Presented to the Interdisciplinary Studies Program:

UNIVERSITY OF OREGON
APPLIED INFORMATION MANAGEMENT

Applied Information Management
and the Graduate School of the
University of Oregon
in partial fulfillment of the
requirement for the degree of
Master of Science

Applications of Lean Methodologies for Improving Information Security

CAPSTONE REPORT

Mark Messenger
Information Security Analyst
University of Oregon

University of Oregon
Applied Information
Management
Program

Spring 2018

Continuing and Professional
Education
1277 University of Oregon
Eugene, OR 97403-1277
(800) 824-2714

Approved by

_____

Dr. Kara McFall
Director, AIM Program

Applications of Lean Methodologies for Improving Information Security

Mark Messenger

University of Oregon

Abstract

Information Technology (IT) Risk Management is critical for large organizations. Lean methodologies describe ways to reduce process waste. Duplicate IT systems and services can be viewed as Lean waste. This paper explores Lean waste reduction in IT to decrease organizational risk. References from foundational works and works in the last ten years are presented. IT managers and security executives can use this work to identify Lean tools that provide value for their organization.

Keywords: lean, it security, risk management, duplicate services, risk analysis

Table of Contents

Introduction to the Annotated Bibliography

Problem Description

The University of Oregon's Information Services (IS) department has a problem. Over the last two years, IS headcount has ballooned 40% through a combination of organic growth and role acquisitions from distributed information technology (IT) groups. These acquisitions have brought with them numerous projects, processes, and peculiarities. IS lacks a mandate from leadership in the area of documentation. As a result, the documentation practices in distributed IT groups are as varied as the groups themselves. These variations have led to significant duplication of effort and conflicts between user groups regarding which documentation standards and systems are appropriate for multi-group and multi-department projects. Benaroch, Lichtenstein, and Robinson (2006) call out "conflicts between user groups and lack of management commitment" as risks to the continued success of IT projects, services, and departments (p. 830).

The details of projects that have recently moved to IS and their data flows, sources, and customers are quartered largely in the minds of the projects' respective owners. Without a mandate for disclosure and documentation, many acquired system and service administrators have not documented the nuances and quirks of their projects. As turnover and attrition take their toll, IS is losing awareness of the digital data that courses through its virtual veins.

This loss of knowledge awareness is evident in different ways. In disparate corners of the organization, well-meaning developers and engineers have birthed redundant systems. Duplicate services exist for identity management/authentication, email, collaboration, virtual private networking (VPN), web hosting, project management, service ticketing, and documentation. Duplicate services may bring additional costs in the form of duplicate resource allocation (Bell &

Orzen, 2011). Bell and Orzen (2011) note that costs also take the form of time lost by staff working on duplicate services and missed opportunities for other processes and projects in the form of "bottlenecks and scheduling delays" (p. 6). Divergent understandings and expectations by IS staff may also be a cost factor (p. 5). These divergences can lead to rework, reengineering, and lowered morale (p. 27). Together, Bell and Orzen (2011) term these conditions "fragmentation" and "systems anarchy" (p. 4).

To make these conditions tractable, management needs to better understand the data and systems in their organization (Niemimaa & Niemimaa, 2017). Niemimaa and Niemimaa (2017) term the process of gaining a better understanding of an organization's data assets "information classification" (p. 7). Information classification includes identifying and documenting the location and description of the data, along with potential disclosure ramifications in the event of a security breach (p. 7). Taitsman, Grimm, and Agrawal (2013) note that these ramifications are often dictated by law, especially when the data is governed by regulations like the Health Insurance Portability and Accountability Act of 1996 (HIPAA).

The information security risks of duplicate systems and services is considerable (Whitman & Mattord, 2011). Vacca (2013) states that as a network expands in size and complexity and as the number of users increases, potential security risks grow "exponentially" (p. xvii). While security of the network is a part of an overall risk management strategy, Kouns and Minoli (2010) observe that the security of the host is of "equal or even greater importance" to the business by virtue of the customer, employee, product, and account data stored on the host (p.15). Whitman and Mattord (2011) note that "operating information systems in a secure fashion become more difficult as the number and complexity of these systems grow" (p. 447).

The challenge in securing large numbers of systems may arise from the challenge in programming large systems that are both secure and profitable (Strebe, 2004).

Strebe (2004) states that software programmers "can't accurately predict flaws" (p. 3). In addition, the unforgiving nature of the free market rewards companies that are first-to-market (p. 4), and software development companies "who spend time on security are eclipsed by the competition" (p. 3). Software development companies that skimp on testing to surface security flaws and ignore security holes in a rush to market typically "are not motivated to reveal potential flaws" as these flaws are externalities for the software publisher (p. 3).

Camp and Wolfram (2004) define externalities as "instances where an individual or firm's actions have economic consequences for others for which there is no compensation" (pp.18-19). Zimba, Wang, and Chen (2018) note that in the realm of computer software, externalities that manifest as security vulnerabilities can have unintended consequences for the software purchaser. Zimba et al. (2018) further warn that an exploitable vulnerability in one software product may lead to the "exposure of other software and systems" on the organization's network (p. 14). Whitman and Mattord (2011) use the term *pivot points* to describe systems or services that can be used by an external attacker to gain access to internal-only systems or devices. Access to business-critical systems that are protected with multiple layers of defense may require an attacker to use chained vulnerabilities, a method that exploits multiple weaknesses in diverse systems to evade detection (Whitman & Mattord, 2011). Taking pivot points and chained vulnerabilities into account, Whitman and Mattord (2011) conclude that duplicating software services will introduce additional costs and risks into the enterprise in the form of administrative security and process "overhead" (p. 446).

Tribelsky and Sacks (2010) note the utility and value of Lean methodologies in "monitoring or measuring the actual flow of information" (p. 190) in an IT environment. For the purposes of this document, The Cambridge University Press (2018) definition of Lean in a manufacturing context is used: "The business of producing goods in large numbers using methods that avoid waste and reduce the time taken" (para. 1). Tribelsky and Sacks (2010) note that while Lean methodologies have been in use in manufacturing operations for decades, they have only recently been applied to the identification of waste in the context of information management.

