Global Information Assurance Certification Paper

Lean Thinking in Information Security

SANS GSEC Practical

Stuart Berman
Version 1.4b
GSEC Option 1
June 20, 2003

Table of Contents

Abstract

Lean Thinking is a powerful tool to improve an organization's performance by optimizing efforts to deliver clear value to the ultimate consumer of a service or product. Very little information is currently available on how to specifically apply Lean principles into Information Technology or information security. This paper blends a description of the five ordered steps of Lean Thinking with information security topics and examples of the challenges and solutions faced by practitioners of IT security. Specifiying value ensures that the whole process is focused on the customer, a discussion of risk acceptance by a business helps information security find relevance to the business. Identifying the value stream helps to analyze the actions that businesses perform, revealing tremendous waste, ergo less value. Strong password policy must be examined as a source of potential waste. "Flow" allows greater efficiency and reduces waste by removing artifical barriers between processes. Centralized logging, event correlation and data mining are technologies which are capable of making sense of voluminous data that inundates a large enterprise and is often too costly to analyze. "Pull" keeps customer desires driving the output of a system, preventing the creation of unwanted or over priced goods and services. An attempt at our company to apply Lean Thinking to our outsourced managed security service are outlined to demonstrate the application of some of these steps. "Perfection" is the target of the final step in Lean by adopting a continual improvement process. IT benchmarking tools and dashboards are a particularly potent technique to align IT efforts to business objectives.

Introduction

Information security is now a top consideration of CIO's. Security in IT is considered a growth area while many other technology spending areas are languishing[1]. Nonetheless, information security specialists need to deal wisely with every dollar. Businesses continue to look for ways to most effectively spend hard to come by budget dollars, with intense scrutiny paid to Return on Investment – many do not see this trend changing soon, nor do many see a need to ever return to the heady days of free spending[2].

Security professionals ought to take note of a trend which is gaining momentum in the world of manufacturing and in other industries, termed "Lean Thinking".

In it's most basic form, Lean Thinking seeks to ensure optimum value to final consumers by driving out waste in the design, production, marketing, sales, and distribution of products and services[3].

Intuitively, this notion should drive down costs and improve profit, which it does, however, other benefits often accompany this phenomenon: release of large amounts of capital (from traditionally capital intensive sectors such as manufacturing), large reductions of physical space required by businesses (which currently need large spaces for inventory or manufacturing processes), reduction in workforce size, increase in workforce satisfaction and the capability and incentive to enter or create new markets. Timely and relevant information flow is seen as an enabler of Lean systems, restriction of that flow will have consequences.

Why is this significant to us?

If you work on IT staff for an organization, the changes in organizational structure will require you to become a strategic asset who understands these principles[4]. Those who work for information security firms (security [product and service] providers and consultants) will need to appreciate this knowledge to serve their customer better. Simply put: if you can't provide value you will be outsourced, if you are an outsourcer – you will need to understand this in order to be considered competent.

You will make better decisions if you understand how you are able to provide true value to (ultimate) end users and you will be better appreciated if you understand the importance of providing this value.

The Five Steps in Lean…

Specify value – to a specific good or service

The first step in thinking Lean is to specify the value that a good or service provides to the customer who will be the ultimate consumer of it[5].

Let's use an example as follows:

A person wants to "buy" some money by refinancing their home. Mortgage rates are at a historic low, a firm might try to differentiate itself by providing a combination of: ease and speed of research and speed of application, low rates and other costs. From a customer's standpoint the value would be the cost and the ease (as measured by convenience and speed) of obtaining money for various purposes. The customer is not concerned with the security issues at hand, customers expect confidentiality, privacy and accuracy. The task of information security in this example is to help management reduce the risk of loss, whether due to fraud, hacking, internal abuse, etc., while at the same time affording the business every opportunity to provide the value identified.

