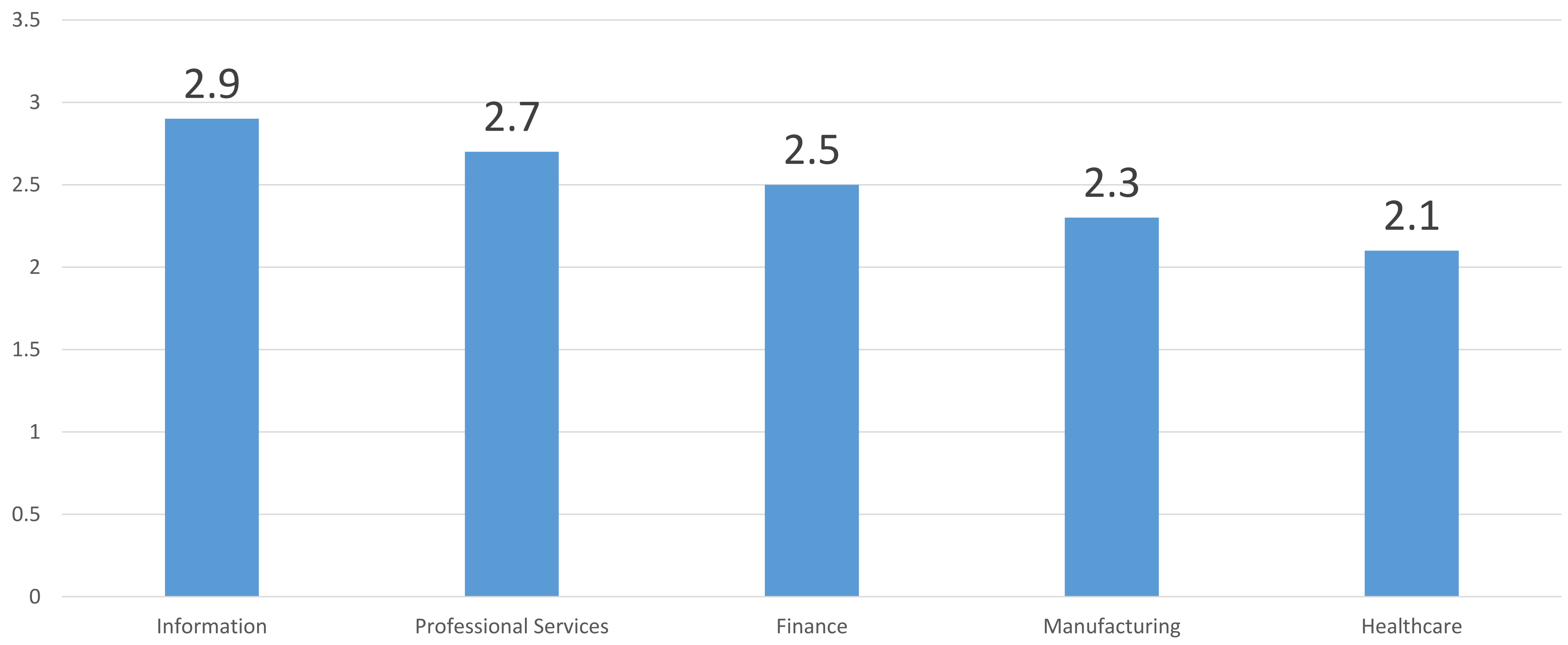
Dollars Lost = (Average %age of projects not meeting goals) (average %age of project budget that is lost if project fails)
Ref: Project Management Maturity & Value Benchmark, 2014 (PM Solutions Research)

Cost Savings Relation to Project Management Maturity



Ref: Project Management Maturity & Value Benchmark, 2014 (PM Solutions Research)

Project Management Maturity in Industries



Ref: Project Management Maturity & Value Benchmark, 2014 (PM Solutions Research)

CMMI De Facto Standard for Process Improvement

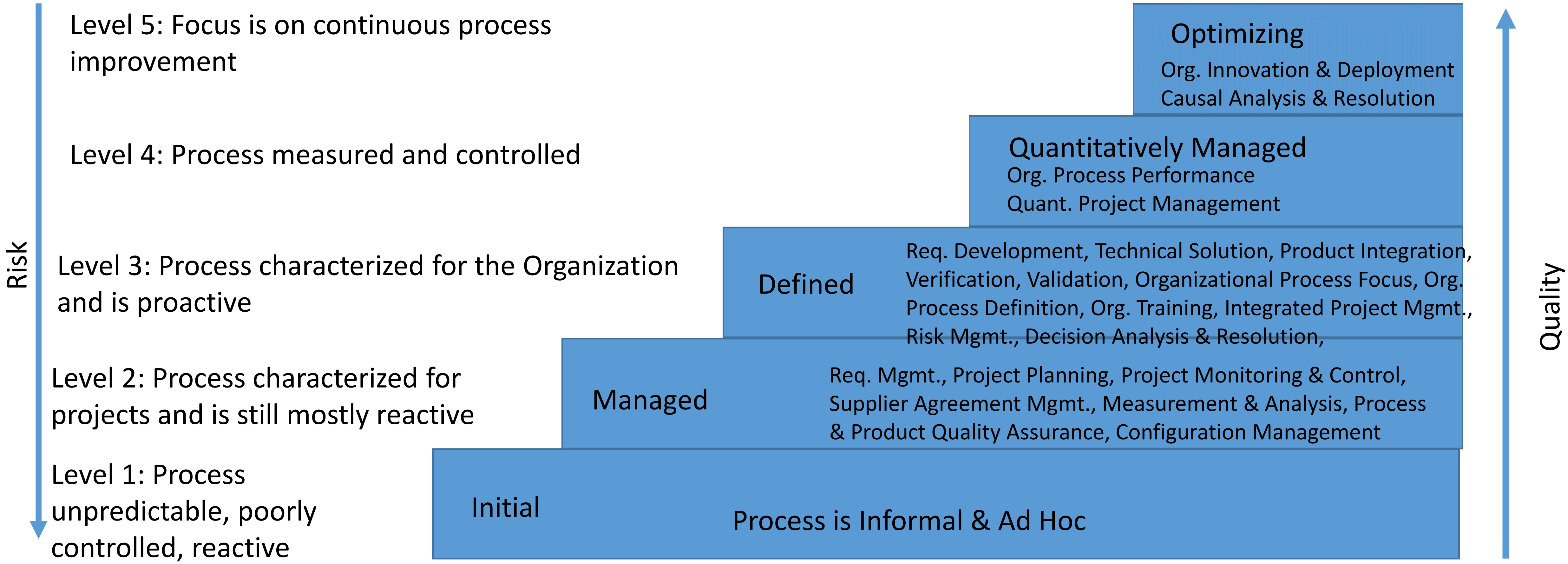
- Thousands of companies across multiple industry sectors across the globe have adopted CMMI:
  - 94 countries (including U.S., China, Germany, Italy, Chile, India, Australia, Egypt, Turkey and Russia….)
  - 12 National Governments and
  - 10 Languages
  - 5000 businesses