Tribelsky and Sacks (2010) state that Lean waste (muda) within the context of information management can be considered to include the consequences of not providing the information consumers what they need. These consequences may include "incomplete utilization of staff resources," "loss of opportunities," and "negative or ineffective outputs" (Tribelsky & Sacks, 2010, p. 190). Arunagiri and Gnanavelbabu (2014) go further, identifying "all activities that do not add value" as waste, including operating unnecessary or duplicate services (p. 2167). Tribelsky and Sacks (2010) tie the concepts together, noting that Lean methodologies' removal of duplication dovetails with Information Security's desire to decrease an organization's attack surface.

Purpose Statement

The purpose of this research is to present literature that addresses the problem of increased organizational risk that arises from waste in the form of duplicate information services. Specifically, this research examines the information security risk inherent in these forms of Lean waste and best practices from Lean methodology to mitigate or eliminate these risks. Managers at all levels of an organization can provide value by identifying and reducing organizational risk. This study will assist managers in identifying and evaluating the information security risk factors intrinsic to duplicate services and best practices from Lean methodology to address them.

Research Questions

Main question. Which best practices from Lean methodology can be used to identify and diminish information security risks that arise from duplicate services?

Sub-questions. What criteria can be used evaluate the organizational risk produced by information security vulnerabilities within an organization? Which Lean tools can be used to prioritize the remediation of these vulnerabilities?

Audience

The primary audience for this paper is managers, directors, and executive staff within organizational Information Services departments who make risk management decisions. Cruz, Peters, and Shevchenko (2015) state that risk management is "those activities performed to prevent accidental loss" (p. 1). Straub and Welke (1998) define risk as "the uncertainty inherent in doing business" (p. 442). Specifically, it is "the probability associated with losses (or failure) of a system multiplied by the dollar loss if the risk is realized" (p. 442). To help these managers internalize information security concepts, it may be beneficial to relate these concepts to direct and familiar themes from management theory.

Managers who have come up through the corporate ranks with a background in management theory may be very capable of estimating the cost and likelihood of losing a customer or contract. Information Security, however, is a separate field, replete with technical pitfalls, errata, and historical artifacts. Accurate estimation of the specific costs and likelihoods of information security incidents may be left to technical staff, extrapolated from a manager's personal experience, or ignored entirely.

The secondary audience includes IT managers and directors. These roles might benefit from the honesty displayed by, and insights gained from, an unflinching examination of IT operations and ways to reduce the associated waste that leads to security risks. Both audiences may benefit from viewing waste within a Lean context as an organizational security risk. This perspective may provide these audiences with additional leverage to improve their organization's risk profile by sunsetting legacy systems or consolidating redundant services.

Search Report

Search Strategy. This Capstone project targeted the intersection of Lean methodology, Information Security, and Information Management. This project explored the specific applicability of Lean concepts as an avenue to improve an organization's security posture by removing unnecessary or wasteful collection, processing, storage, and delivery of data. One of my Capstone goals is to use Lean Methodology topics to inform the construction of strategies to winnow useful infrastructure from those that are costs or liabilities to the organization.

I utilized the University of Oregon's Libraries website (https://library.uoregon.edu) in the search for academic reference works for this project. The LibrarySearch function on the main page provides several search methods. I used keywords as the primary search method. I occasionally used the Title search method to locate an online resource when I knew the full title

of that particular resource. I leveraged all available databases (UO + Summit + Articles) in the creation of this work. For statements of fact, I limited cited results to peer-reviewed journals and published books. I leveraged non-academic sources for some term definitions that are widely accepted, but were not readily available as explicit definitions in academic literature.

Key Terms. I used the following search keywords:

- Lean AND Information Management.
- Lean AND Information Security.
- Lean AND IT Security.
- Information Security AND Incident Management.
- FERPA AND Information Security.
- Lean Manufacturing.
- Lean AND Tim Woods.
- Information Security AND Redundant.
- Information Security AND Legacy.
- Microsoft and Windows AND WannaCry.
- Patient AND Information AND Privacy.
- Security AND IT Infrastructure.
- Security AND Scaling.
- Security AND Large Network.

Documentation Strategy. I accrued and maintained search strings in a plain-text document on cloud storage. I included relative success indicators for each set of search terms in this document. I kept electronic copies of reference documents in a private cloud storage folder away from other documents (e.g., weekly assignments). For separation and easy integration into

the final project document, I maintained references and their associated abstracts in a cloud document separate from the search strings file.

Reference Evaluation Criteria. Research sources were evaluated based on criteria from *Evaluating Information Sources* from the University of Florida's Center for Public Issues Education (2014). The overarching criteria categories listed are Authority, Timeliness, Quality, Relevancy, and Bias.

Bias is an interesting criterion to judge. University of Florida Center for Public Issues Education (2014) suggests three main criteria for evaluating bias: financial motivations, consideration of opposing viewpoints, and logical foundations built on credible sources. Research sources were evaluated for bias based on discernible irrational or financially-motivated viewpoints that affected the source's stance on the topic cited, credible support for the author's conclusions, and the time or consideration given to opposing viewpoints. Sources with significant irrationality, visible commercial ties, little credible support, or asymmetrical consideration were discarded.

I used additional questions to evaluate research sources. To determine an author's authority, I considered whether the journal in which the article appeared is peer-reviewed according to the UO Libraries search engine. Peer reviewed journals tend to have higher quality work from authors with authority in their fields. In addition, I considered whether the author's credentials reflected a depth of knowledge sufficient to be qualified to speak on the matter of reference.

Given the rate of change in the field of inquiry, I considered whether sources were timely enough to reflect current practices and understandings. Some fields are highly dynamic while others are fairly mature. Is the specific quote, idea, conclusion, or statement relevant to the

research question? Does the source appear to be well edited with grammar, spelling, punctuation becoming of a research institution? Do the author's credentials reflect a depth of knowledge sufficient to be qualified to speak on the matter being referenced? For this specific study, I adapted date ranges for each field to provide high-value, available results:

- Information Security: 2008-2018

  As of 2018, Information Security is a highly dynamic field. Articles prior to 2008 may not represent the current understandings, problems, and tools in the Information Security field.

- Information Management: 2008-2018

  Information management is a fairly new field of study. Most of the search results for articles published in peer-reviewed journals landed between 2008 and 2018. Some articles published in the 1990s did not appear to be congruent with the modern business technology landscape.

- Lean Methodology: 2000-2018

  Lean methodology is a more mature field, with some articles dating back to the 1990s. Many terms and definitions in this field are solidified and have not changed in the last two decades. Not all of the older articles are available online. In an attempt to only view articles that were immediately available, these searches were limited to the last 18 years.