It is important to consider at this point that there is not an objective and simple standard for acceptable risk tolerance from an IT standpoint. From a business standpoint, the matter may be more quantifiable since it is established business practice to consider loss unavoidable and manageable. Let's take the example of a financial term, "bad debt" – something that occurs when customer is unable or unwilling to pay for a good or service received. It is obvious that too much bad debt is harmful to a company, in our mortgage company example, if I lend money out to a significant quantity of people that will not be able to repay their loans, I will be out of business soon. What is also considered "bad" is to have too little bad debt, this means that you are losing business because your policies are too strict (Bank of America catapulted into success when it started loaning money to people with little or no credit after the great 1906 earthquake in San Francisco[6]). Each business must determine within its business model what level of risk they are going to pursue.

Security practitioners will do well to learn what is an appropriate level of risk for any system and not how to reduce all risks in all cases. Risk is seen as factoring threat by vulnerability, and reducing vulnerability is often considered a principle effort of security professionals. But reducing vulnerability often equates to certain negative consequences, higher costs (systems or efforts) and/or user burden (passwords, tokens, inconvenience, time), so it is imperative that policy makers clearly understand and accept the level of risk the business has chosen.

This is not the step for designing security mechanisms, that comes next. The outcome of this step is that we understand that success will be measured by our identified goals of: convenience, speed and lowest cost for the customer. The identified value must be at the forefront of all decisions in subsequent steps.

Identify the entire value stream – look at each and every action

This step involves analyzing each action performed in the creation, operation and delivery of the good or service in each of the following three phases[7]:

1) Problem solving phase – from ideation, detailed design, to engineering and launch of a product or service (some products like software have the highest cost in this area, so any waste contributes to high cost).
2) Information management phase – from order taking to delivery schedule.
3) Transformation phase – from raw material to delivery of something into a customer's hands.

In our example, determining a risk model, requirements, design and construction for our solution would be the problem solving phase, we'll say our solution is a web site. The next phase of managing information is the operation of the web site, including monitoring and transaction processing. Finally, in our case, the transformation of surety into funds, from securing a binding agreement and title insurance to electronic funds transfer is handled in the transformation phase.

From a Lean Thinking perspective this is the step which exposes the value or waste as identified in three categories[8]:

1) An action unambiguously creates value – let's say we can rate a customer's credit, that is value, if we can do it instantly and show it immediately to a customer, there's more value. Another value action is the electronic transfer of funds to a customer's mortgage holder or personal bank account.

2) Actions that don't create value, but are unavoidable with current technology are considered Type 1 *muda* (or waste). These are areas that security professionals are seeing change rapidly. Whereas mechanisms such as user IDs, passwords, and challenge response were once considered the only feasible option, newer available technologies such as bio-metrics & digital certificates may eliminate many concerns though often are not available to the extent that makes it viable.

3) Actions that create no value and are immediately avoidable are Type 2 *muda*, an example would be filling out the same fields on a web forms that you already filled out, such as your "bill to" information being the same as your "ship to" information. From a security perspective this would be putting in an unnecessary process, such as having a person create an account in our web site and then mailing them a password via post in our example. We are sacrificing speed for what? While we could argue about how "effective" this approach is, if the customer doesn't perceive value then we must reconsider our solution.

The result of this step is the creation of a map of the only specific actions that are required to perform the delivery of a product or service.

A good example of Type 1 *muda*, is the progressively more difficult situation with password standards (or "best practices"). While security professionals make a sound technological case for longer, stronger and frequently rotated passwords – the human condition makes this less feasible than may meet the eye.

Strong passwords have the following characteristics[9]:

- Contain both upper and lower case characters (e.g., a-z, A-Z)
- •Have digits and punctuation characters as well as letters e.g., 0-9, !@#$%^&*()_+|~-=\`{}[]:";'<>?,./)
- •Are at least eight alphanumeric characters long.
- •Are not a word in any language, slang, dialect, jargon, etc.
- •Are not based on personal information, names of family, etc.
- •Passwords should never be written down or stored online.
- Changed every four months

Often tips are given as to how to easily "remember" such as complex string, such as using the first characters of a song title, affirmation, or other phrase. For example, the phrase might be: "This May Be One Way To Remember" and the password could be: "TmB1w2R!" or "Tmb1W>r~" or some other variation.