Organizations use CMMI to elevate performance

Reference: kpmg.com , CMMI and its potential benefits – Improve Performance, 2015

Capability Maturity Model Integration– Dev (Staged Representation)

Ref: CMMI Institute



Risk

Level 5: Focus is on continuous process improvement

Level 4: Process measured and controlled

Level 3: Process characterized for the Organization and is proactive

Level 2: Process characterized for projects and is still mostly reactive

Level 1: Process unpredictable, poorly controlled, reactive

Optimizing
Org. Innovation & Deployment
Causal Analysis & Resolution

Quantitatively Managed
Org. Process Performance
Quant. Project Management

Defined
Req. Development, Technical Solution, Product Integration, Verification, Validation, Organizational Process Focus, Org. Process Definition, Org. Training, Integrated Project Mgmt., Risk Mgmt., Decision Analysis & Resolution,

Managed
Req. Mgmt., Project Planning, Project Monitoring & Control, Supplier Agreement Mgmt., Measurement & Analysis, Process & Product Quality Assurance, Configuration Management

Initial
Process is Informal & Ad Hoc

Quality

CMMI Success Rates

Benefits of CMMI

- Cost Improvement: 3-87 (n = 29)%
- Schedule: 2-95% (n = 22)
- Productivity: 11-329% (n = 20)
- Quality: 2-132% (n = 34)
- Customer Satisfaction: - 4- 55% (n = 7)
- Return On Investment: 1.7 : 1 – 27.7 : 1 (n=22))

Refer:
University of Missouri - St. Louis
IS6840 - Fall 2008 , Jakrapan Somsakraksanti

Quality Levels of the 5 Levels of the CMMI

For applications of 1000 function points in size

CMMI Level	Defect Potential per FP	Defect Removal Efficiency	Delivered Defects per FP
1	5.25	82 %	0.95
2	5.00	85.00%	0.75
3	4.75	90.00%	0.48
4	4.50	94.00%	0.27
5	4.00	98.00%	0.08

Ref: Capers Jones, Function Points a Universal Software Metric, July 2013, Namcookanalytics.com

Quality Results for CMMI Levels

For applications with 10000 function points

Levels	Defect Potential per FP	Defect Removal Efficiency	Delivered Defects per FP
1	6.50	75.00%	1.63
2	6.25	82.00%	1.13
3	5.50	87.00%	0.72
4	5.25	90.00%	0.53
5	4.50	94.00%	0.27

Ref: Capers Jones, Function Points a a Universal Software Metric, July 2013, Namcookanalytics.com

Six Sigma Formula

- Defects Per Million Opportunities (DPMO) – (Total Defects)/(Total Opportunities) * 1000,000
- Defects (%) = (Total Defects)/ (Total Opportunities) * 100
- Yield (%) = 100 – (Defects Percentage)
- Process Sigma = NORMSINV (1- ((Total Defects)/ (Total Opportunities))) + 1.5
- Or Process Sigma = 0.8406 + SQRT (29.37 – 2.221 * (ln (DPMO)))

- Ref: Breyfogle, F,. 1999, Implementing Six Sigma: Smarter Solutions Using Statistical Methods, 2nd edition, John Wiley & Sons.