- General Management: 1990-2018

  Management theory has been around in many forms for over 50 years. Like Lean methodology, older articles on general business management topics may not be available online. To only view articles that were immediately available, these searches were limited to the last 28 years.

To determine the quality of a potential source, I considered whether the source appeared to be well edited with grammar, spelling, and punctuation becoming of a research institution. Finally, I approached relevancy by considering if the specific quote, idea, conclusion, or statement was relevant to my research questions.

Annotated Bibliography

Introduction to the Annotated Bibliography

This Annotated Bibliography presents 15 peer-reviewed references that inform my research into the intersection of Lean methodologies, Information Security, and Risk Management. These references were selected to introduce managerial staff to the notion that system and service redundancies can be an information security risk to the organization. These references are placed into three categories: a) references for Lean methodologies, b) risk management perspectives on IT and c) information security costs of duplicate services.

Each reference contains three components: a) a citation in APA format, b) an abstract, introduction, or preface, and c) a summary. References from academic journals will have an abstract. References from published books will have an introduction or preface. Abstracts, introductions, and prefaces are presented as published by the original authors.

The summaries provided in this Annotated Bibliography are the work of this document's author. However, the *ideas* presented in these summaries belong to the respective authors of the works being summarized.

Category A: Background and Supporting References for Lean Methodologies

Alhuraish, I., Robledo, C., & Kobi, A. (2017). A comparative exploration of lean manufacturing and six sigma in terms of their critical success factors. *Journal of Cleaner Production, 164*, 325-337. doi:j.jclepro.2017.06.146

Abstract. Lean manufacturing and six sigma methodologies have been widely used in a large number of companies worldwide. However, many companies have found it difficult to successfully implement and sustain lean manufacturing and six sigma. It is, therefore, very important for companies to identify and understand the critical success factors for

successfully implementing either six sigma or lean manufacturing. A comparative examination of lean manufacturing versus six sigma was conducted, and the success factors relevant to these two methodologies were identified. It was found that the most important success factors differed in terms of their significance for six sigma and lean manufacturing. Specifically, for organizations that have successfully implemented six sigma, skills and expertise ranked highest in importance. In contrast, for organizations that have successfully implemented lean manufacturing, employee involvement and culture change ranked highest. This study builds on current knowledge and fills a gap in the literature by providing more insight into the most critical success factors within companies that have already successfully implemented these methodologies. The results of the study will help organizations to make more mature and careful decisions regarding the critical success factors of each method. Therefore, in the pre-implementation stage, organizations can identify how their capabilities and resources can be utilized to accomplish the critical success factors for the implementation of lean manufacturing and six sigma, either simultaneously or sequentially. This is the first study that has conducted an examination to compare lean manufacturing and six sigma in terms of the importance of the same specific critical success factors.

Summary. This article explores the intersection between Lean methodologies, Six Sigma variation reduction, and green manufacturing. A Lean and Six Sigma literature review outlines previous academic work on the benefits and potential pitfalls of Lean implementations; key findings include that the lack of top-tier management support and lack of skills and training were the most dependable indicators of Lean implementation failure. The authors present key success factors for Lean implementations including

managerial support, culture alignment, and employee participation. Culture alignment in this context refers to the willingness to undertake a dispassionate analysis of existing practices and an openness to change processes that are redundant or found lacking. While this article does not reference IT departments by name, the concepts presented are relevant to generic organizations, including IT. This article supports my research by identifying potential hurdles for Lean adoption in an organization.

Arunagiri, P., & Gnanavelbabu, A. (2014). Identification of major lean production waste in automobile industries using weighted average method. *Procedia Engineering, 97*, 2167-2175. doi:10.1016/j.proeng.2014.12.460

Abstract. Industrial muda elimination is a major challenge that is faced by the experts in the day to day activities of production systems. Mostly there are seven types of industrial muda in lean systems such as Defects, Overproduction of things not demanded by actual customers, Inventories awaiting further processing or consumption, Unnecessary over-processing, Unnecessary motion of employees, Unnecessary transport and handling of goods, Waiting for an upstream process to deliver, or for a machine to finish processing, or for a supporting function to be completed. Every organization faces particular type of waste that occurs in day to day production activities. In order to find out the most influential lean waste based on the ranking, a survey has been conducted in 91 automobile industries based on the 5 point likerts scale to find the highly impacted lean muda. The survey results stating that 3 types of waste arising out of 7 waste which heavily affect the production system. Hence this work mainly deals with assessing the most deadly waste by ranking the major waste using the weighted average method in which each waste is assigned a weight. Based on the results, the major muda, which are

identified that affects the production activities are discussed in detail and how this muda can be eliminated and incorporated with the production system are discussed.

Summary. This article is a case study of Lean waste elimination at an automotive manufacturer. The authors explore seven of the eight major types of Lean waste (Transportation, Inventory, Motion, Waiting, Over-production, Over-processing, and Defects). Employees at the automotive manufacturer were surveyed to identify visible instances of Lean waste in the organization. Survey results highlighted a high incidence of waste in the forms of Transportation, Waiting, and Motion. A causal connection between excess transportation and waiting is noted and described. The authors find that Lean defects in an office or IT environment can manifest as slow communication, poor planning, fracturing of services, and errors in transcription or translation of requirements. Other types of Lean waste, including excess inventory, are identified and described as costs to the business that generate no return. This article supports my research by providing a logical foundation for several Lean concepts, including the assessment of duplication of services as Lean waste.

Bell, S., & Orzen, M. A. (2011). *Lean IT: Enabling and sustaining your lean transformation*. New York, NY: Productivity Press.

Introduction. This is the first definitive and comprehensive text on the Lean IT body of knowledge, demonstrating how the various aspects of Lean can be applied to the continuous improvement of information and information systems in order to enable and sustain the Lean enterprise. Written by Lean IT pioneers Steve Bell and Mike Orzen, this book distills over 40 years of experience in applying Lean principles, systems, and tools to information technology across many industries. This book was written to help you—

whether you are a business executive, manager, IT professional, or member of an improvement team—to proactively improve, integrate, align, and synchronize information and information systems to enable breakthrough performance and agility.

