Join the Discussion
Connect

A Lean Approach to Information Security

By Frederick Scholl – ISSA member, Middle Tennessee, USA Chapter

The crisis in manufacturing quality and costs in the 1970s gave birth to the concept of lean manufacturing. This article looks at how and where to apply lean concepts to information security.

Abstract

Information security today is under attack. Over the past decade, our technical security knowledge has vastly improved, but security breaches continue to make headlines. As we have become more and more reliant on online services, we are more vulnerable to targeted attacks to breach or even take down those online services. Regulatory compliance has been offered as a solution to keep us more secure. Regulations such as SOX, GLBA, HIPAA, PCI, FISMA have been offered as solutions in their respective domains. But still the security breaches continue. Today, they have the potential to take down our critical infrastructure or even our political system. Life-threatening crises have been faced before by other industries and overcome. The crisis in manufacturing quality and costs in the 1970s gave birth to the concept of lean manufacturing, which has now been widely applied to the auto industry and increasingly to other manufacturing and service industries. I believe that these concepts also apply to information security. This article looks at how and where to apply lean concepts to information security. It is an introduction to those concepts and is presented with the firm belief that security practitioners will be able to apply the ideas to their own environments. Lean security is not a new idea, but the present revolution in IT warrants a fresh look at how lean concepts can protect our data while we move forward with implementing the mobility and social media revolutions.

Information security today is under attack. A few examples in the news can confirm this statement. One is the recent hack of two respected information security firms.[1] Second is the well-publicized Wikileaks exposure of 250,000 internal State Department cables.[2] Third is the impairment of the Iranian uranium processing facility caused by the Stuxnet worm.[3] Fourth is the email breach at ISO 27001-certified marketing firm Epsilon.[4] Clearly each of these organizations has the knowledge and funds to protect its assets from information attacks. But they were unable to do so. At an industry level, in any given six-month period, over one million medical records are reported breached. This, despite the passage of HIPAA Security Rule in 2003 and subsequent extensive documentation on how to secure electronic medical records.

Since 2001 many groups, private and public, have authored new security compliance regulations. These regulations in the U.S. include PCI DSS, SOX 404, HIPAA, GLBA, FISMA, FTC Section 5, FERPA, NERC CIP, HITRUST as well as many individual state security and privacy laws.[5] A significant percentage of enterprise information security budgets is spent to meet one or more of these requirements. Compliance to these regulations may lead management to believe that the enterprise is secure until the next audit. However, the regulations are most often drafted to set a minimum standard for good security and do not help practitioners respond to rapid threat changes.

Some security professionals point to excessive reliance on security audit compliance as one cause of security shortcomings. Amoroso[6] highlights the disparities between *measurable* security controls tested by audits and *meaningful* controls

1 Peter Bright, "Anonymous Speaks: The inside story of the HBGary hack," http://arstechnica.com/tech-policy/news/2011/02/anonymous-speaks-the-inside-story-of-the-hbgary-hack.ars/3, February 16, 2011; "Security Firm Is Vague on Its Compromised Devices," *New York Times*, March 18, 2011 – http://www.nytimes.com/2011/03/19/technology/19secure.html.

2 "Open Secrets," *New York Times*, 2011 – http://www.nytimes.com/opensecrets/.

3 "W32.Stuxnet Dossier," Symantec, November 2010 – http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf.

4 "The phishers' big catch," *The Economist*, April 7, 2011 – http://www.economist.com/node/18529913?story_id=18529913.

5 *ABA Information Security and Privacy*, Thomas Shaw, Editor, 2011.

6 Edward Amoroso, Cyber Attacks: Protecting the National Infrastructure, Butterworth-Heinemann (November, 2010).

that will truly support better security. The challenge is to find controls that are meaningful *and* measurable.