Sigma Performance Levels – One to Six Sigma

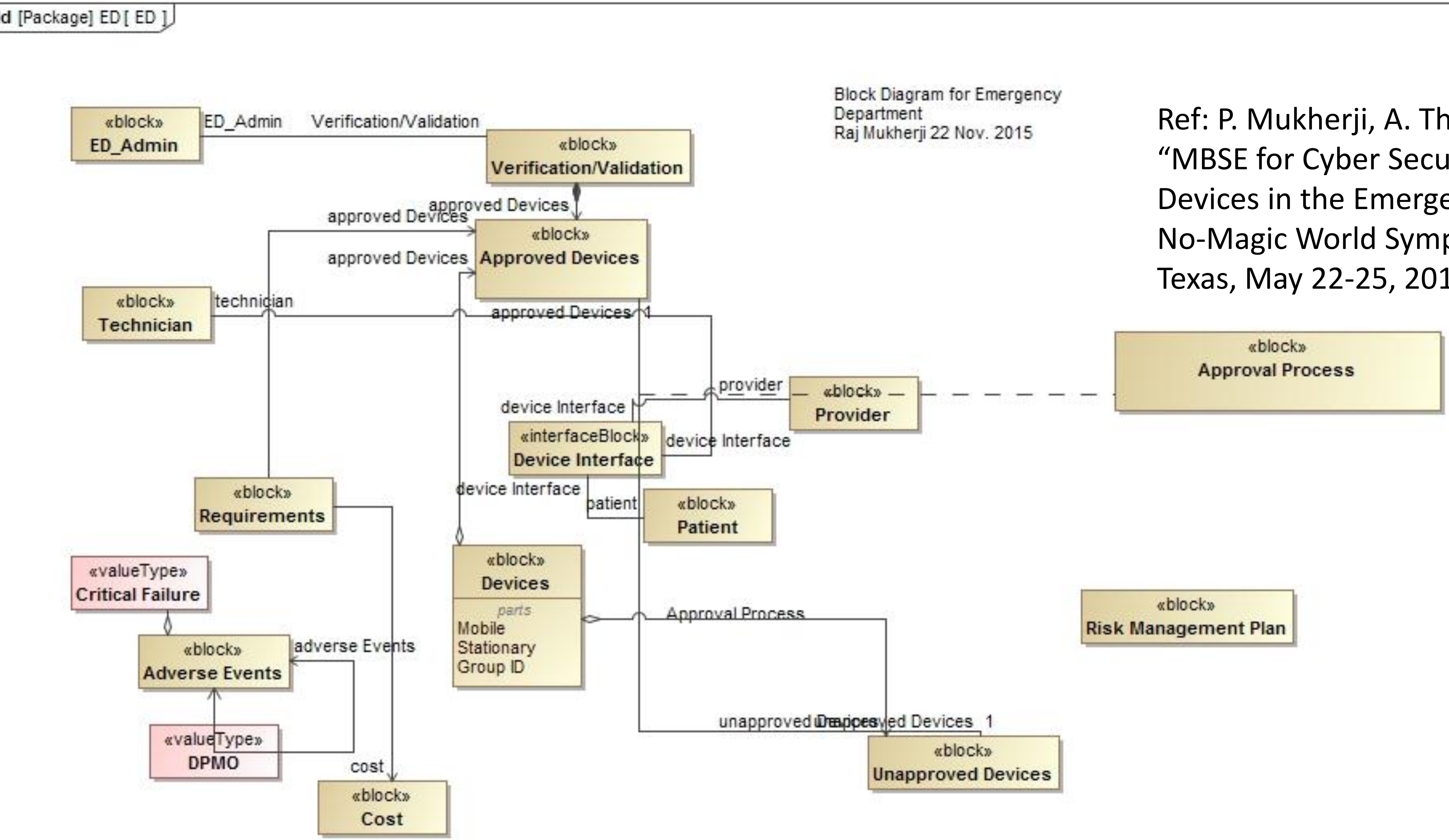
Sigma Level	Defects Per Million Opportunities
1	690,000
2	308, 537
3	66,807
4	6,210
5	233
6	3.4

Ref: isixsigma.com

Real World Examples

Ref: isixsigma.com

Situation/Example	1 Sigma World	3 Sigma World	6 Sigma World
Pieces of your mail lost per year (assuming 1600 opportunities per year)	1,106	107	< 1
Breaches in Medical Devices (assuming 60,000 devices)		150	< 1
Number of empty coffee pots at work (680 opps. per year)	470	45	<1
Number of telephone disconnections (7000 talk minutes)	4839	467	0.02
Erroneous business orders (250,000 opps. per year)	172,924	16,694	0.9