Summary. This book is a complete guide to implementing Lean methodologies in an IT department. Lean's historical background in manufacturing from 1890 to present is presented; key events include the deployment of assembly lines by Henry Ford in the early 1900s, the development of the Toyota Production system in Japan after World War II, and the integration of Lean and Six Sigma in the early 2000s.

Lean concepts of muda (waste), muri (overburden), and mura (unevenness) are defined and related to IT operations. One example of muda in an IT context is the continued operation of sunsetted services; that is, services that have been migrated off of, but are kept running for lack of staff time or management will to decommission. Email overload is cited as an example of muri (overburden). In an IT context mura (unevenness) would include inconsistent results when dealing with different helpdesk staffers.

Applications of Lean in IT auditing, planning, and analysis are presented. The authors note that Lean can be applied to an IT auditing context by performing Value Stream Mapping of existing processes and groups to differentiate the components that provide value to the customer from those that do not. Lean in the context of IT planning includes evaluating new projects for overlap with existing projects and for overall customer value-add. Finally, the authors note that Lean in the context of IT analysis includes the identification of excess inventory. The authors provide the example of excess file copies that reside in email inboxes.

This article relates to my research through the presentation and definition of the connections between Lean methodologies and ongoing IT operations.

Hicks, B. (2007). Lean information management: Understanding and eliminating waste. *International Journal of Information Management, 27*(4), 233-249. doi:10.1016/j.ijinfomgt.2006.12.001

Abstract. This paper deals with the development of a new approach for supporting the improvement of information management and the overall information systems infrastructure. In particular, the paper discusses the application of lean thinking to information management; where information management can be considered to involve adding value to information by virtue of how it is organized, visualized and represented; and enabling information (value) to flow to the end-user (customer) through the processes of exchange, sharing and collaboration. The potential benefits of lean thinking are discussed and the fundamental barriers for its application to information management are highlighted. These include the need to characterize the nature of waste and establish the five principles of; value, value streams, flow, pull and continuous improvement in the context of information management. It follows that the core contribution of this paper is the development of an understanding of these critical elements and the creation of a conceptual framework for a set of lean principles within the context of information management. This framework offers a unique and arguably generic approach for supporting the retrospective improvement of information management systems and the overall information systems infrastructure.

Summary. The author explores information management through the Lean concept of value. The author discusses the value of information systems to the information

consumer as collators, connectors, and visualizers of data. In these specific contexts, the author identifies the value of information systems as commercial off-the-shelf (COTS) applications. Examples include Customer Relationship Management (CRM) packages and database (DB) engines. The author links managerial concepts, including Key Performance Indicators (KPIs) and Enterprise Resources Planning (ERP), to Lean methodologies. The author notes the parallels between KPIs and muda measurements within Lean methodologies and between ERP and Value Stream Mapping in a Lean context. The author outlines parallels between product manufacturing and knowledge manufacturing, including the potential for misalignment with business goals, the importance of customer focus, the need for a thorough understanding of core competencies, and the idea of duplication of effort and service as waste. The author presents blockers to the rationalization and improvement of information systems, including initial cost outlays, organizational inertia, organizational perception of IT departments as 'gatekeepers' of data, and perceived loss of autonomy in business functional units.

This article supports my research by providing findings from which one can deduce an argument for de-duplication and consolidation of redundant information systems with support from well-known managerial principles.

Tribelsky, E., & Sacks, R. (2010). Measuring information flow in the detailed design of construction projects. *Research in Engineering Design, 21*(3), 189-206.

Abstract. Waste in engineering design has many facets, from partial utilization of the solution space, to wasteful management of design resources, and creation of erroneous

and ineffective design documents. In the detailed construction documentation design phase of construction projects with teams comprising multiple independent designers, slow and interrupted information flows lead to significant waste. Applying lean principles, such as reducing batch sizes, cycle times and work in progress inventories, to the management of information flows may improve processes and reduce waste in this phase of the design process, but the lack of a method for measuring the volume, rate and effectiveness of information flow is an obstacle to research. This study proposes measuring the flow of information in the process of detailed design where construction documents are prepared. Measures and indices of flow were formulated based on examination of empirical data compiled by monitoring flows of design information in the detailed design stage of each of fourteen construction projects. Data describing the flows was drawn from the database logs created through practitioners' use of a project extranet service. Indices for identifying information flow bottlenecks, large batch sizes and accumulation of work in process were computed and validated for four of the projects by comparing them with the results of independent observations of design coordination meetings. An index for measuring rework was also computed but could not be validated. The indices and information flow graphs are intended to assist in identifying faults or bottlenecks in the process either as they happen or in retrospective study, indicating disruptions in the information flow. As such, they are important tools for research of engineering design and may be of practical use in design management if incorporated in future online design management tools.

Summary. This article is a treatment of information waste in the construction field through the lens of Lean methodologies. Lean concepts of bottleneck, velocity, and

rework are detailed. The authors term bottleneck a constraint on the flow of material at one step in a process. Velocity is the concept of an individual item's average speed through a manufacturing facility or process, where higher speeds are better. Rework is defined as a form of waste that arises from problems in a manufacturing process that lead to unacceptable defects in the final product that require corrective action.

While the authors concentrate on applications to the construction field, many of their general conclusions, definitions, and notes are relevant to information management and Lean analysis in other organizations. Specific conclusions that are useful to this study include a finding that the use of information access logs from online collaboration services to estimate the amount of knowledge rework performed by a project team was inconclusive. The authors note that while rework estimation was not conclusive, use of automated log analysis to identify bottlenecks and batch size inefficiencies was feasible and effective.

The authors provide examples of waste in the information design process. One example given was the preponderance of miscommunication and isolation between subcontractors on a large job. While the work of each subcontractor depended on at least one other subcontractor, many subcontractors were reticent to disclose their upstream needs for fear of giving a competitor leverage that might be used against them when bidding on a future project.

This article supports my research by defining select Lean terms, by exploring ways in which Lean can dovetail with information management, and by giving real-world examples of waste in the information design process. One example given was the preponderance of miscommunication and isolation between subcontractors on a large job.

While the work of each subcontractor depended on at least one other subcontractor, many subcontractors were reticent to disclose their upstream needs for fear of giving a competitor leverage that might be used against them when bidding on a future project.

