MANAGING DAILY SECURITY OPERATIONS WITH LEAN AND KANBAN

Branden R. Williams (@BrandenWilliams)
EVP, Sysnet Global Solutions

RSA CONFERENCE EUROPE 2013

Session ID: GRC-T01A

Session Classification: General Interest

AGENDA AND OBJECTIVES

- Discuss Lean & Applicability
- Reveal Challenges with the Volume of Work
- Show Kanban and why it works
- Drink and be Merry

HOW IS AN IT/IS PERSON'S DAY PRIORITIZED TODAY?

#RSAC

RSA CONFERENCE EUROPE 2013

1: THE BIGGEST FIRE

2: THE LOUDEST EXECUTIVE

WHERE DOES THIS LEAD US?

- To the hamster wheel of pain and suffering!

The Familiar Problem

- 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

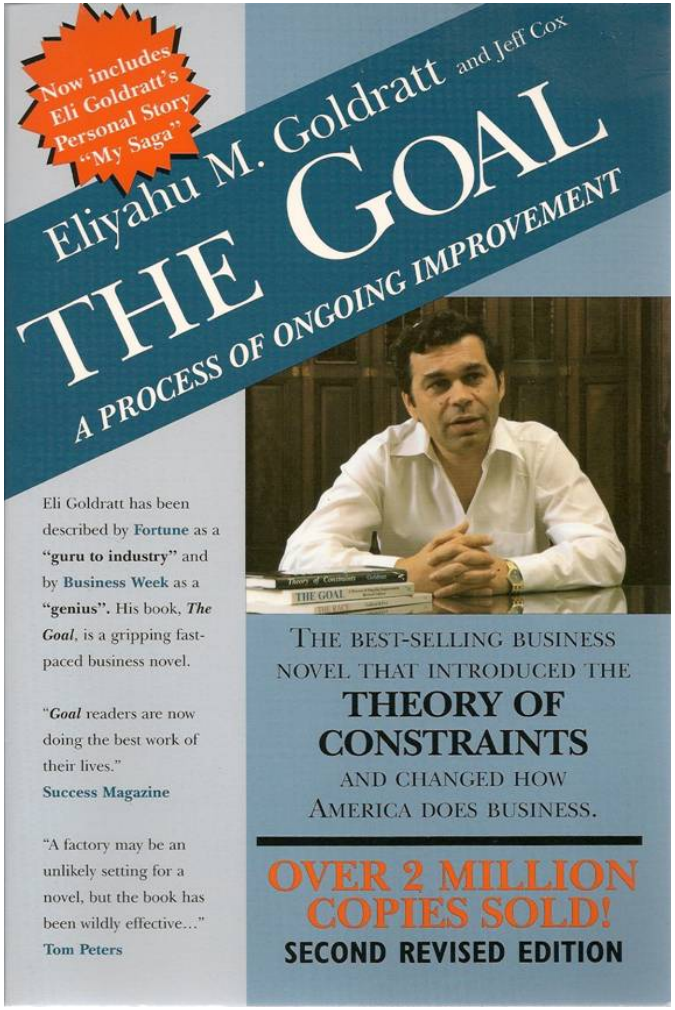
THERE MUST BE A BETTER WAY. . .

#RSAC

RSA CONFERENCE EUROPE 2013

THE GOAL, DR. ELIYAHU M. GOLDRATT

- Who here is an MBA?
- You've probably read this!
- Introduces Theory of Constraints



IT SECURITY IS AN ELECTRONIC FACTORY

- 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

SYSTEMS THINKING

- 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 constraint
- 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

But wait....
THERE'S
MORE!! (duh)