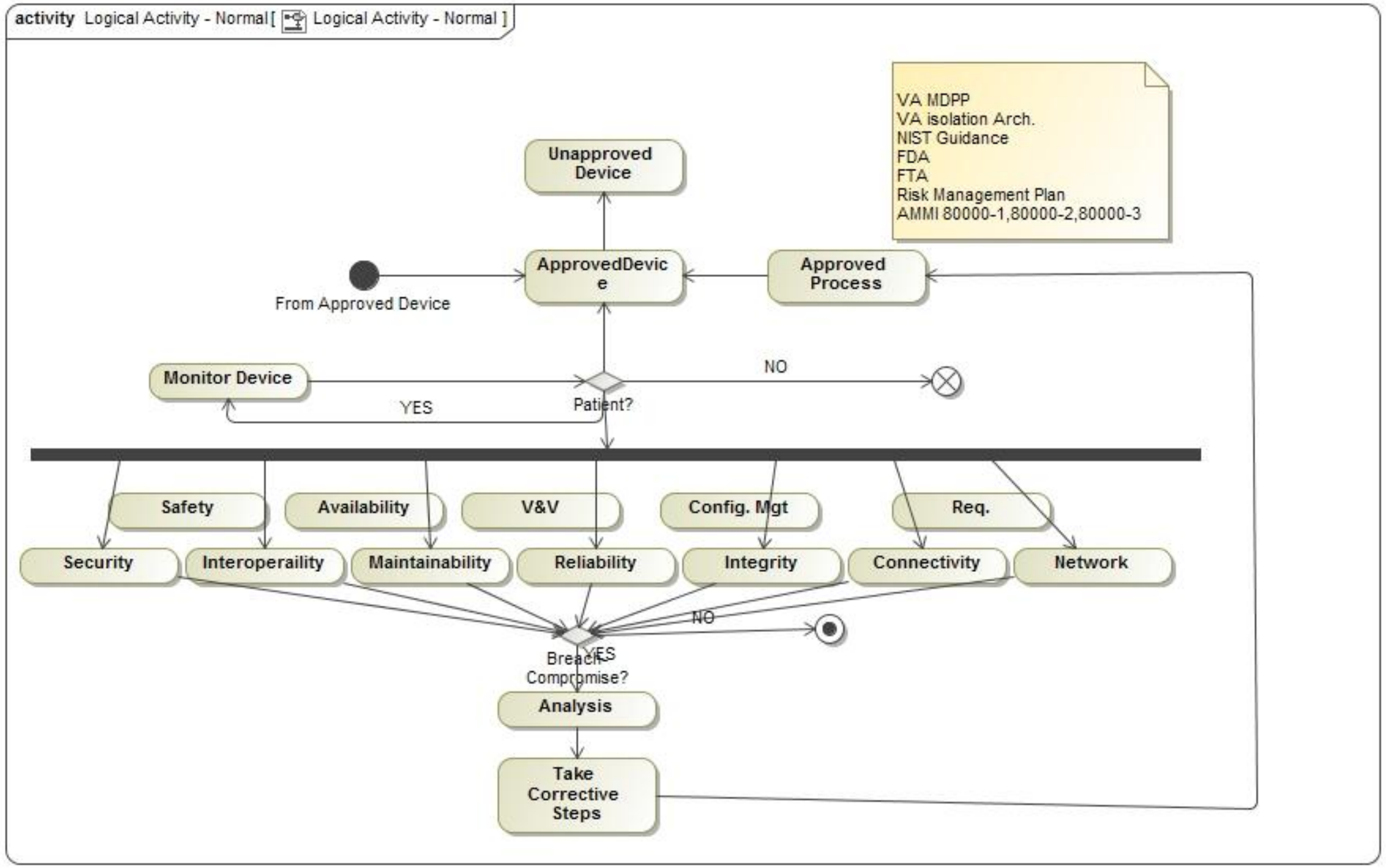


Block Diagram for Emergency
Department
Raj Mukherji 22 Nov. 2015

Ref: P. Mukherji, A. Thukral, V. Thukral, “MBSE for Cyber Security of Medical Devices in the Emergency Department”, No-Magic World Symposium, Allen, Texas, May 22-25, 2016

Logical Activity Diagram

Ref: P. Mukherji, A. Thukral, V. Thukral, “MBSE for Cyber Security of Medical Devices in the Emergency Department”, No-Magic World Symposium, Allen, Texas, May 22-25, 2016



Maturity Models for Cyber Security

A number of security maturity programs use the maturity levels. Examples include:

- Security Awareness Maturity Model – securingthehuman.sans.org
- Security Governance Series – nigesecurityguy.wordpress.com
- Open Web Application Security Project's (OWASP) Chief Information Security Officer Guide, March 2015
- Security Program Maturity – community.hpe.com
- Security Management Maturity Model – EMC2, www.slideshare.net

Open Web App. Security Project (OWASP) Top Ten:

1. **Unvalidated input**: Information from web requests is not validated before being used by a web application. Attackers can use these flaws to attack backend components through a web application.

2. **Broken access control**: Restrictions on what authenticated users are allowed to do are not properly enforced. Attackers can exploit these flaws to access other users' accounts, view sensitive files, or use unauthorized functions.

3. **Broken authentication and session management**: Account credentials and session tokens are not properly protected. Attackers that can compromise passwords, keys, session cookies, or other tokens can defeat authentication restrictions and assume other users' identities.

4. **Cross site scripting (XSS) flaws**: The web application can be used as a mechanism to transport an attack to an end user's browser. A successful attack can disclose the end user's session token, attack the local machine, or spoof content to fool the user.

5. **Buffer overflows**: Web application components in some languages that do not properly validate input can be crashed and, in some cases, used to take control of a process. These components can include CGI, libraries, drivers, and web application server components.

Ref: OWASP Application Guide for Chief Information Security Officers, 2013

Top 10 Continued

6. Improper Error Handling: Error conditions that occur during normal operation are not handled properly. If an attacker can cause errors to occur that the web application does not handle, they can gain detailed system information, deny service, cause security mechanisms to fail, or crash the server.

7. Injection flaws: Web applications pass parameters when they access external systems or the local operating system. If an attacker can embed malicious commands in these parameters, the external system may execute those commands on behalf of the web application.

8. Insecure storage: Web applications frequently use cryptographic functions to protect information and credentials. These functions and the code to integrate them have proven difficult to code properly, frequently resulting in weak protection.

