MANAGING DAILY SECURITY OPERATIONS WITH LEAN AND KANBAN

Gene Kim
IT Revolution Press

Branden R. Williams
HireBranden.com
AGENDA AND OBJECTIVES

- Discuss Lean & Applicability
- Reveal Challenges with the Volume of Work
- Discuss the Three Ways
- Show Transformation Phases
- Drink and be Merry
HOW IS AN IT/IS PERSON’S DAY PRIORITIZED TODAY?
WHERE DOES THIS LEAD US?

- To the hamster wheel of pain and suffering!
The Familiar Problem (Scrub for non-dupes)

- We get dumped on by everyone
- Our work is always late
- We sometimes make promises that we can’t deliver on
- We defer work that we shouldn’t
- No one takes ‘no’ for an answer
- We act before understanding the business
- Business is dissatisfied with our work
THERE MUST BE A BETTER WAY...
Who here is an MBA?
You’ve probably read this!
Introduces Theory of Constraints
Concepts that drive physical factories can drive IT/IS work
  - Lean production in factories can teach us quite a bit about systems and types of work
  - Physical or digital, the concepts apply universally

We have inputs, WIP, and outputs
  - Some of our inputs and outputs may not be tangible (unless printed)

What is WIP?
  - Work In Process, or work that is incomplete
  - It is neither raw materials nor a finished product
  - Ties up input resources and prevents useful outputs from flowing through
  - It’s the gunk in the IT/IS machine!
WHAT IS LEAN?

► Lean is a system that does two things:
  ► Reduce waste
  ► Improve throughput

► Common analogies:
  ► Manufacturing (plants)
  ► Supply chain

► Key differentiator:
  ► PULL system
  ► VISUALIZED work
THE FIRST WAY: SYSTEMS THINKING (L TO R)

- Understand the flow of work
- Always seek to increase flow
- Never unconsciously pass defects downstream
- Never allow local optimization to cause global degradation
- Achieve profound understanding of the system
WHAT IS WORK?

► Inputs:
  ► Dev project reviews
  ► Prep for upcoming audits
  ► Deploy security technologies
  ► Fix audit findings
  ► Migrate from virtual to cloud
  ► Preventive projects to elevate constrain

► WIP:
  ► Unfinished projects
  ► Code changes prior to deploy
  ► Uncommitted changes
WHAT IS WORK? (CONTINUED)

- Outputs
  - Completed projects
  - Services running
  - Audits complete
  - Completed projects
  - Happy customers
EXAMPLE: A TYPICAL TODO LIST

- Prepare budget presentation for exec staff
- Approve change 35133 for Order Entry application
- Pull log files for PCI assessors
- Create report on Microsoft Super Tuesday
- Respond audit findings for SOX audit (OVERDUE)
- Apply firewall rules from last change control meetings
- Review due diligence report from cloud vendor
- Build service catalog for infosec program
- Research new web attack technique: does it affect us?

But wait.... THERE’S MORE!! (duh)
EXAMPLE: A LONGER TYPICAL TODO LIST

- Reach out to new internal auditor
- Think about unified control strategy for compliance (3rd year on TODO list)
- Create appointment with developer, asking to stop avoiding input validation (who is his manager?)
- Find out who owns server TWX-44-9113: is port 9050 really supposed to be open? (TOR?)
- Respond to angry email from Marketing director: privacy regulations aren’t optional (!!)
- Email Sarah: please take me off the physical security alert list
- Read that report from external auditor: can’t TL;DR any more
KANBAN

What is it, and why does it work?
- Created by Taiichi Ohno (Toyota)
- Scheduling board for lean production
- Good: Visualizes work in a system
- Better: Visualizes work FLOW THROUGH a system

Outcomes: WORK GETS DONE!
- Work takes less time to complete (i.e., reduced cycle time, on time!)
- Better tracking of effort and costs
- Find recurring work that we can automate
- Find work where there’s too much time ‘waiting’ or ‘in queue’
- Business gets what they need, when they need it
- Infosec becomes viewed as a reliable partner
SAMPLE KANBAN PROCESS
W/WIP LIMITS

READY
- Write project plan for new automated code deployment
- Review code for Project Hoosegow, Sprint 39

DOING (2)

DONE
WHAT WORK IS REALLY MOST IMPORTANT?