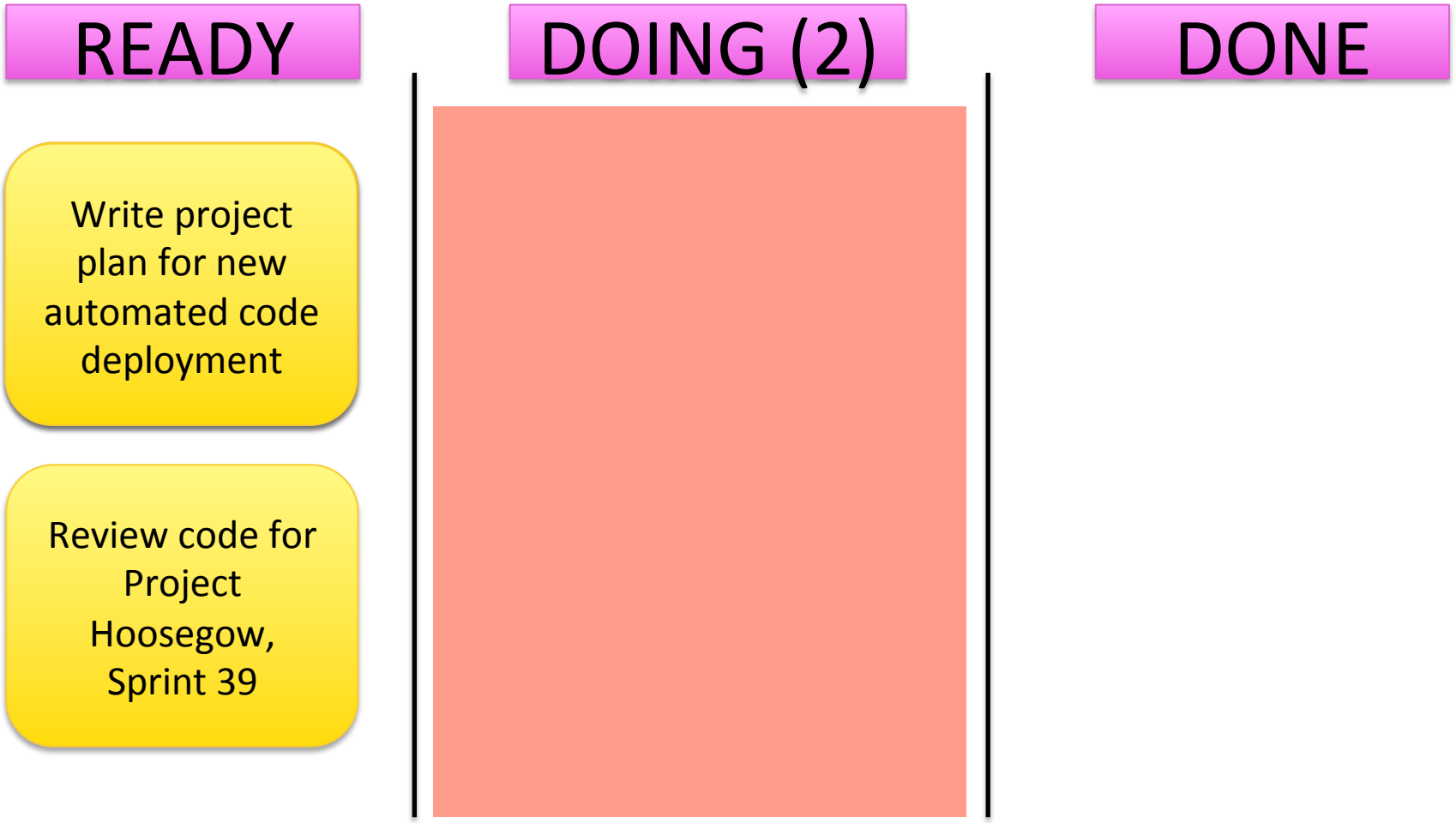
EXAMPLE: A LONGER TYPICAL TODO LIST

- ❑ 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?
  - Popularized 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



WHY DOES KANBAN WORK?

- Work visualization is POWERFUL
  - Most teams don't have good ways to see all of the work in a system
  - It's easier when you are looking at a plant, harder when dealing with knowledge work
- Work taken out of the system is as important as work put into the system.
  - Saying no signals capacity
  - Forces re-alignment with business objectives

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?

USE CASE FOR KANBAN

- Managing Audit Findings
  - Which ones are a priority? (aligned with biz objectives)
  - How do we report commitments up? (visualize flow)
  - How do we take work out of the system? (don't overcommit)
- Latest audit finding generates massive remediation
- With Lean & Kanban you will:
  - Visualize the current backlog
  - Work around the constraint (your one key resource)
  - Understand what backlog impacts audit finding
  - Automate where possible
  - Potentially make other adjustments to reduce workload

USE CASE FOR KANBAN (2)