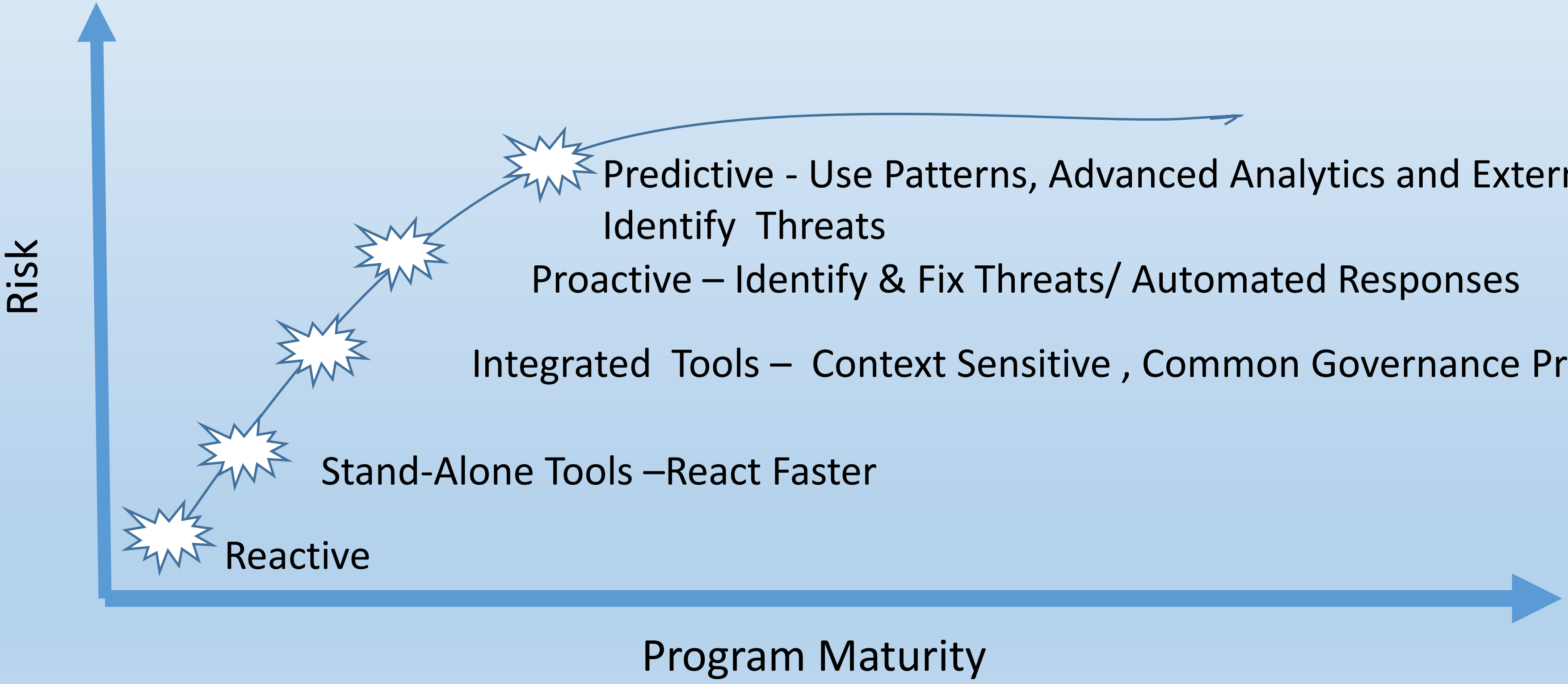
9. Denial of service (DoS) Attackers can consume Web application resources to a point where other legitimate users can no longer access or use the application. Attackers can also lock users out of their accounts or even cause the entire application to fail.

10. Insecure configuration management: Having a strong server configuration standard is critical to a secure web application. These servers have many configuration options that affect security and are not secure out of the box.

Ref: OWASP Application Guide for Chief Information Security Officers, 2013

Security Program Maturity

Ref: community.hpe.com



Predictive - Use Patterns, Advanced Analytics and External/Internal Data to Identify Threats

Proactive – Identify & Fix Threats/ Automated Responses

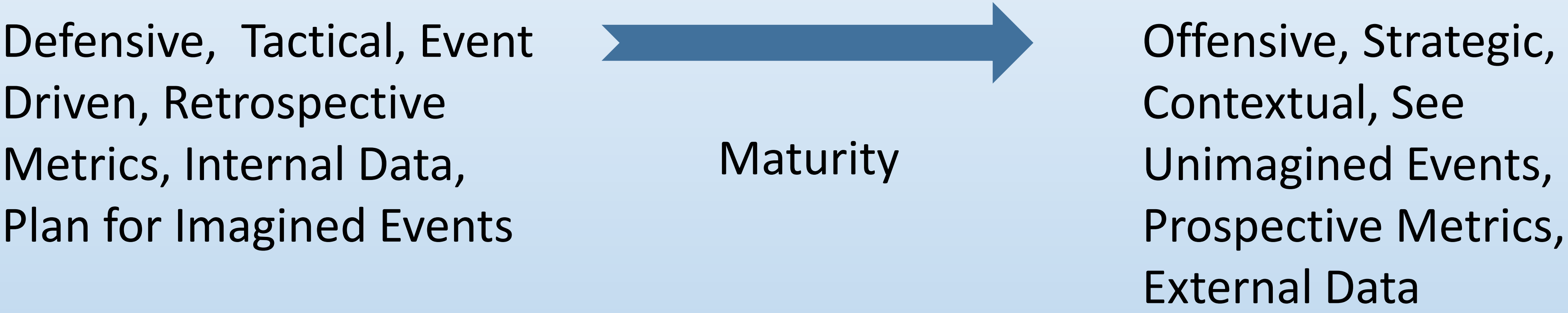
Integrated Tools – Context Sensitive , Common Governance Processes

Stand-Alone Tools –React Faster

Reactive

Security Program Maturity

Ref: community.hpe.com



Defensive, Tactical, Event Driven, Retrospective Metrics, Internal Data, Plan for Imagined Events