- Top line goals of top executives exist for a reason
  - Does your work align to those goals?
  - Does it help those executives meet those goals?
  - If not, WHY ARE YOU DOING IT?

- Understand where controls exist in the business
  - As the keeper of the IT controls, are you responsible for catching everything?
  - What other controls exist in the business that you can leverage to avoid putting work into the system?
  - Or, even better, if you identify a constraint around another control, can you do work to elevate that constraint for the business?
WORK SHOULD ALWAYS SUPPORT BUSINESS

► Top line goals of top executives exist for a reason
  ► Does your work align to those goals?
  ► Does it help those executives meet those goals?
  ► If not, WHY ARE YOU DOING IT?

► Understand where controls exist in the business
  ► As the keeper of the IT controls, are you responsible for catching everything?
  ► What other controls exist in the business that you can leverage to avoid putting work into the system?
  ► Or, even better, if you identify a constraint around another control, can you do work to elevate that constraint for the business?
Infuriating platitude: “Infosec needs to enable the business”

- Goal: Grow European business by 20% Y/Y
- Response: Because we are good at information security, we can run the business at a lower fraud rate and take on riskier (and more lucrative) business than our competitors

Going from “mythical, consultant-sounding speak” to actions is hard.
SELLING INFOSEC

► Pride before fall, fall before redemption
► Offense is profit center (NFL: scoring points on board; projects)
  ► Steal market share, acquiring companies
  ► Investing in new products (giving budget)
  ► Diversify or enable new channels/markets
► Defense is a cost center
  ► Exclusive use of scarce resource or supply chain resource
  ► Divestig business to protect the core (getting rid of POS system); Business waste
**Performance Measures** | **Area of IT Reliance** | **Business Risk Due to IT** | **IT Controls Relied Upon**
--- | --- | --- | ---
1. Understanding customer needs and wants |  |  |  
2. Product portfolio |  |  |  
3. Time to market (R&D) |  |  |  
4. Sales forecast accuracy |  |  |  
5. Sales pipeline |  |  |  
6. Customer on-time delivery |  |  |  
7. Customer retention |  |  |  
### BUSINESS ALIGNMENT EXAMPLE (CONT.)

<table>
<thead>
<tr>
<th>Performance Measures</th>
<th>Area of IT Reliance</th>
<th>Business Risk Due to IT</th>
<th>IT Controls Relied Upon</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Understanding customer needs and wants</td>
<td>Order entry and inventory management systems</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2. Product portfolio</td>
<td>Order entry systems</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3. Time to market (R&amp;D)</td>
<td>Phoenix</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4. Sales forecast accuracy</td>
<td>(same as #1)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>5. Sales pipeline</td>
<td>CRM, marketing campaign, phone/voicemail, MRP systems</td>
<td></td>
<td></td>
</tr>
<tr>
<td>6. Customer on-time delivery</td>
<td>CRM, phone/voicemail, MRP systems</td>
<td></td>
<td></td>
</tr>
<tr>
<td>7. Customer retention</td>
<td>CRM, customer support systems</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Performance Measures</td>
<td>Area of IT Reliance</td>
<td>Business Risk Due to IT</td>
<td>IT Controls Relied Upon</td>
</tr>
<tr>
<td>-----------------------------------------------------------</td>
<td>--------------------------------</td>
<td>----------------------------------------------------------------------------------------</td>
<td>------------------------</td>
</tr>
<tr>
<td>1. Understanding customer needs and wants</td>
<td>Order entry and inventory management systems</td>
<td>Data not accurate, reports not timely and require rework</td>
<td></td>
</tr>
<tr>
<td>2. Product portfolio</td>
<td>Order entry systems</td>
<td>Data are inaccurate</td>
<td></td>
</tr>
<tr>
<td>3. Time to market (R&amp;D)</td>
<td>Phoenix</td>
<td>three-year cycle time &amp; WIP makes clearing IRR hurdle rate unlikely</td>
<td></td>
</tr>
<tr>
<td>4. Sales forecast accuracy</td>
<td>(same as #1)</td>
<td>(same as #1)</td>
<td></td>
</tr>
<tr>
<td>5. Sales pipeline</td>
<td>CRM, marketing campaign, phone/voicemail, MRP systems</td>
<td>Sales mgmt can’t view/manage pipeline, customers can’t add/change orders</td>
<td></td>
</tr>
<tr>
<td>6. Customer on-time delivery</td>
<td>CRM, phone/voicemail, MRP systems</td>
<td>Customers can’t add/change orders</td>
<td></td>
</tr>
<tr>
<td>7. Customer retention</td>
<td>CRM, customer support systems</td>
<td>Sales cannot manage customer health</td>
<td></td>
</tr>
</tbody>
</table>
### BUSINESS ALIGNMENT EXAMPLE (CONT.)