Here is where the human condition fits in, how many user IDs and passwords do I need on a regular basis? I have a variety of IDs and passwords at work (it really isn't a good idea to have only one ID and/or common password… let's say I use my single ID and common password at a weak site, a web site that gets hacked, now the one and only key I use is compromised and all systems I might possibly access) and for personal use (various sites for online banking, shopping, educational, professional, entertainment, instant messaging). You get the idea… I counted the sites I access online, require ID and passwords and are active - I count 113 separate IDs and passwords (I am prepared to reuse certain IDs and passwords on less sensitive sites, but in many cases I can't even use my ID of choice…. Perhaps someone else already is using it (think AOL), or the ID requires a certain length (minimum and maximum), or excludes certain characters (mainframes, various versions of Windows, Unix and other systems restrict certain character sets – such as colons, whitespace, ampersands, pound sign, etc). Oh… and I am going to take my favorite 113 phrases and rotate them every few months? Right… Perhaps not all of my passwords need to be strong… does that really help? Now I would need to remember a multitude of IDs, with strong and not so strong passwords.

What is a user to do?

That's easy, look around a typical office – IDs and passwords under the keyboard (for those who at least try to be cautious), on the keyboard, on the phone, on the monitor, on the message board, in the Palm Pilot (those can't be stolen and hacked, right?), in a file on a PC or laptop (those never get hacked, lost or stolen).

Net effect, stronger passwords are technically superior to plain passwords, but with the human factor accounted for, they reduce the effectiveness of passwords to less than that of the most simple passwords.

So, as professionals we have various options: push the standard harder, more employee awareness followed by rigorous checking and enforcement; or how about promoting a policy of password eradication? (When I once suggested this in the vicinity of other IT *non-security* professionals I was literally cheered. If I had stayed a little longer, who knows, they may have made me king?) Although there are reasons user IDs are going to stick around for a while, efforts into replacing them with something better would be time well spent and the sooner you get on that path, the sooner you begin making progress. All too often good practices are based on policies that are not based on the culture of the organization and its customers, the policies are drawn up from a perspective of a world without humans, or derived from the calculated direct cost (a typical article cites a cause and effect cost of changing the password reset policy from 60 days to 30 days[10]).

From a Lean Thinking standpoint, memorizing scads of passwords is wasteful (even if there are no direct costs associated with it), because it does not directly produce value. When passwords are capable of being substituted with less cumbersome technology, then they shift from being Type 1 *muda* to Type 2 *muda* – that is, there is now an imperative to retire them[11].

A suggestion for those required to enforce more stringent passwords is to embrace password eradication and make it a stated goal. Then seek examples of how your organization has reduced the rate of growing ID and password needs among applications through common underlying (and hidden) authentication mechanisms such as Kerberos or other ticketing, digital certificates and directory based authentication, and determine how developers can leverage those mechanisms. Then promote the stronger password policies as a stopgap measure on the road to elimination of passwords and IDs. This will allow management and staff to embrace the concept and understand the value and respect the eventual costs that will be incurred to deploy the appropriate technology.

The outcome of this step is a detailed mapping of each and every action performed within the three phases that result in the delivery of a product or service. In information security, those maps will be a subset of the larger mapping that the business creates. An abbreviated and simplified high level map for our refinancing example that touches security issues might look like:

- Public offered “quick and easy” online refinancing with “best rates” possible. They choose their terms and “customize” their program.

- Public goes to any notary public for “free” authentication. (Type 1 *muda*) (Only applies if customer doesn’t already have digital certificate) Notary issues digital certificate to e-mail address provided by customer

- Customer goes to web site from e-mail link sent to them. (Type 1 *muda*)

- Customer issued free personal digital certificate by web site. (Type 1 *muda*)

- Customer able to see best rates, choose any type of program allowed. Customer may browse all programs and rates. Customer may fill out wizard to determine qualifications. Customer may choose any options allowed by law. (FHA,VA, etc) Customer chooses options such as escrow waiver, appraisal type, title insurance, rate lock period, length, prepayment and other penalty options, buy down, funds disbursement methods, etc – each option lists associated costs – a key here is to offer full disclosure as part of choices offered.