Category B: Risk Management Perspectives on Information Technology

Benaroch, M., Lichtenstein, Y., & Robinson, K. (2006). Real options in information technology risk management: An empirical validation of risk-option relationships. *MIS Quarterly, 40*(4), 827-864. doi:10.2307/25148756

Abstract. Recently, an option-based risk management (OBRiM) frame work has been proposed to control risk and maximize value in information technology investment decisions. While the framework is prescriptive in nature, its core logic rests on a set of normative risk-option mappings for choosing which particular real options to embed in an investment in order to control specific risks. This study tests empirically whether these mappings are observed in practice. The research site is a large Irish financial services organization with well established IT risk management practices not tied to any real options framework. Our analysis of the risk management plans developed for a broad portfolio of 50 IT investments finds ample empirical support for OBRiM's risk-option mappings. This shows that IT managers follow the logic of option-based risk management, although purely based on intuition. Unfortunately, reliance on this logic based on intuition alone could lead to suboptimal or counterproductive risk management practices. We therefore argue that managerial intuition ought to be supplemented with the use of formal real option models, which allow for better quantitative insights into which risk mitigations to pursue and combine in order to effectively address the risks most worth controlling.

Summary. This article explores one particular branch of risk management, Options-Based Risk Management (OBRiM). In pursuit of a solid argument for OBRiM, the authors present and detail several risks to new and continuing IT projects and services, including size, complexity, outsourcing, and lack of managerial involvement. While the authors use an example organization in Ireland, the management principles they explore are applicable to U.S. organizations. This article relates common business and technology management mistakes to the viability of the services and projects being managed. Among these common mistakes is a lack of thorough understanding of the existing environment, including lack of awareness of existing projects and services that compete with proposed initiatives. This article provides support for my research by detailing potential costs to the organization of duplicate services.

Cruz, M. G., Peters, G. W., & Shevchenko, P. V. (2015). *Fundamental aspects of operational risk and insurance analytics: A handbook of operational risk*. Hoboken, NJ: Wiley.

Introduction. Operational risk (OpRisk) has been through significant changes in the past few years with increased regulatory pressure for more comprehensive frameworks. Nowadays, every mid-sized and larger financial institution across the planet has an OpRisk department. However, if we compare the pace of progress of OpRisk to market and credit risks, we would realize that OpRisk is not advancing as fast as its sister risks moved in the past. Market risk management and measurement had its major breakthrough in the early 1990s as J.P. Morgan released publicly its Value-at-Risk (VaR) framework. Only a couple of years after this release, most of the 100 global largest banks had developed a market risk framework and were using, at least to a certain level, VaR methods to measure and manage market risk. A few years later, the Basel Committee

allowed banks to use their VaR models for regulatory capital purposes. From the release of JP Morgan's methodology to becoming accepted by Basel and local regulators, it took only about 4 years. This is basically because the methods were widely discussed and the regulators could also see in practice how they would work. As we see it, one of the biggest challenges in OpRisk is to take this area to the same level that market and credit risk management are at. Those two risks are managed proactively and risk managers usually have a say if deals or businesses are approved based on the risk level. OpRisk is largely kept out of these internal decisions at this stage and this is a very worrying issue as quite a few financial institutions have OpRisk as its dominant exposure. We believe that considerable effort in the industry would have to be put into data collection and modeling improvements, and making a contribution to close this gap is the main objective of our book.

Summary. This book provides a systematic look at the risks to ongoing operations that an organization may face. The methods, data, and conclusions are tailored toward a private-sector business. However, many of the concepts are generic and may be applied to any large organization. Internal risks from data loss, inappropriate access controls, collateral damage, system failures, and business interruption are detailed. From an information security perspective, loss of control of sensitive data can lead to public exposures and extortion attempts. Exposure of data from one division of an organization may have collateral effects on public opinion and customer acquisition costs in another division.

The authors also explain external risks from regulatory compliance, vendors, and incorrect customer records. As an example, through an information security lens the

security posture of a vendor (e.g., a cloud services provider) may indirectly expose the organization and its data via lax background checks, inadequate access controls, or non-existent auditing. This book supports my research by outlining many risks to business operations that may arise from information security oversights.

Kouns, J., & Minoli, D. (2011). *Information technology risk management in enterprise environments: A review of industry practices and a practical guide to risk management teams*. Hoboken, NJ: Wiley.

Preface. This book aims at surveying industry approaches, best practices, and standards for how an organization can position itself to properly handle this ever-increasing and perennially mutating tsunami of risks to their business-critical IT assets. The book has two major sections. Part 1 reviews industry practices in the area of risk assessment and mitigation. The aim is to provide an overview of the well-known risk management approaches and methodologies. Part 2 focuses on helping an organization to develop a repeatable program that will address technological issues and human resources within the organization, to effectively undertake the risk assessment and mitigation function. It looks at the best use of IT resources, procedures, tools, and preparedness, and it places emphasis on implementing a risk assessment team that can properly foresee, prevent, and/or rapidly remediate potential infractions. This text is intended to be used by information security managers, security analysts, systems developers, auditors, consultants, and students, among others.

Summary. This book is a soup-to-nuts documentation of risk management in IT. The authors start by defining risk management as the process of evaluating IT security "whereby threats, vulnerabilities, and potential impacts from security incidents are

evaluated against the cost of mitigation" (p. 35). The authors present domestic and international frameworks for IT security and risk management. Domestic frameworks include National Institute of Standards and Technology (NIST) Special Publication (SP) 800. International frameworks include the International Standards Organization (ISO) 27000-series publications. The authors give blueprints for designing, funding, establishing, and operating risk management groups. They identify staffing skill sets, including information security operations, information security management, and business analysis. The authors recommend skill set mixes, including a 30/70 ration of generalists to specialists. They discuss planning for change in a risk management group and note that while the cost of remediation for some vulnerabilities will decrease over time, so will the likelihood of their exploitation. This book supports my research by tying together technical information security topics and risk management topics with a plethora of real-world examples and considerations.

Straub, D. W., & Welke, R. J. (1998). Coping with systems risk: Security planning models for management decision making. *MIS Quarterly, 22*(4), 441-469. doi:10.2307/249551

Abstract. The likelihood that the firm's information systems are insufficiently protected against certain kinds of damage or loss is known as "systems risk." Risk can be managed or reduced when managers are aware of the full range of controls available and implement the most effective controls. Unfortunately, they often lack this knowledge, and their subsequent actions to cope with systems risk are less effective than they might otherwise be. This is one viable explanation for why losses from computer abuse and computer disasters today are uncomfortably large and still so potentially devastating after many years of attempting to deal with the problem. Results of comparative qualitative

studies in two information services Fortune 500 firms identify an approach that can effectively deal with the problem. This theory-based security program includes (1) use of a security risk planning model, (2) education/training in security awareness, and (3) Countermeasure Matrix analysis.