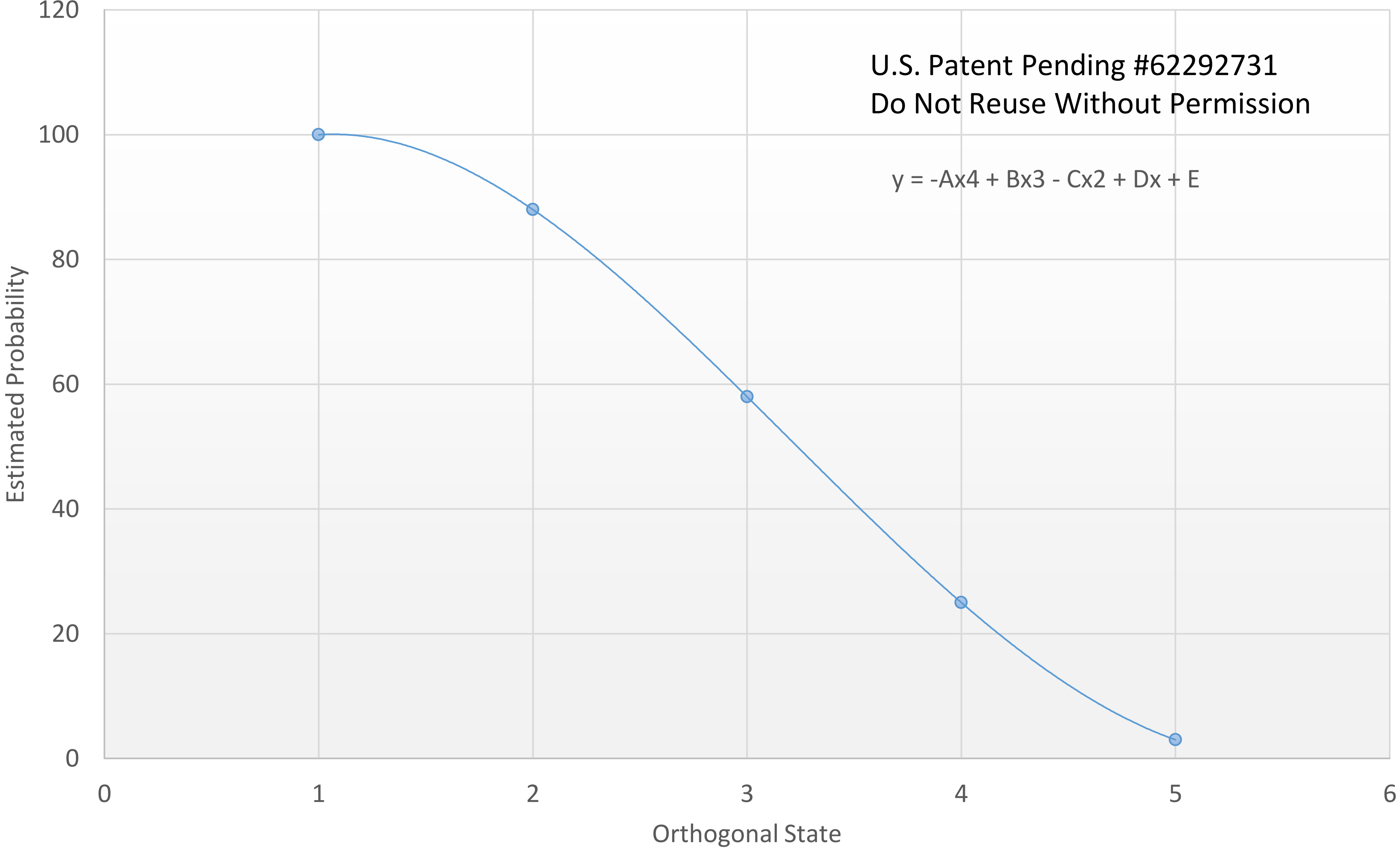
Maturity

Offensive, Strategic, Contextual, See Unimagined Events, Prospective Metrics, External Data

Simulation of Maturity States in CMMI space

- Slides 25 and 26 shows the output from a Simulation of maturity states when applied to cybersecurity for medical devices in an emergency department of any hospital or medical treatment facility.
- The Simulator called "Protracker" takes in input on the existing (current) state of cyber security management processes through a black box GUI and outputs through a GUI estimates of the probability of success for minimizing security breaches using a patented (U.S. Patent Pending # 62292731) interface and method.
- The Simulator Protracker is described in a paper to be submitted for publication in the Journal of Enterprise Transformation in 2016.