Some practitioners may turn to the ISO 27001 framework and its continuous improvement PDCA model to organize an effective information security program. But even this becomes audit-compliance to a set of controls. It is typically applied to a subset of the organization's information assets contained within the information security management system scope. Threats may easily develop to assets outside of that scope. Further, the ISO standard does not readily describe how to implement the security framework, other than as a series of compliance efforts.

For implementation guidance, practitioners may next turn to the ITIL standard, a series of best practice books on the IT life cycle. But ITIL is focused on the life cycle for an IT service, and security today does not fit into the model of a discrete service. Instead security should be viewed as a complex system of interconnected controls in which failures in groups of controls will lead to overall system failure (breach or outage).

From manufacturing to information security

The concepts from *lean manufacturing* were pioneered by Toyota and embodied in the Toyota Production System. Today these concepts are increasingly being applied with success to *business processes*.[7] These concepts are directly applicable to the security business process. Instead of manufacturing widgets, the overall role of IT is adding value to data and presenting it in a timely way, with no leakage, to customers. Lean concepts can help managers understand how to create, transform, or maintain a security program. Compliance with regulations will be a side benefit of this approach.

Berman was one of the first to address lean thinking in information security.[8] Kim and coworkers further applied lean thinking concepts to security and described the benefits that good security practice can have on IT operational excellence.[9]

The purpose of this article is not to solve all security problems but to introduce lean concepts in the context of information security. These concepts can then be adapted by security practitioners in their own organizations. Lean concepts and tools will improve security and have many other benefits to organizations, such as lowering the cost of compliance and improving system availability. At an industry level, adopting a lean approach to security may help get us out of the regulation-response cycle we are in and thereby help in creation of both business and social benefits.

Lean concepts for security managers

Lean is a management philosophy as well as a toolkit. It was originally developed to improve manufacturing processes; the best known practitioner has been Toyota. We can draw the analogy with a manufacturing process and an information life cycle, from creation through processing to supply to end customer. Lean principles can be applied to the internal security process itself and to security processes imbedded in business processes. It is not necessary to draw a 100% perfect analogy to the original lean manufacturing concepts, since bits do not have all of the attributes of physical objects. For example, bits are usually destroyed by the owner at end of useful life (records management), while destruction of manufactured goods may be carried out by others (recycling).

Security should be viewed as a complex system of interconnected controls in which failures in groups of controls will lead to overall system failure.

Lean concepts are concisely explained by Bell and Orzen.[10] These principles, adapted to information security, are:

- **Voice of the Customer.** This is the number one principle of lean thinking. There are multiple customers that security needs to satisfy, since security processes necessarily cut across the IT department and into business operations. Customers include users, executive management, and the customers of the business itself. Before any security tool or process is implemented it must be clear how it will contribute to satisfying the needs of these constituents.
- **Continuous Improvement.** While PDCA is well known, it is not often consistently carried out in security management. Each PDCA cycle must lay the ground work for the next improvement. Continuous improvement applies to individual security processes like access management as well as to the entire security program.
- **Proactive Behavior.** One function of the security program is to prevent major incidents and outages. Research on reliable enterprises show that large-scale disruptions rarely take place without any warning.[11] Taking proactive action when small-scale security events are detected is critical.
- **Systems Thinking.** The castle-and-moat thinking is outdated, as is weakest-link theory, as is the approach of securing the data. Lean systems thinking is to rely less on sophisticated architectures, but build the best system we know how to build and then make it effective through constant monitoring and improvement. Real security is achieved only through the steps of monitoring and improvement.
- **Constancy of Purpose.** A living security policy document is critical to support the security program. This document must reflect the way information is handled within the

7 Pascal Dennis, *The Remedy*,Wiley (July 6, 2010); Steven Spear, *The High Velocity Edge*, McGraw-Hill; 2 edition (April 12, 2010); Mark Graban, *Lean Hospitals*, CRC Press, 2009; Steven Bell and Michael Orzen, *Lean IT*, CRC Press, 2011.