- Additionally a wizard may be offered to help guide a customer to the lowest cost options (not highest profit option) give the customer's preferences. This feature builds trust, as a customer is building trust in the provider because the options and costs are clearly laid out for a customer to scrutinize.

- Customer chooses loan program, offered option to accept non-binding offer.

- Finalized disclosures prepared for customer, if customer accepts final terms, approval given (based on qualifications already determined), funds transferred. Notary receives $50 fee for each new customer who was issued certificate.

Flow – no batch and queue processes

The next step takes the map created in the value stream step, and ensures that the performance of those steps is continual, not based on "batch-and-queue" systemology. For our mortgage example, this means that when I go to the web site, I get a rate and complete quote, and immediately I can accept a loan. Wouldn't it be wild to pay off your old mortgage and other debts that easily?

Security take: This presents the challenge to offer real time analysis, eliminating the time waste of a manual (and perhaps subjective) security review. In the example above, some of these steps are becoming a reality as industry based standards are adopted such as Federal acceptance of legality of electronic signatures (2000), county recorders adopting technology to record electronic loans, Freddie Mac and Fannie Mae willing to start accepting electronic loans[12].
As policy and practices mature, it becomes possible to write business logic (whether into an electronic application or as a manual series of steps to follow) that removes individual interpretation and subjectivity, allows greater speed and faith in a system.

This highlights the need for a standard in our field to handle event logging and correlation. SANS teaches the value of remote logging, whereby events should be logged to a remote and secured system. Every security related system, from network infrastructure such as firewalls, IDS probes, and routers, to various operating systems and applications on servers and clients (including Linux, Windows, UNIX and Apple) should have the ablility and be configured to send logging messages (in a syslog fashion) to collector points (so as to allow a scalable and distributed logging system). These collector points would accept messages, (indeed could be platform (OS or application) or message type specific [syslog, SNMP traps, agent type]) and be capable of reformatting to a database standard format. Then each collector would forward the messages to a database or system of databases. The real value now would be to use data mining techniques (based on mature and detailed policy) to discover patterns that are of interest (data mining techniques allow for correlating events, finding interesting/alarming trends that were unnoticed but suspected, or even finding associations that are unsuspected[13].

The obvious benefit here is that today's monitoring is very time consuming and manual, error prone (easy to overlook the few but critical details), often not correlated between systems (network analysts watch IDS logs, UNIX sysadmins watch UNIX server logs) and far from real time (often log analysis is used after the fact as a post mortem forensics tool). Industry sources such as Gartner[14] consider that we have entered into an era of 2nd generation correlation tools, and longing for 3rd generation tools.

An example of the security value of correlation and data mining might be this…

1) A firewall denies access to a particular IP address over several ports.
2) The firewall allows same IP access to an allowed port.
3) An application level IPS prevents the same source IP from disallowed CGI commands.
4) The Network Operating System detects that a user has just been properly authenticated (from same IP source).
5) Application logs determine that same user is accessing confidential data (but user is authorized).
6) Data mining tool detects several interesting "facts":
    - Source IP had been engaged in several suspicious events
    - Source IP associated with European address block
    - User accessing from "unusual" IP range and at an "unusual" hour
    - User accessing unusual data
    - User recently had accessed system from US based IP block
    - (Confidential data accesses always raise flags)

Another tool might react to this by denying access, recording all moves closely, injecting spurious data (at user) to invalidate legitimacy of accesses.
Security staff might be alerted to phone user to determine authenticity of actions, perhaps warning user that ID has been compromised and issuing new ID.

Another way of looking at this concept is to realize that there is a balance between methods to secure a system and the ability to monitor it. For a system facing a certain amount of risk, if you can't make a system suitably secure, then you had better ensure it is well monitored. If you can't monitor it, you had better suitably secure it.