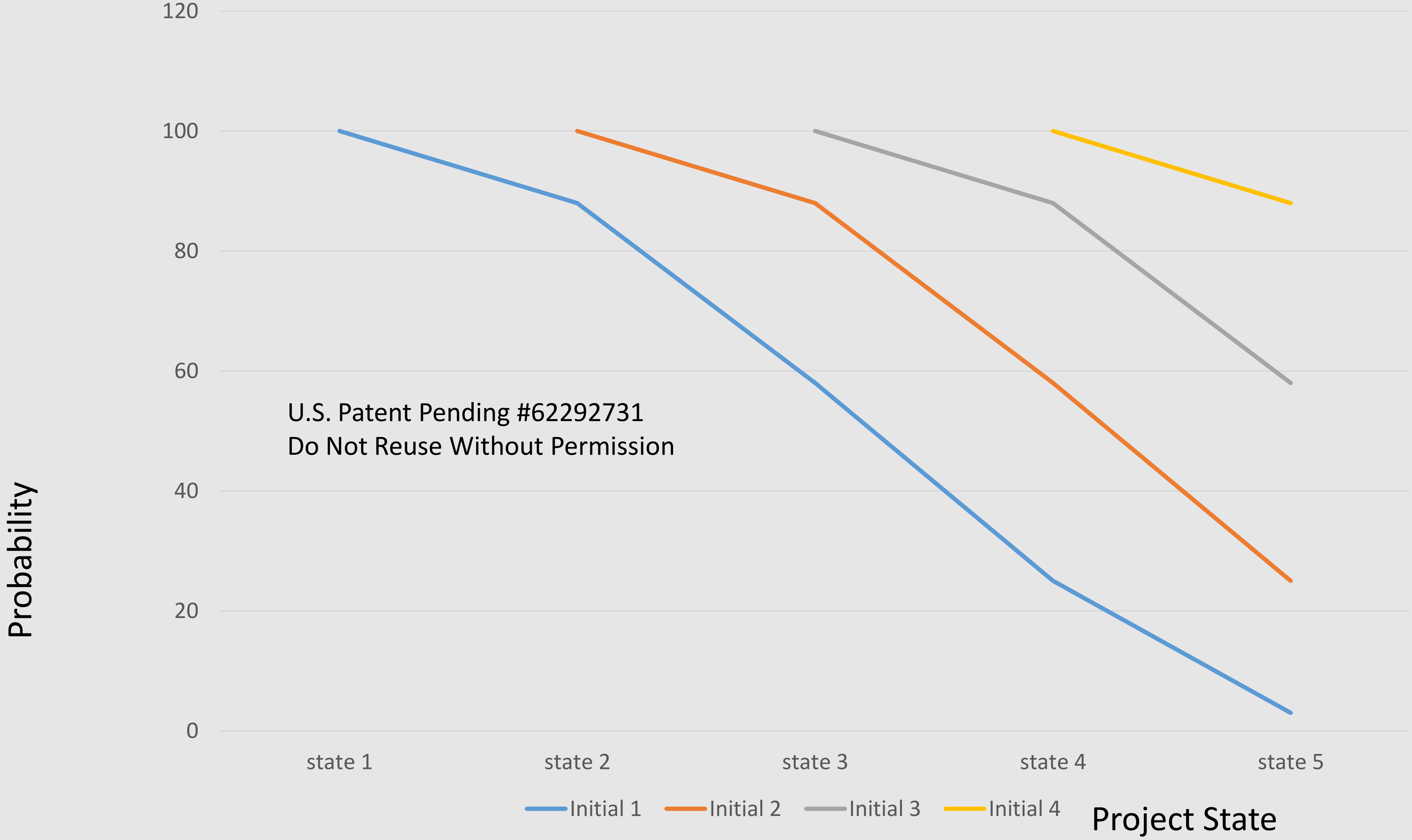
Probability Estimates for Project Management Maturity



U.S. Patent Pending #62292731
Do Not Reuse Without Permission

$y = -Ax4 + Bx3 - Cx2 + Dx + E$

Estimated Probabilities for Project State Transitions



U.S. Patent Pending #62292731
Do Not Reuse Without Permission

Simulation Results

- Shown in slide 27 is the estimated probability of success given maturity level 1 as the initial state. The simulation model assumes five clearly distinguishable (possible) states.
- Simulator Protracker also works for Lean Six Sigma and any other mode such as the Project Management Institute's Maturity Model, Security Governance/Maturity/ Awareness Models (see references on slide 21).
- Results: The probability for successfully minimizing breaches drops off in a 4th order polynomial with distance from state 5 given the initial state of any cybersecurity management process is 1. (US Patent Pending # 62292731)

Simulation Results

- Slide 28 shows the relationships between initial state (starting state) and the probability for successfully minimizing cyber breaches in medical devices.
- Slide 28 shows that with increasing maturity of initial states, the likelihood for success goes up.

- The simulator Protracker is calibrated using historical data and Bayesian inference networks in an “adaptive assessor” software module of the Protracker black box.

