Lean Security….
….can it be done?

Can it help us to change and be more successful?

Jaap Halfweeg

November 2012

ISF World Congress Chicago

Information Security Forum

Content

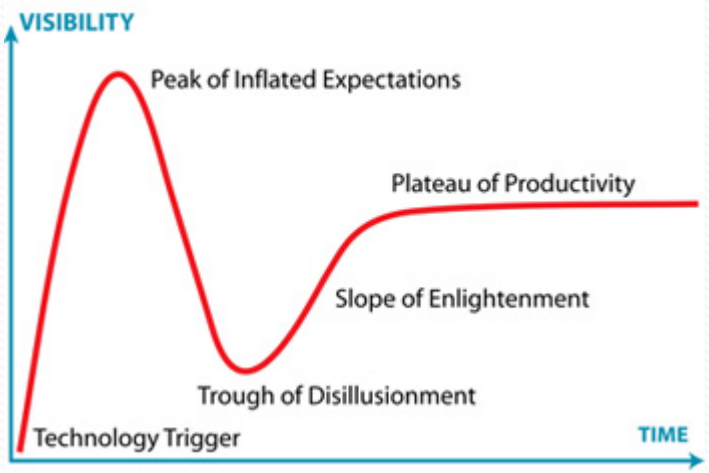
- Why a change?
- The Lean Philosophy
- Mapping Lean on Information Security Management
- “The Lean Security Management System”
- Conclusion

Note : I am not presenting the opinion of KPN. It’s is my personal view and that of a few (former) colleagues with whom we have discussed this topic extensively.

Why is change needed?

For some reason we still haven't got where want to be (at least most of us)

- **<u>Urgent need for Security effectiveness</u>**
  - In a very dynamic context. Can we follow the pace of change?
  - The need for speed. And ever increasing b
  - 'Continuous in control'; is a must
- **<u>What do we need?:</u>**
  - a faster PDCA-cycle (or none)?
  - bring more value (meaning…)?
  - a simpler approach?
  - **when is secure, secure enough?**
- **<u>Doing more with less, means…</u>**
  - Doing the **right things**, the **right way**, at the **right time**
  - And **stop wasting** resources on wrong things!



Where are we?

The Lean Philosophy

The lean principles began in Manufacturing environments (Toyota/Ford) Its a way of thinking, a Philosophy.

- Definition of Lean;

  "A systematic approach to identifying and eliminating waste through continuous improvement, following the product at the pull of the customer in pursuit of perfection".

- In short:

  "Do what the customer wants (to pay for) and consider the rest as potential waste".

- Lean manufacturing in turn evolved into:
  - Lean Services, Lean Project Management, Lean IT …

- **Why not Lean Security?**

The five-steps process of Lean

1. Identify **value** for the end **customer**
2. **Map** all the steps in the **value stream** and eliminate steps that do not create value (**waste**).
3. Tight the sequence of the value-creating steps so the flow is smooth
4. Let customers **pull** value from the next upstream activity.
5. Begin the process again and continue **improving** until a **state of perfection** is reached in which perfect value is created with no waste