<table>
<thead>
<tr>
<th>Performance Measures</th>
<th>Area of IT Reliance</th>
<th>Business Risk Due to IT</th>
<th>Controls Relied Upon</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Understanding customer needs and wants</td>
<td>Order entry and inventory management systems</td>
<td>Data not accurate, reports not timely and require rework</td>
<td>Need input validation to prevent bad data from Marketing</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Need weekly reporting capability</td>
</tr>
<tr>
<td>2. Product portfolio</td>
<td>Order entry systems</td>
<td>Data are inaccurate</td>
<td>Need testing of automated controls to ensure integrity of data</td>
</tr>
<tr>
<td>3. Time to market (R&amp;D)</td>
<td>Phoenix</td>
<td>three-year cycle time &amp; WIP makes clearing IRR hurdle rate unlikely</td>
<td>Need better review of new projects to ensure business goals achievement likely</td>
</tr>
<tr>
<td>4. Sales forecast accuracy</td>
<td>(same as #1)</td>
<td>(same as #1)</td>
<td></td>
</tr>
<tr>
<td>5. Sales pipeline</td>
<td>CRM, marketing campaign, phone/voicemail, MRP systems</td>
<td>Sales mgmt can’t view/manage pipeline, customers can’t add/change orders</td>
<td>Need better change and configuration controls around app and environment</td>
</tr>
<tr>
<td>6. Customer on-time delivery</td>
<td>CRM, phone/voicemail, MRP systems</td>
<td>Customers can’t add/change orders</td>
<td>Loosen report controls to allow managers to add/modify reports</td>
</tr>
<tr>
<td>7. Customer retention</td>
<td>CRM, customer support systems</td>
<td>Sales cannot manage customer health</td>
<td>Change control &amp; sec reviews to ensure uptime</td>
</tr>
</tbody>
</table>
Exercise: Compare

- Resulting infosec program

- Vs. Typical Infosec program
  - Respond to audits
  - Prepare for audits
  - Convince IT Operations to implement patches
THE SECOND WAY: AMPLIFY FEEDBACK LOOPS (R TO L)

► Understand and respond to the needs of all customers, internal and external
► Shorten and amplify all feedback loops: stop the line when necessary
► Create quality at the source
► Create and embed knowledge where we need it
THE TWITTER INFOSEC PROGRAM

Manual security workflow

1. Run tool
2. Wait for it...
3. Interpret reports
4. Fix stuff

Repeat

#appsecusa #sadb
@silematodie | @alsmola | @presidentbeef
WHAT THE TWITTER INFOSEC TEAM DID

- They integrated brakeman into the Dev continuous integration process
- It does static code analysis upon ‘code commit’ or even ‘developer save’
- It emails them whenever a vulnerability is found, along with instructions on how to fix it
- It sends them a congratulation email when the developer fixes the vulnerability
STATIC CODE ANALYSIS EARLY

Brakeman can run anytime


Save Code

#appsecusa #sacb
@nilematofle | @aismola | @presidentbeef
OUTCOMES

- Developers get immediate feedback: issues are found and fixed earlier
- We’ve encoded our expertise into the automated testing framework
- We’ve reduced our workload
THE THIRD WAY: CONTINUAL EXPERIMENTATION

- Foster a culture that rewards:
  - Experimentation (taking risks) and learning from failure
  - Repetition is the prerequisite to mastery

- Why?
  - You need a culture that keeps pushing into the danger zone
  - And have the habits that enable you to survive in the danger zone
WHOOPS!

Amazon EC2 outage downs Reddit, Quora

The sky is falling! Amazon's cloud seems to be down (raining?) so we're experiencing some issues too. Be back soon!