Simulation Results

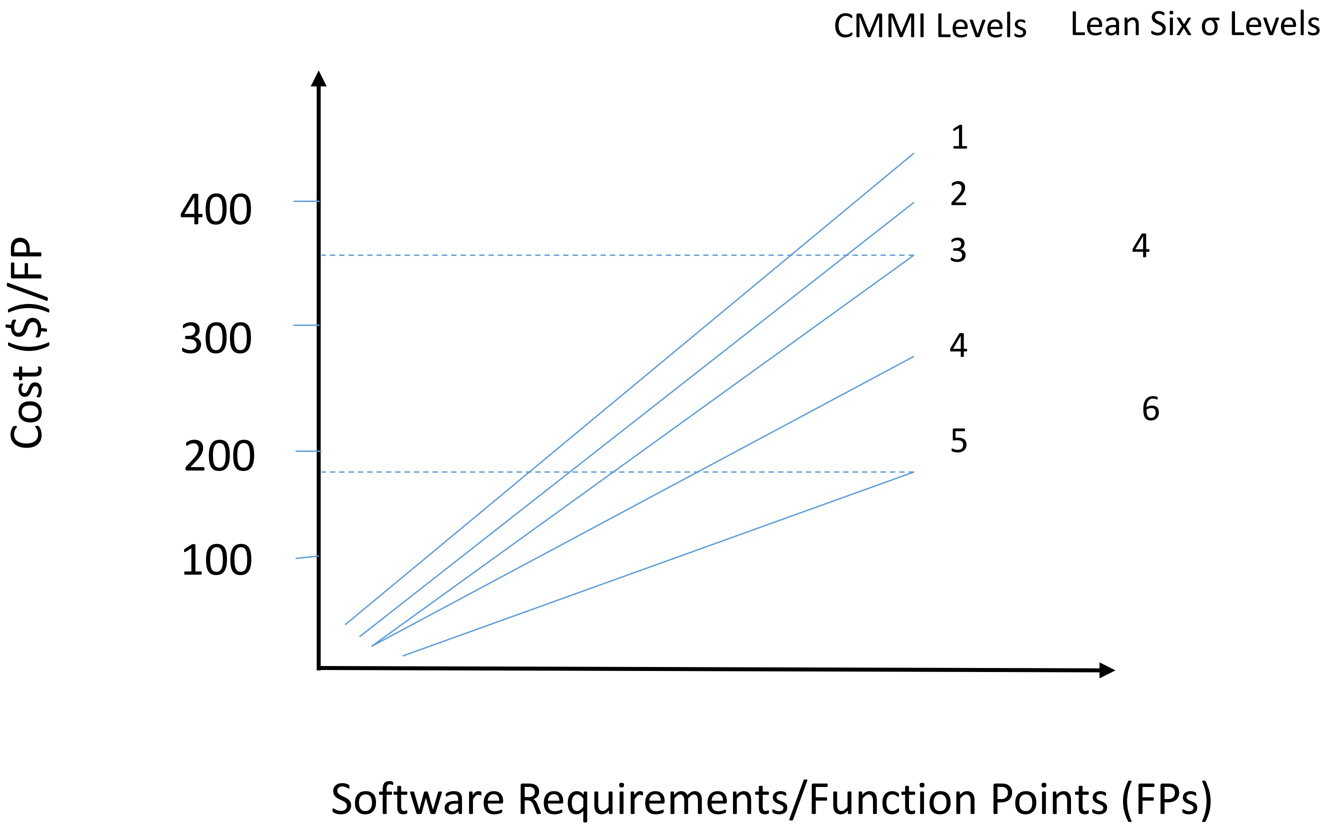
- The Bayesian inference engine ensures that Protracker simulates a real word context for cyber breaches in medical devices by using prior data published or available with the agency performing the improvement effort. So the question of “does it work?” is moot because historical data is used to calibrate the simulator.
- For example, if the starting maturity level is 2, the probability f successfully minimizing breaches (performing at level 5 while remaining at level 2 is shown in slide 26 as 25%.
- Protracker suggests methods for improving this estimated probability (25%) by indicating several options and costs associated with moving the project to a higher initial level of performance.
- For example, if the starting maturity is level 4, then there is an estimated chance of 88% for successfully minimizing breaches.
- For zero cyber breaches, the device must be disconnected from the local or wide area network and no patches or updates to its software can be made after initial testing ensures that malware (trapdoors and backdoors) are absent in storage for the software that operates the device.

Bayesian Inference for Costs

- Slide 33 shows the cost per function point assuming a Bayesian inference network connecting maturity levels and published “historical data” or prior rate for costs per function or story point.
- It is evident from slide 33 that costs per function point or story point may be reduced by as much 100 % if the security governance process maturity can be improved from an average of 2.3 to 5. We believe that a great portion of this return is due to prevention of specific defects (OWASP Top 10 deficiencies for cyber security) during development of the software for the medical devices.
- It is important to note that similar estimates apply for Lean Six Sigma methods for quantifying improvements in metrics such as # of breaches per million opportunities (slide 33, LSS).

Cost per Function Point versus CMMI Levels

Ref: Capers Jones, Namcook Analytics, 13 July, 2013



References

- Slide 6 – PMI’s Pulse of the Profession: The High Cost of Low Performance, Feb. 2014
- Slide 7 - Project Management Maturity & Value Benchmark, PM Solutions Research, 2014
- Slide 8 - Project Management Maturity & Value Benchmark, PM Solutions Research. 2014
- Slide 9 - Project Management Maturity & Value Benchmark, PM Solutions Research. 2014
- Slide 10 - Project Management Maturity & Value Benchmark, PM Solutions Research, 2014
- Slide 11 - kpmg.com , CMMI and its potential benefits – Improve Performance, 2015
- Slide 12 - : Capability Maturity Model Integration Institute
- Slide 13 - Jakrapan Somsakraksanti. University of Missouri - St. Louis IS6840 - Fall 2008
- Slide 14 - Capers Jones, Function Points a Universal Software Metric, Namcookanalytics.com. July 2013
- Slide 15 - Capers Jones, Function Points a Universal Software Metric, Namcookanalytics.com, July 2013
- Slide 16 - Breyfogle, F., Implementing Six Sigma: Smarter Solutions Using Statistical Methods, 2nd edition, John Wiley & Sons, 1999

References

- Slide 17 - isixsigma.com
- Slide 18 - isixsigma.com
- Slide 19 - P. Mukherji, A. Thukral, V. Thukral, "MBSE for Cyber Security of Medical Devices in the Emergency Department", No-Magic World Symposium, Allen, Texas, May 22-25, 2016
- Slide 20 - P. Mukherji, A. Thukral, V. Thukral, "MBSE for Cyber Security of Medical Devices in the Emergency Department", No-Magic World Symposium, Allen, Texas, May 22-25, 2016
- Slide 22 - OWASP Application Guide for Chief Information Security Officers, March 2015
- Slide 23 - OWASP Application Guide for Chief Information Security Officers, March 2015
- Slide 24 - community.hpe.com
- Slide 25 - community.hpe.com
- Slide 27 – P. Mukherji. Mukherji Consulting, U.S. Patent Pending #62292731
- Slide 28 - P. Mukherji. Mukherji Consulting, U.S. Patent Pending #62292731
- Slide 26 - Capers Jones, Function Points a Universal Software Metric, Namcookanalytics.com, July 2013