Flow continues value delivery rather than stopping everything and waiting until someone can process and ask the same questions that a system could. The outcome of this step is that obstacles to flow are identified and minimized.

Pull – create it when it is wanted

This step is used by manufacturers to reduce or eliminate inventory. Don't build something before someone orders it. (If no one wants it, that is waste, or if you need to discount it to move it – waste again.) In the financial world, this means a revolution in accounting, a switch from standard costing to activity-based costing, which often reflects very poorly from a traditional Wall Street financials perspective as a business changes its model.

From a security perspective, this could be translated into the idea of a real time security evaluation, such as the OCSP[15] certificate check, versus the practice that an employee's ID is valid until someone gets around to shutting down their account.

An example of adopting Lean Thinking into security practice is illustrated when our contract with a managed firewall service provider was up for renewal and we reconsidered how we should be thinking about this service. We wanted to cut costs, but streamline the processes and improve security. Interested in applying Lean principles to this process, we noticed an abundance of waste.

The old process required the web infrastructure group to fill out a form to request NATT'ed IP addresses and firewall policy changes whenever they wanted to put up a new web site or modify an existing one. The form generated an e-mail to a staff member on the data network team, who would "consider" the request. This often took a day or so, if the staff member was busy or out of the office it could take longer. The staff would call the MFSP and request the policy change for the next "run" of updates.

We identified a value as the creation of a secure web presence for various business needs.

We mapped out all of the actions required from the request (which usually came from the same person, who was now very fluent in firewall concepts) to the delivery of a change.

We came up with this solution which was written into our RFI to various providers.

1) Requestor given direct access to MFSP to make requests.

2) MFSP categorizes request into one of three types:

   A. Standard Request – Internet access for web or FTP services to DMZ server.
   B. Unusual Request – non web or FTP services to DMZ – or - any access to intranet from DMZ or Internet.
   C. Problematic Request – Any request that significantly degrades the security posture of the company.

3) Flow based on above three categories (A, B or C):

   A. Implement change immediately, and notify requestor and Information Security group contacts.
   B. Obtain approval from Information Security Group, then implement and notify requestor and security contacts.
   C. Obtain written approval from Security management authority, then implement and notify requestor and security contacts.

4) Detailed audit trail published for authorized contacts.

This solution obviously calls for a provider with serious talent and exceptional governance. In doing our analysis, we found that the majority of change requests would fit the standard category and in this model would benefit the most from improved flow. As certain requests require more scrutiny, those requests are given more effort and handling, as is appropriate.

Several companies stood out at being fully capable at providing this service, and at far lower cost than our previous "wasteful" process. We believe that those companies are capable of providing that type of service because they have "Leaned" their own organizations, providing investment in automation of event correlation and log analysis, but even more importantly, putting very skilled eyes (a key value point in what we were looking for) on the critical moments within the service, such as change requests and event handling.

We chose our new provider based on compatibility, skill, credibility and trust, affordability and global presence. The last item is important due to the global nature of our business and the need for a partner who had presence and cultural compatibility with our non US organizations.

The outcome of this Lean step is that we ensure that we are involved in actions only when a customer is driving them. Security should be involved when and as it is needed.

Perfection – the cycle of these steps never stops

The final step of continuous improvement is important, the job isn't over when you get the system in, you must always seek to find and reduce waste, the dynamic environment we live in, whether due to technology, system evolution or regulation makes this required.

In security we will undoubtedly see changes in how people view privacy and openness, how we measure "authenticity" (traditionally by signature, biometrics assume this by someone's physical presence but what about their state of mind, can't a contract be voided if a person is under duress or drunk, etc?), and how the variety of laws around the globe affect our work (The Patriot Act, Sarbanes-Oxley Act, and HIPAA are recent examples of US law, the European Union's electronic privacy laws have had a tremendous impact upon multinational firms).