8 Stuart Berman, "Lean Thinking in Information Security," SANS Institute, 2003.

9 Gene Kim, Paul Love, George Spafford, *Visible Ops Security*, IT Process Institute, 2008.

10 Steven Bell and Michael Orzen, *Lean IT*, CRC Press, 2011.

11 Yossi Sheffi, *The Resilient Enterprise*, MIT Press, 2005.

organization and must be enforced with minimal exceptions.

- **Respect for People.** This does not mean that individuals are handled with "kid gloves." Instead this principle means that each employee and contractor has the ability to successfully do and improve upon his or her job and is held accountable for doing so.
- **Quality at the Source.** Doing it right the first time applies to internal security processes and to other business-facing processes like application and system development.
- **Flow, Pull, and Just in Time.** This is a classic lean manufacturing process principle. It can be applied to security processes such as access management and change management, where multiple steps can often result in delays or inaccuracies.
- **Culture.** At the top is culture; without demonstrated executive support, no security program can be effective. Any true security program must effect a cultural change within the organization.

The first four principles can be utilized by the security function itself. The second five will be most successfully implemented when a lean approach is adopted across the IT department. Supporting these principles are lean tools which enable the principles to be implemented. These include Kaizen, PDCA, Value Stream Mapping, Standardized Work, and others. The available tools[12] have been developed for a manufacturing environment, but can be adapted to IT and information security needs.

Applying lean techniques to information security management

The lean approach to information security is dependent on mental models for protecting information. Everyone is familiar with the moat, drawbridge, and castle wall model. It was a great architecture and kept out our adversaries for thousands of years. But it does not lend itself to continuous improvement.

Lean concepts suggest an approach focused on operational excellence through continuous improvement, not better architectural models. Lean also focuses on people as the resource to solve problems and improve performance. While security architectures are valuable, they only go so far in implementing real security. Systems and threats have become so complex and dynamic that we cannot rely on security architecture. We have to rely on continuous improvement of the chosen security architecture. Failures in today's security defenses do not result from failure of one weak link; they result from accumulated and undetected failures in multiple areas. Adding in more layers of security does not work either. This is perfectly illustrated by the steps reported in the intrusion cited earlier: vulnerable web application; SQL injection; password cracking; easy-to-guess passwords; passwords shared across systems; privilege escalation from user to super-user via unpatched OS vulnerability; and last, but not least, social engineering.

Lean manufacturing is based on four capabilities:[13] identifying problems immediately, immediate root cause analysis and problem resolution, sharing knowledge and learning, and developing these capabilities across the organization. Together, they enable the organization to implement *Kaizen*, or continuous improvement. Kaizen is applicable to individual systems and the organization as a whole. None of these ideas will be new to security practitioners, but putting them at the top of the priority list can help in attaining real security.

Failures in today's security defenses do not result from failure of one weak link; they result from accumulated and undetected failures in multiple areas.

How can we apply these ideas to the practice of information security? While lean concepts have to be selectively adapted to the individual organization, here are some possible areas of application:

Security awareness training

Users are often seen as the weak link in a security program whose architecture would otherwise be effective. Users are described by some as "liabilities." The offered antidote is regular awareness training. A lean approach engages the users as part of the solution, not the problem. If user awareness training can answer the question of "why" adopt a security control and not just "how" to adopt it, then users can become part of the extended security team. In today's complex organizations, this is the only approach that will protect enterprise information.

Root cause analysis and problem resolution

This step is the basis for the famous Kaizen approach that has led to revolutionary levels of quality and cost within the automotive industry. When a security event occurs, make a practice of investigating the cause and taking corrective action. Many outages may occur where it is not obvious whether or not it is a "security event" with malicious activity. Nonetheless the security role can take an active part in the structured investigation and resolution of such events, as well as "traditional" security events like virus and intrusion attempts.