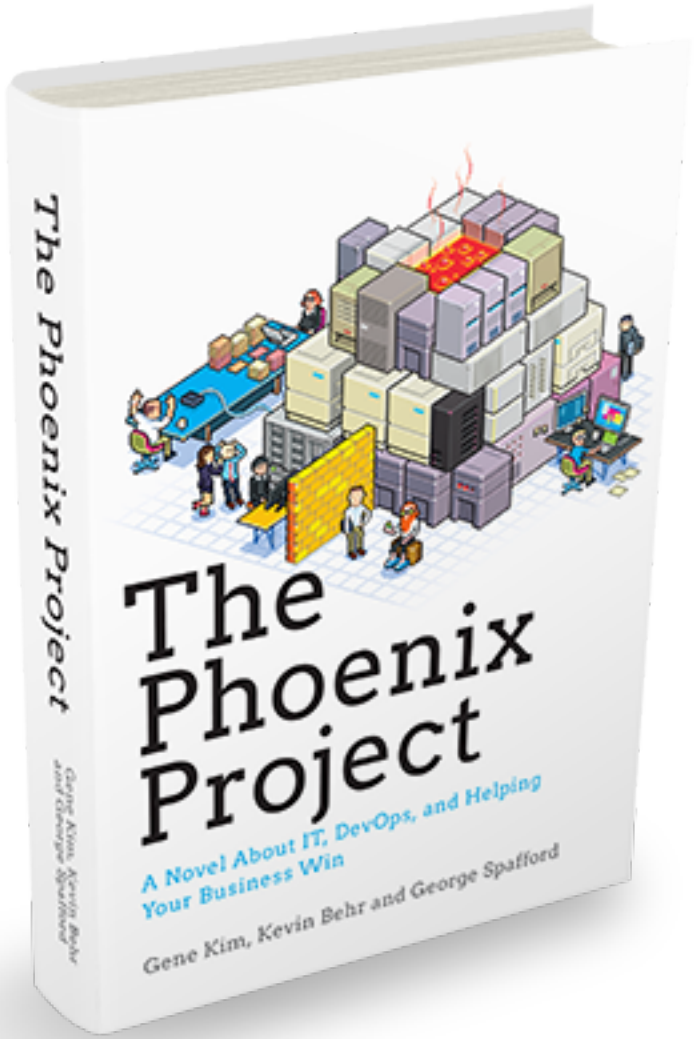
- Code Deploys
  - Ensuring broken code does not end up in production (auto-test/TDD)
  - Reduce cycle time for frequent deploys (Agile)
  - Ensure compliance with stds remains intact (system-driven)
- New feature proposed that impacts user experience
- With Lean & Kanban you will:
  - Build out workflow (IT is a factory)
  - Visualize work in process
  - Automate around your constraint (uptime?)
  - Ensure IT process flows include security checks (automated gates)

WHERE CAN I LEARN MORE?

#RSAC

RSA CONFERENCE EUROPE 2013

THE PHOENIX PROJECT*



RESOURCES

- Gartner Risk-Adjusted Value Management
  - Contact Paul Proctor, Chief of Research, Risk and Security, Gartner, Inc. (paul.proctor@gartner.com) – Or your Gartner rep
- Leankit.com
  - FREE Kanban board system, with iFunctionality
- Personal Kanban
  - By Jim Benson and Tonianne DeMaria Barry, Personalkanban.com
- Kanban (tougher reading, but treats enterprise problems)
  - By David J Anderson

Starting With The Business Goals

The KRI Catalog

Business Aspect	Outcomes	Key Risk Indicators				
Demand Management	Market Responsiveness	Channel Costs	Marketing	On-line reputation	Transparency	
	Sales Effectiveness	Lost Sales	Forecast Inaccuracy	Lost Customers		
	Product Development Effectiveness	Product Management	R&D Failure	Aging Products		
Supply Management	Customer Responsiveness	Service Performance	Privacy	Returns	Material Quality	Late Delivery
		Agreement Effectiveness	Customer Care Failure	Order Fill Failures	Service Inaccuracy	
	Supplier Effectiveness	Enterprise Sourcing	Supply Chain Planning	Vendor Risk Management	Supplier Agreement Effectiveness	Supplier Service Performance
	Operational Efficiency	Risk Management	Strategic Planning	Internal Controls	Quality Management	
		Asset Management	Business Continuity Management	Facilities Management	Manufacturing	
Support Services	Human Resources Responsiveness	IT Workforce	Skills Inventory	Identity and Access Management	Training	
	Information Technology Responsiveness	Applications	Infrastructure and Operations	Information Security	IT Investment	Service Level Effectiveness
		Change Management	Cloud	Project and Portfolio Management	Availability	Internal Audit (IT)
	Finance and Regulatory Responsiveness	Compliance	E-Discovery	Environmental, Health and Safety	Internal Audit (Finance)	Records Management
		Governance	Insurance	Ethics	Financial Integrity	
		Legal	Liquidity	Policies	Sustainability	

Gartner

Questions?

@BrandenWilliams
BrandenWilliams.com

#RSAC

RSA CONFERENCE EUROPE 2013

Thank you!

#RSAC

RSA CONFERENCE EUROPE 2013