5 hours ago via web

Retweeted by RealAmandaStone and others

SCVNGR and other sites took to Twitter after a rare and major outage of Amazon's cloud-based Web service.

By Julianna Pepitone, staff reporter April 22, 2011: 7:26 AM ET

NEW YORK (CNNMoney) -- A rare and major outage of Amazon's cloud-based Web service on Thursday took down a plethora of other online sites, including Reddit, HootSuite, Foursquare and Quora.
INJECT FAILURES OFTEN

The Netflix Tech Blog

5 Lessons We’ve Learned Using AWS

We’ve sometimes referred to the Netflix software architecture in AWS as our Rambo Architecture. Each system has to be able to succeed, no matter what, even all on its own. We’re designing each distributed system to expect and tolerate failure from other systems on which it depends.

One of the first systems our engineers built in AWS is called the Chaos Monkey. The Chaos Monkey’s job is to randomly kill instances and services within our architecture. If we aren’t constantly testing our ability to succeed despite failure, then it isn’t likely to work when it matters most – in the event of an unexpected outage.
YOU DON’T CHOOSE
CHAOS MONKEY…

Chaos Monkey
Chooses You!
Defects and vulnerabilities are fixed faster than ever
Surface area of risk keeps shrinking
Infosec activities integrated into the daily work of Dev and IT Operations
Technical debt is finally paid down
Information security risk has been reduced
Infosec recognized as helping the business win
More budget and staff given to infosec
THE PHOENIX PROJECT

The Phoenix Project
A Novel About IT, DevOps, and Helping Your Business Win

Gene Kim, Kevin Behr and George Spafford
QUESTIONS?

Gene Kim
@realgenekim

Branden R. Williams
@brandenwilliams
http://hirebranden.com
# Starting With The Business Goals

## The KRI Catalog

<table>
<thead>
<tr>
<th>Business Aspect</th>
<th>Outcomes</th>
<th>Key Risk Indicators</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Demand Management</strong></td>
<td>Market Responsiveness</td>
<td>Channel Costs</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Marketing</td>
</tr>
<tr>
<td></td>
<td>Sales Effectiveness</td>
<td>Lost Sales</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Forecast Inaccuracy</td>
</tr>
<tr>
<td></td>
<td>Product Development Effectiveness</td>
<td>Product Management</td>
</tr>
<tr>
<td></td>
<td></td>
<td>R&amp;D Failure</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Aging Products</td>
</tr>
<tr>
<td><strong>Supply Management</strong></td>
<td>Customer Responsiveness</td>
<td>Service Performance</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Privacy</td>
</tr>
<tr>
<td></td>
<td>Agreement Effectiveness</td>
<td>Returns</td>
</tr>
<tr>
<td></td>
<td>Supplier Effectiveness</td>
<td>Customer Care Failure</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Order Fill Failures</td>
</tr>
<tr>
<td></td>
<td>Risk Management</td>
<td>Enterprise Sourcing</td>
</tr>
<tr>
<td></td>
<td>Asset Management</td>
<td>Supply Chain Planning</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Vendor Risk Management</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Supplier Agreement Effectiveness</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Supplier Service Performance</td>
</tr>
<tr>
<td><strong>Support Services</strong></td>
<td>Human Resources Responsiveness</td>
<td>IT Workforce</td>
</tr>
<tr>
<td></td>
<td>Information Technology Responsiveness</td>
<td>Skills Inventory</td>
</tr>
<tr>
<td></td>
<td>Change Management</td>
<td>Infrastructure and Operations</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Information Security</td>
</tr>
<tr>
<td></td>
<td>Finance and Regulatory Responsiveness</td>
<td>Compliance</td>
</tr>
<tr>
<td></td>
<td></td>
<td>E-Discovery</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Environmental, Health and Safety</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Internal Audit (Finance)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Records Management</td>
</tr>
<tr>
<td><strong>RSACONFERENCE 2013</strong></td>
<td>Gartner</td>
<td></td>
</tr>
</tbody>
</table>
GARTNER RISK-ADJUSTED VALUE MGMT

► Contact Paul Proctor, Chief of Research, Risk and Security, Gartner, Inc. (mailto:paul.proctor@gartner.com)

► Or your Gartner rep
THANK YOU!