Expect new methodologies, such as IT Balanced Scorecard approach[16] to become standard practice. The Balanced Scorecard attempts to objectively measure an organization's performance and business contributions. Managers are finding this very helpful in taking a metrics based view of IT efforts and quantifying results, which allow the business to evaluate IT contributions and form a basis of benchmarking. The proposed generic Balanced Scorecard is intriguing because it acknowledges the four areas that make up the realm of information security, that is:

1) People – the culture and human side of the security equation
2) Policy – the standards and regulations that interpret strategy
3) Process – the mechanisms for putting policy into practice
4) Technology – the tools that enable us to bring security to IT

Dashboards may become more popular as well, as a way to quantify and display risk assessment. Executives need to be given a business view of the risk posture of the organization (as well as the ability to model what-if scenarios). In a Lean environment, instrumentation will provide data feeds to provide low level technical assessments of a variety of systems, from network components to servers, applications, data flows, customer satisfaction, training and so on. These in turn will feed balanced scorecard like assessments that rate a process to goals and best in class benchmarks. Then these roll up to higher aggregated views of organizational segments. As in any good data warehousing application, one could slice and dice the data to provide relevant views, i.e., "how is the security posture of the North American organization", or "how is the security posture of the Unix systems", or "how has the security posture of this group changed since we implemented PKI"… A powerful driving factor to this model is that once you quantify security (versus a qualitative approach), you can easily import the ratios into financial analysis for more objective financial and management decision making.

The outcome of this step is that an organization is continually recreating itself, committing to agility, and ensuring its continued success by delivering maximum value to the customers who actually drive the business.

Concluding remarks

Visualization is another key concept of Lean Thinking which stresses the value of affording real time feedback, so that employees are given knowledge (information) about their condition, giving them the tools to improve the system that they are an integral part of.

Transparency also plays an important role as partners will need to trust each other more and need access to information that at one time was closely guarded.

Lean Thinking offers a new way of thinking and breaking away from traditional habits and thinking patterns. As companies consider the techniques of Lean, they often find them counterintuitive, such as the inefficiency of batch and queue systems. As such, historically many of the companies that adopt Lean are desperate, trying to avoid impending financial doom in the world of commerce, making them good candidates to take dramatic risks for a potential high stakes pay off. The irony is that as failing companies take this step and do succeed they raise the performance "bar", then former front runner businesses are forced to adopt Lean just to survive and stay competitive.

Introducing Lean into IT organizations is a real challenge, as there is very little case material to draw on, and IT is often seen as an enabler of Lean rather than as adopter of Lean – simply put most companies consider other organizational parts to be in much more dire need of Lean Thinking, such as manufacturing or distribution.

Security practitioners who learn to engage in this thinking will benefit greatly by learning to value efforts by what the business values.

List of References

Womack, James and Jones, Daniel, Lean Thinking: banish waste and create wealth in your corporation, New York:Simon & Schuster, 1996.
Additional information may be found at: Lean Enterprise Institute web site
URL: http://www.lean.org/ (June 20, 2003).

James, Marquis, The Story of Bank of America, Frederick:Beard Books, 2002 URL http://www.beardbooks.com/the_story_of_bank_of_america.html (June 20, 2003).

Berry, Michael and Linoff, Gordon, Data Mining Techniques: for marketing, sales, and customer support, New York:John Wiley & Sons, 1997.

Friedman, Thomas, The Lexus and the Olive Tree, New York:Anchor Books, 2000.

Cameron, Bobby, "The Death of IT", The Forrester Report, Forrester Research, 2000. URL:
http://www.matrixres.com/matrix/website.nsf/Files/CRCMarket_1/$File/Death_IT_2000.pdf?Open

Ware, Lorraine, "CSOs Prioritize Security Spending for 2003", CSOonline, Jan 7, 2003, URL: http://www.csoonline.com/csoresearch/report50.html (June 20 2003).

Berinato, Scott and Scalet, Sarah, "The ABC's of Security", Feb. 20 2002,
URL: http://www.cio.com/security/edit/security_abc.html#roi (June 20, 2003).

SANS web site, The SANS Security Policy Project
URL: http://www.sans.org/resources/policies/Password_Policy.pdf (June 20, 2003).