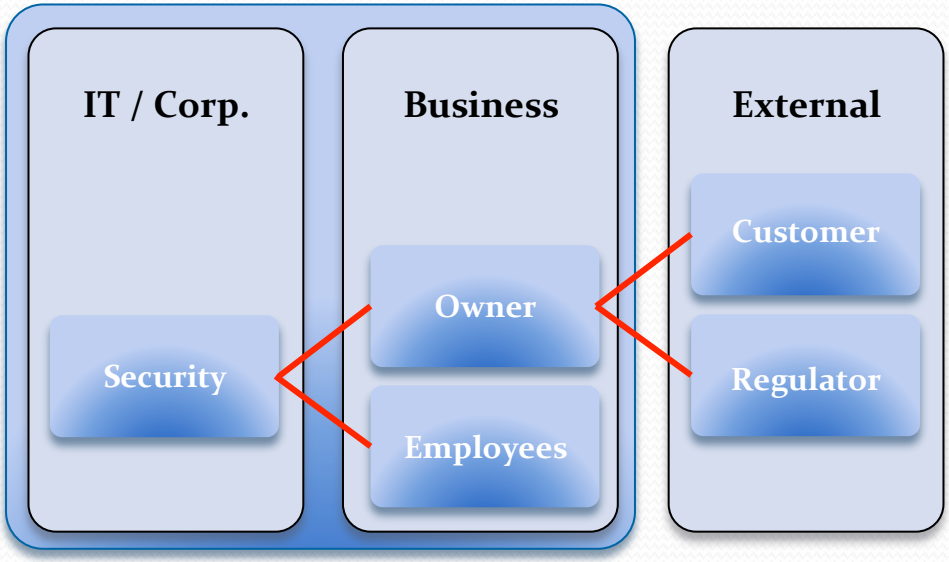
Defining Lean Information Security

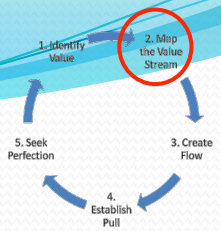
What is "value" and "waste" in Security?

Value	Efficient and agile security management	Adequately managed security risk	Usable and efficient controls
Waste	Cumbersome, rigid security management	Unnecessary, inadequate or missing controls	User unfriendly or inefficient controls

The five steps in Lean & Information Security

1. **<u>Identify value:</u>** – (value for the 'customer'):
   - Who really is our Customer?
   - Do you understand where the value is created in the Business?
   - What needs to be protected and secured?
   - What is the opinion of Business Management about the value?
   - ....

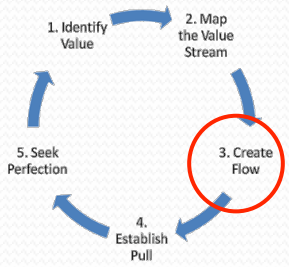




2. Map the value stream: - (reduce waste)

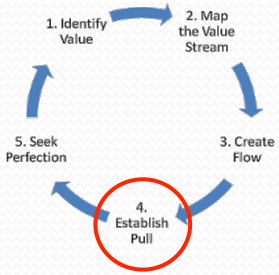
Type	Some examples	Business Outcome
Overproduction	Unnecessary security controls due to lacking risk appetite, liability culture or mindless following of standards. Over collection of system logs.	Unnecessary high cost and waste of resources
Defects	Unmonitored or poorly configured IPS/IDS, Inadequate paper controls just to survive audits, Too low a threshold in the deviation process	False sense of confidence under high costs
Unclear communication	Reports that are not read or do not fit in the regular Business/IT reporting, Poor control requirements. Misunderstood or misinterpreted KPI's,	Miscommunication leading to unnecessary high cost and waste of resources
Non-value added processing	Elaborated theoretical models for AC/BIA/RA, Inefficient audit & reporting process, Lacking proper tooling leading to manual labor	Unnecessary high cost and overhead
Employee knowledge (unused)	Policy misaligned with operational reality, Control design neglects operational knowledge, Employees spend time on inadequate controls	Increased cost and overhead, increased level of risk, talent leaving the company
Waiting	Lacking agility of control framework, long cycle, Long throughput times for authorizations, Inefficient on-boarding process,	Reduced flexibility, reduced productivity, unnecessary high cost, increased level of risk due to circumventions
Inaccuracy	Over-, underestimating impact & likelihood resulting in inadequate or expensive controls, Applying wrong or inappropriate standards	Unnecessary high cost and overhead, false sense of confidence under high costs

The five steps in Lean & Information Security



3. **Create flow:** - (Tight the sequence of the value-creating steps so the flow is smooth for the value adding steps. Like with JIT)
   - Set the right priorities – Protect/support the most value adding steps first
   - Distinguish between:
     - flow in the security process - faster
     - efficient controls – user friendly
   - Make use of regular Business processes for corrective actions and management of incidents.
   - Secure by design and not bolt on - integrated in Business processes
   - …

The five steps in Lean & Information Security



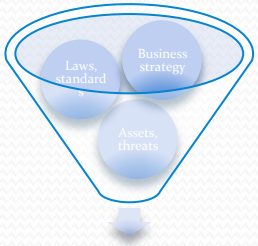
4. **Establish Pull:** - (do something when the 'customer' asks for it)
   - Only act when the Business really demands it (& wants to pay)
   - Implement controls that address risks/issues that have been acknowledged by the Business.
   - Clarify and point out risks and expectations from the end customer to create pull.
   - Continuous / real-time assurance – reduces need to audit (is waste)
   - If they don't want it, don't do it (but have formal risk acceptance).