Summary. This article explores IT risk from both an information security and business continuity perspective. The authors term this collective risk "Systems Risk" (p. 442). This collective risk would be termed the "CIA Triangle" by information security practitioners, referencing the Confidentiality, Integrity, and Availability of business systems. The authors present four classes of countermeasures to these risks: Deterrence, Prevention, Detection, and Recovery. The authors argue that in the age of international threats (e.g., eastern European hacking groups) deterrence is not a valid or viable option as the certainty of sanctioning for an attack and the severity of the sanctions are vanishingly slim. The authors posit that managers are unaware of the full spectrum of actions available to reduce risk.

The authors detail two qualitative case studies in private-sector businesses. The case studies involve interviews with organizational leadership, risk inventories, information risk identification training, and follow-up surveys. The authors conclude that managers who are more fully informed of the risk mitigation options for systems risk are more likely to leverage these options to reduce risk within their organization. This article assists my research by connecting managerial understanding of information security risk and managerial comfort with risk mitigation strategies to the chance of success for information security risk assessment and reduction projects. This article also provides

backing for the idea that the uncertainty around information security risk for a business, while ever-present, can be knowable and tractable at a high level.

Wangen, G. (2017). Information security risk assessment: A method comparison. *Computer, 50*(4), 52-61. doi:10.1109/mc.2017.107

Abstract. Numerous methods for information security risk assessment (ISRA) are available, yet there is little guidance on how to choose one. Through a comprehensive risk identification, estimation, and evaluation framework, the author evaluates the practical application of three ISRA methods in terms of tasks required, user experience, and results.

Summary. This article is a comparison of three methods of Information Security Risk Assessment (ISRA): Operationally Critical Threat, Asset, and Vulnerability Evaluation – Allegro (OCTAVE A); ISO 27005; and the Norwegian Security Authority's Guidelines in Risk and Vulnerability Assessment (NSMROS). The authors posit that while plenty of ISRA methods exist, no method for evaluating the completeness and applicability of those methods exists. The authors use the Core Unified Risk Framework (CURF) to evaluate these methods on their completeness of coverage on 32 criteria and give each method a score of 0-2 for each criteria. The scores are tallied in both directions, for each method and each framework. This allows the reader to not only compare frameworks, but also to get an idea of which CURF criteria are best covered by all frameworks. The authors concluded that while the ISO 27005 total score was the highest, no single method had complete coverage of all criteria. This article assists my research by identifying business-friendly language to describe certain sub-processes within an overall project to design and implement a risk management strategy. Mapping existing information

security tasks to these sub-processes may improve the "digestibility" of information security project proposals to management.

Category C: Information Security Costs of Duplicate Services

Niemimaa, E, & Niemimaa, M. (2017). Information systems security policy implementation in practice: From best practices to situated practices. *European Journal of Information Systems*, *26*(1), 1-20. doi:10.1057/s41303-016-0025-y

Abstract. Organizations face institutional pressure to adopt information systems security (ISS) best practices to manage risks to their information assets. The literature shows that best practices should be contextualized, that is, translated from universal and general prescriptions into organizational documents and practices. Yet, little is known about how organizations actually make the translation from the best practices into situated practices. In this ethnographic study, we draw on practice theory and related concepts of canonical and non-canonical practices to analyze the process of translation. We explore how an IT service provider translated the ISS best practice of information classification into an ISS policy and into situated practices. We identify three translation mechanisms: (1) translating global to local, (2) disrupting and reconstructing local non-canonical practices, and (3) reconstructing and enacting local canonical practices. We find that while the translation was inhibited by incongruent practices, insufficient understanding of employees' work, and the ISS managers' lack of engagement in organizational practices, allowing situated practices to shape the ISS policy and actively engaging employees in the reconstruction of situated practices contributed positively to the translation. Contributions and implications for research and practice are discussed and conclusions are drawn.

Summary. This article explores the process of adapting and integrating Information Systems Security (ISS) best practices into organizational policies through an ethnographic study of a single organization. The authors relate the process of initial adaptation, iterative policy development through collaborative and gradual rework of existing policies, and the arrival at fully situated practices. The authors arrive at seven conclusions in the form of implications for putting ISS standards into practice. Among these implications are the acknowledgement that communication of new practices and methods to employees needs to be continuous and not a one-off event. Another implication notes that integration is by nature iterative and gradual and may last several years in organizations with high inertia or a large gap between existing and best practices. A third implication cautions that for an integration to be successful, the size and shape of this gap must be assessed by management before integration work begins. This assessment includes data classification, systems inventory, and extensive leveraging of employees' ground-level understanding of day-to-day operations. This article supports my research by providing definitions for keys terms, including data classification, and by providing insight and methods for realizing ISS changes in larger organizations.

Strebe, M. (2004). *Network security foundations*. San Francisco, CA: Sybex.

Introduction. The world of IT is always evolving, but in every area there are stable, core concepts that anyone just setting out needed to know last year, needs to know this year, and will still need to know next year. The purpose of the Foundations series is to identify these concepts and present them in a way that gives you the strongest possible starting point, no matter what your endeavor. Network Security Foundations provides essential knowledge about the principles and techniques used to protect computers and

networks from hackers, viruses, and other threats. What you learn here will benefit you in the short term, as you acquire and practice your skills, and in the long term, as you use them. Topics covered include: Why and how hackers do what they do [*sic*] How encryption and authentication work [*sic*] How firewalls work [*sic*] Understanding Virtual Private Networks (VPNs) [*sic*] Risks posed by remote access[*sic*] Setting up protection against viruses, worms, and spyware [*sic*] Securing Windows computers [*sic*] Securing UNIX and Linux computers [*sic*] Securing Web and email servers [*sic*] Detecting attempts by hackers [*sic*]

Summary. This book is a hybrid between a reference work and a course textbook. The author presents and explains concepts in each chapter, , and at the end of each chapter is a quiz consisting of 1-2 dozen questions about the chapter's content. The author reviews in moderate depth the technical foundations of information security. Examples include the difference between authentication (verifying a user's identity) and authorization (determining whether a user has the rights or permissions to use a particular resource). The author explains some of the causes of poor information security from an incentive model. As an example, companies that spend too many resources on security bear an opportunity cost that other companies that optimize their security spend do not. The author describes the needs of usage requirements and security requirements as largely overlapping. A usage requirement for user control over document permissions aligns well with the security requirement that document permissions be formalized in an Access Control List (ACL) and enforced by the Operating System (OS).