Spread knowledge

Effective information security transformations require sharing of information throughout the organization. Unfortunately information security events or processes are often

12 For example, see www.systems2win.com; www.qimacros.com.

13 Steven Spear, *The High Velocity Edge*, McGraw-Hill; 2 edition (April 12, 2010).

treated with secrecy. If a vulnerability is identified in one business unit, that information may not be shared with others in the enterprise that may have the same or similar vulnerability. The result is that a security best practice database does not get built up for the firm and mistakes are repeated. How else can we explain security breaches like the 2008 ChoicePoint breach after the well-publicized 2005 breach? Or the series of breaches at Wyndham hotels from 2005-2008. Or the Health Net PHI breach of 2009 and again in 2011? These organizations are not cited here to imply that they have below average security. In fact, a recent Ponemon Data Breach Report[14] states that 82% of firms surveyed had multiple breaches. At least one possible suspect cause would be lack of effective sharing of best practices within the firms.

At least one possible suspect cause would be lack of effective sharing of best practices within the firms.

The very good news is that collaboration tools are moving into enterprises. New tools can be used to create a secure virtual workspace for an extended security team. This team can be imbedded in business units and can share security vulnerabilities and best practices amongst themselves. A balance, however, needs to be achieved between sharing security information and exposing too many details.

A summary of the characteristics of a security program with and without lean is included in the table below:

Pre-Lean Security Program	Lean Security Program
Focus on compliance and regulatory requirements	Focus on end-customer requirements
Annual security improvements	Continuous improvements through small changes
End user security awareness	End user security understanding
Technology and architecture focus	Operational excellence focus
Use of specialized security technical terminology	Use of standardized business terminology

Specific examples from industry where lean thinking is now being applied within the security program include:

- A Fortune 100 health care provider has adopted lean across its IT department and is using it to improve multiple processes. Lean has enabled the security function to facilitate improvements in the patch management process and to better document the business benefits of improved processes.
- A global leader in the office furniture business used lean techniques to achieve effective email spam filtering with high levels of end user satisfaction and significant cost savings.
- A global consumer products company is using lean thinking and focus on end-customer requirements to reduce the number of security tools in use.
- Government agencies have used lean thinking to reduce the time required for Certification & Accreditation under the DIACAP process.
- A global medical products and services company has incorporated lean into its security program to do more with less; as an example, using patrolling security guards to check for rogue access points.[15]

Conclusions and action plan

The synergy between information security and lean thinking is based, at a high level, on two concept:

1. Lean is about how to accomplish cultural changes. A cultural change is necessary for any information security program to "stick."
2. Lean is focused on people. Utilizing the people resources in our organizations is the only way to implement a security program today.

It is not necessary to use the formal machinery of lean (or Six Sigma or Lean Six Sigma, or any other acronym) to get started using these principles. In fact, if your user group is unfamiliar with these concepts, this may hinder your efforts. But you can use the ideas without the jargon.

As a starting point, online lean training is available for manufacturing environments[16] and service environments.[17] You can then start to introduce lean concepts into your security program. If your organization has not yet embraced lean, then a next step is to promote the lean concept to a broader audience within your organization. In this way lean security can then help security process development across the organization.

Security intrusions have gotten qualitatively worse this year. Unfortunately, they have only begun to reach into systems that could affect a broad range of our economy. Ideas from lean and operational excellence offer another arrow in the quiver of countermeasures. Now seems like a good time to start using them.

About the Author

Fred Scholl, PhD, CISSP, CISM, CHP, is a security risk management consultant based in Nashville, Tennessee. He helps clients develop security programs that mitigate risks and meet compliance objectives. He can be reached at freds@monarch-info.com.

14 "2009 Annual Study: Cost of a Data Breach," Ponemon, January, 2009.

15 Ray Bernard, Lynn Mattice, Derrick Wright, "Lean Security," *Security Technology Executive*, July, 2008.

16 For example: www.shingoprize.org.

17 For example: www.asq.org