The five steps in Lean & Information Security

5. **<u>Seek perfection:</u>** (begin the process again and continue it until a state of perfection is reached: perfect value & no waste)
   - This might require a very fast or 'continuous' ISMS.
   - Continuous improving performance and effectiveness of controls
   - Go for Lean security policies (less and practical)
   - High value streams only. Perfection does not mean 100% secure.
   - Define perfection: balance between mitigate/detect/act.
   - Accept that the organization has a self-healing capability (enhance this if necessary)
   - ....

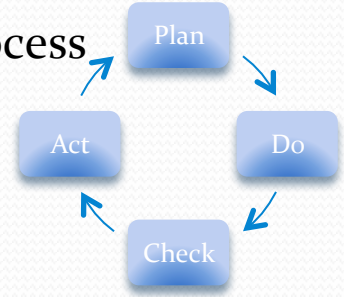
What would a Lean Security Mgmt System look like?

Input



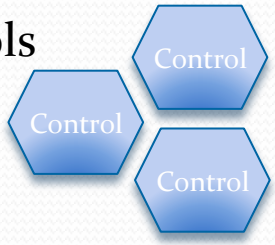
Bring Business value by using an agile, integrated and efficient process that, based on various contextual inputs and….

A process



…a solid understanding of value streams, related assets, security threats and existing controls, results in adequately managed risk, ….

Controls



…by means of necessary, adequate, usable and efficient security controls.

…Not really simple and to the point yet….. Needs work.

Lean Security Management System – PDCA Cycle

- **Plan phase**
  - Lean policies (aimed at usability)
  - Lean AC/BIA/RA methods (aimed at efficiency and effectiveness)
  - Lean principles applied in control selection (question their Business value)
- **Do phase**
  - Lean principles in security control design; flow, pull, no waste…
  - Lean project management for implementation
- **Check phase**
  - Lean assurance (real-time, self-assessment, integrate & reduce audit activities)
  - Lean control framework (deploy efficient process and tooling)
  - Business relevant reporting
- **Act phase**
  - Lean corrective actions (stream into regular change management process)

- **Management review**
  - Continually improve the ISMS itself and its output using Lean principles

Lean Security Controls

Applying the definition, would mean that in Lean Security Management, the controls …

- provide the right value in terms of what the customer wants and when
- Contain and create as little waste as possible
- Are based on customer pull where relevant
- Create flow by aligning process steps
- Are continually improved

Example

- **<u>Identity & Access Management</u>**
- **<u>On/off boarding of staff</u>**
  - Align business HR, owner, IT & security involvement
  - Reduce delays and manual processing
  - Create pull by automated self-service
  - Benefits
    - Save involvement of the Service helpdesk
    - Save a lot of time and money
    - Avoid risks from “work-around” by staff
    - Improve customer satisfaction
  - Show (sell) benefit to Business Management

Conclusions

- **Lean Information Security has potentially great benefits**
  - For creating much more business value,
  - while wasting less time and resources
  - Thereby helping the business, and getting their attention
  - by doing the right things, the right way!
- **How to continue…. Might be interesting enough for ISF to investigate.**
  - A Lean Information Security methodology does not exist yet
  - Continue the discussion on ISF Live
- **Looks promising enough ……!**

Any remarks or questions

"Make everything as simple as possible, but not simpler"

Albert Einstein

Contact & More information

jaap.halfweeg@kpn.com or
m: +31 (0)651535400

More information about Lean:
http://www.lean.org/WhatsLean/Principles.cfm
http://en.wikipedia.org/wiki/Lean_IT
http://en.wikipedia.org/wiki/Lean_manufacturing
On LinkedIn:
http://www.linkedin.com/groups?gid=4458082&trk=myg_ugrp_ovr