This book supports my research by providing definitions for some information security terms, including ACLs, and by providing a dispassionate, non-judgmental description of some of the reasons that information security is absent, lax, or underutilized.

Vacca, J.R. (Ed.). (2013). *Network and system security*. Rockland, MA: William Andrew.

Introduction. In this book, you will learn how to analyze risks to your networks and the steps needed to select and deploy the appropriate countermeasures to reduce your exposure to physical and network threats. This book will enhance the skills and knowledge of practitioners and IT professionals who need to identify and counter some fundamental security risks and requirements. Practitioners and IT professionals will learn some advanced network security skills pertaining to network threat identification and prevention. They will also examine Internet security threats and measures (audit trails IP sniffing/spoofing etc.) and learn how to implement advanced security policies and procedures.

Summary. This book is a technical dive into the state of modern information security as it relates to several common technologies. Each chapter is written by one or more leading experts in the field of information security. The book explores cloud security from the perspective of business continuity, regulatory compliance, and degree of control. The authors present Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS) with increasing levels of operational freedom at the cost of increasing security responsibility. The authors discuss cryptographic topics, including single- and mutual-authentication, key agreement, and encryption algorithms. As an example, mutual authentication allows a server and client to authenticate each other before exchanging private data. In a single-authentication scenario, the client

authenticates the server, a secure connection is established, and the two exchange data. If client authentication is required in a single-authentication scenario, it may be performed via higher level methods, for example, login/password combinations.

Intrusion Detection Systems (IDSs) are defined as hardware or software components that analyze network traffic to spot known malicious content and unknown anomalies. IDSs can alert a network administrator to malicious or suspect activity in Local Area Network (LAN) or Wide Area Network (WAN) traffic.

This book supports my research by providing definitions for some information security terms (e.g., IDS, IaaS), by presenting technical information security background (e.g., SSL), and by enumerating some of the ways that modern information security infrastructure helps to protect organizational assets.

Whitman, M. E., & Mattord, H. J. (2011). *Principles of information security*. Boston, MA: Cengage Learning.

Preface. The purpose of Principles of Information Security, Fifth Edition, is to fill the need for a quality academic textbook that surveys the discipline of information security. While there are dozens of quality publications on information security and assurance that are oriented to the practitioner, there is a dearth of textbooks that provide the student with a balanced introduction to both security management and the technical components of security. By creating a book specifically from the perspective of the discipline of information systems, we hope to close this gap. Further, there is a clear need for criminal justice, political science, accounting information systems, and other disciplines to gain a clear understanding of the principles of information security, in order to formulate interdisciplinary solutions for systems vulnerabilities. The essential tenet of this textbook

is that information security in the modern organization is a problem for management to solve, and not one that technology alone can address. In other words, the information security of an organization has important economic consequences, for which management will be held accountable.

Summary. This book is an extensive roadmap for planning and implementing information security within an organization. The authors lay out the case for managerial buy-in for information security infrastructure from business continuity and intellectual property (IP) perspectives. The authors conclude that modern businesses cannot feasibly function without information systems, and that a compromise of the confidentiality, integrity, or availability of these systems can cause significant harm to the business. Information security protects the organization's ability to function in an environment that can be uncertain and hostile. The authors detail instructions for configuring and auditing firewalls, planning for ongoing costs, and auditing and adapting existing security infrastructure; key recommendations include the deployment of multi-factor authentication (MFA), the installation and maintenance of hardware firewalls at network borders, and the use of offensive tools, including port scanning software, for defensive purposes.

As with any reference work in a highly dynamic field, this book will likely undergo significant updates and edits over the next decade. This book supports my research by providing definitions for several information security terms, including Virtual Private Networks (VPNs) – services that provide protected, private network connections over untrusted networks, and port scanners – software programs that send probing packets to remote computers to identify network-exposed services. This book also supports my

research by connecting increased system and network complexity with increased security risks through increased costs of asset inventory, through an increased likelihood of being affected by newly discovered software vulnerabilities, and by increased cost and complexity of defense and remediation efforts.

Zimba, A., Wang, Z., & Chen, H. (2018). Multi-stage crypto ransomware attacks: A new emerging cyber threat to critical infrastructure and industrial control systems. *ICT Express*, *4*(1), 14-18. doi:10.1016/j.icte.2017.12.007

Abstract. The inevitable integration of critical infrastructure to public networks has exposed the underlying industrial control systems to various attack vectors. In this paper, we model multi-stage crypto ransomware attacks, which are today an emerging cyber threat to critical infrastructure. We evaluate our modeling approach using multi-stage attacks by the infamous WannaCry ransomware. The static malware analysis results uncover the techniques employed by the ransomware to discover vulnerable nodes in different SCADA and production subnets, and for the subsequent network propagation. Based on the uncovered artifacts, we recommend a cascaded network segmentation approach, which prioritizes the security of production network devices.

Summary. This article explores the recent leveraging of unsecured or improperly secured systems by a particular class of malware known as ransomware. Ransomware is a class of malware that attempts to impact a service's availability by encrypting files on the target computer. The decryption key for those files is held for ransom by demanding payment in cryptocurrency for its release. The authors discuss potential vectors for malware to invade an organization from non-obvious connections and gaps in internal security. An example of non-obvious connections include the exposure of internal

systems to external attackers via legitimate but insecure functionality present in an external-facing system. Gaps in internal security include stale firewall rules that permit unnecessary traffic from low-security networks to high-security networks. The authors present a detailed analysis of malware obfuscation, logic traps, and anti-analysis code for the now-famous WannaCry worm; key findings include a rising sophistication of malware, an increase in multi-stage attacks targeted at specific assets within business internal networks, and the potential for increased damages to an organization if an initial compromise of a low-security asset leads to the compromise of a more valuable internal asset. This article supports my research by documenting the potential for multiplied costs to the organization of information security lapses beyond an initial infection or incident.