Gaspar, Suzanne, "Systematic Security", Network World, May 5, 2003.
URL: http://www.nwfusion.com/careers/2003/0505man.html (June 20, 2003).

Messmer, Ellen, "Johnson & Johnson solidifies security". Network World, May 19, 2003 issue. URL: http://www.nwfusion.com/news/2003/0519jj.html (June 20, 2003).

Barta, Patrick, "What Happened to the Paperless Mortgage?", The Wall Street Journal, June 16, 2003, pg. R4, URL:
http://www.emailthis.clickability.com/et/emailThis?clickMap=viewThis&etMailToID=1848844763&pt=Y

Prencipe, Loretta, "Capturing Security's fine lines", Infoworld, April 7, 2003.
URL: http://www.infoworld.com/article/03/04/04/14sem_1.html (June 20, 2003).

Faial, Jose, An Introduction to Information Security performance measurement Using Balanced Scorecards for measuring IS performance, SANS GSEC Practicals, 2002, http://www.giac.org/practical/Jose_Carlos_Faial_GSEC.rtf (June 20, 2003).

http://www.ietf.org/rfc/rfc2560.txt &
http://www.openvalidation.org/whatisocsp/whatindex.htm

Glossary

Activity-based costing – A management accounting system that assigns costs to products based on the amount of resources used (including floor space, raw materials, machine hours, and human effort) in order to design, order, or make a product[17].

CGI – Common Gateway Interface - Allows web servers to perform certain data functions and interact with users.

DMZ – Demilitarized Zone – Computer and network infrastructure between an intranet and the Internet.

IPS - Intrusion Prevention System – A new class of technology that attempts to prevent malicious computer activity from harming its target.

Lean Thinking – An extension of the "Lean Production" approach pioneered by Taiichi Ohno at Toyota which redefines the defintions and boudnaries of value.

MFSP – Managed Firewall Service Provider – A subset of managed security service providers who offer to manage a customer's firewalls.

Muda – a Japanese word for any activity that consumes resources but creates no value.

NAT – Network Address Translation – A protocol widely used to overcome the IPv4 address shortage by mapping RFC (such as 10.0.0.0) addresses to publicly routable addresses.

OCSP – Online Certificate Status Protocol – A technology which attempts in real time to validate the validity of a digital certificate, the current CRL (Certificate Revocation List) technology is cumbersome and not transparent to the user.

RFI – Request For Information – A streamlined method for quickly reducing the eligible vendors offering a paricular service or product to a shorter listof qualified candidates. The longer method is RFP – Request for Proposal.

Standard costing – A management accounting system which allocates costs to products based on the number of machine hours and labor hours available to a production department during a given period of time. Standard cost systems encourage managers to make unneeded products or the wrong mix of products in order to minimize their cost-per-product by fully utilizing machines and labor.

End notes

[1] Ware, http://www.csoonline.com/csoresearch/report50.html
[2] Berinato, http://www.cio.com/security/edit/security_abc.html#roi
[3] Womack, Lean Thinking, pg 15.
[4] Cameron, http://www.matrixres.com/matrix/website.nsf/Files/CRCMarket_1/$File/Death_IT_2000.pdf?Open
[5] Womack, op cit, pp 16 - 19.
[6] James, The Story of Bank of America.
[7] Womack, op cit, pp 19 –21.
[8] Womack, loc cit.
[9] SANS, http://www.sans.org/resources/policies/Password_Policy.pdf
[10] Gaspar, http://www.nwfusion.com/careers/2003/0505man.html
[11] Messmer, http://www.nwfusion.com/news/2003/0519jj.html
[12] Barta, "What Happened to the Paperless Mortgage?", pg R4.
[13] Berry, Data Mining, pp 5-6.
[14] Prencipe, http://www.infoworld.com/article/03/04/04/14sem_1.html
[15] http://www.ietf.org/rfc/rfc2560.txt and http://www.openvalidation.org/whatisocsp/whatindex.htm
[16] Faial, http://www.giac.org/practical/Jose_Carlos_Faial_GSEC.rtf
[17] Womack, op cit, pg 305.