Conclusion

With a growing workforce, a growing service catalog, and pressure to optimize return-on-investment (ROI), the University of Oregon's Information Services (IS) department needs to find ways to improve the efficiency of operations. The removal of waste in the form of duplicate services is a viable avenue for IS to free labor and server resources while continuing to provide business functionality to the University. Risk management and Lean methodologies provide tools for identifying and categorizing waste.

Lean Background and Methodologies

Lean methodologies use the term *muda* and *mura* to describe waste and unevenness in production processes, respectively (Bell & Orzen, 2011). Muda and mura wastes in Information Technology (IT) organizations can surface in a variety of ways, including lost staff time, missed opportunities, duplicate services, and duplicate resource allocations (Bell & Orzen, 2011; Tribelsky & Sacks, 2010). Lean analysis of duplicate systems reveals additional costs in terms of duplicate computing resources, increased complexity of operations and regulatory compliance, duplicate documentation, misunderstandings between staff, divergent expectations from management, decreased technical agility, and lowered morale (Bell & Orzen, 2011; Taitsman, Grimm, & Agrawal, 2013). Decreased technical agility can lead to friction between IS and organizational leadership, especially if agility in IT departments at comparable organizations provides those organizations with a sustained competitive advantage (Bell & Orzen, 2011). To avoid these negative effects, IT leadership can evaluate implementing Lean methodologies to reduce duplication of services (Alhuraish, Robledo, & Kobi, 2017;).

Implementing Lean methodologies in IT will likely require cultural change for the IT department (Alhuraish, Robledo, & Kobi, 2017). To have the best chance of success, Lean

implementations need to include staff training and employee participation and have an organizational culture that is malleable and adapts to new challenges and clear support from organizational leadership (Alhuraish, Robledo, & Kobi, 2017; Hicks, 2007). Organizational leadership may be more amenable to the support of Lean IT implementation proposals that include perspectives from risk management (Hicks, 2007; Wangen, 2017).

Information Technology Risk Management Perspectives

Risk management views new issue mitigation proposals through the lenses of severity, likelihood, and remediation costs for a business-impacting event (Benaroch, Lichtenstein, & Robinson, 2006). Proposals that attempt to mitigate an issue that has a low severity, low likelihood of occurrence, or a high or uncertain remediation cost are often rejected or assigned a lower priority (Benaroch, Lichtenstein, & Robinson, 2006). Issue mitigation proposals must take into account not only the financial costs of mitigation, but the likelihood of implementation success within the current organization's culture (Cruz, Peters, & Shevchenko, 2015).

The success rates of projects that address these issues drop with political conflicts between user groups (Alhuraish, Robledo, & Kobi, 2017). Success rates rise with clear and consistent support from organizational leadership, sufficient resource allocation, and proposals that are written with terms and language that are familiar and easy for management to grasp and incorporate (Alhuraish, Robledo, & Kobi, 2017; Benaroch, Lichtenstein, & Robinson, 2006; Wangen, 2017). Projects that are likely to involve user group conflicts may still succeed with a strong mandate and adequate funding from leadership (Benaroch, Lichtenstein, & Robinson, 2006). The organizational risks of implementing Lean IT methodologies may not be inconsequential, as Lean implementation projects can be derailed by intractable employees or capricious leadership (Alhuraish, Robledo, & Kobi, 2017; Benaroch, Lichtenstein, & Robinson,

2006). However, the risks to the organization of doing nothing may be even greater (Kouns & Minoli, 2010; Vacca, 2013; Whitman & Mattord, 2011; Zimba, Wang, & Chen, 2018).

Leaving duplicate services in place can perpetuate situations where organizational risk is unnecessarily elevated (Whitman & Mattord, 2011). Free market forces incentivize software publishers to only fix bugs that bring loss of sales, legal liability, or a negative reputation to the publisher (Strebe, 2004). A linear increase in the number of servers and software packages involved in providing duplicate services leads to an exponential increase in the possibility of undiscovered software bugs (Vacca, 2013, Zimba, Wang, & Chen, 2018). A rise in undiscovered software bugs leads to an elevated risk of losing or exposing data that is sensitive to the organization or to the customer (Kouns & Minoli, 2010; Zimba, Wang, & Chen, 2018). Leaving duplicate services in place also has direct and indirect administrative costs (Bell & Orzen, 2011; Straub & Welke, 1998; Whitman & Mattord, 2011).

Maintaining duplicate services has a direct cost in staff time and process overhead (Whitman & Mattord, 2011). Duplicate services may also suffer from non-uniform competency and customer service levels among technical administrative staff (Bell & Orzen, 2011; Cruz, Peters, & Shevchenko, 2015). Duplication of services carries an additional elevated risk of mistakes in internal documentation that lead to discrepancies in the handling of customer issues (Bell & Orzen, 2011). This unevenness (mura) can surface as inconsistency in the service users' experiences, leading to an elevated risk of internal and external customer frustration (Bell & Orzen, 2011). Indirect administrative costs of maintaining duplicate services also include costs from information security operations (Whitman & Mattord, 2011).

Information Security Costs of Duplicate Services

Information security operations attempt to mitigate vulnerabilities and risks to organizational data and digital infrastructure (Whitman & Mattord, 2011). Each additional software package that is deployed comes with its own set of operational security and data confidentiality considerations (Kouns & Minoli, 2010; Niemimaa & Niemimaa, 2017). The integration of duplicate services increases the complexity of organizational infrastructure in a way that can lead to nonobvious or unexpected vulnerabilities that would not exist in either service individually (Niemimaa & Niemimaa, 2017; Whitman & Mattord, 2011). Duplicate services administered by disparate groups with different priorities and motivations may not be uniformly secured (Whitman & Mattord, 2011). As the number of software packages increases, so do the permutations of paths and pivot points that an attacker can exploit for additional access by moving vertically and laterally within an organization's network (Whitman & Mattord, 2011).

Final Thoughts

Duplicate services have hidden costs beyond their immediate operational budgets (Bell & Orzen, 2011; Cruz, Peters, & Shevchenko, 2015; Whitman & Mattord, 2011). Increasing infrastructure complexity increases opportunities for attackers and increases the chance of nonobvious risks that arise from combinations of existing security vulnerabilities (Whitman & Mattord, 2011; Zimba, Wang, & Chen, 2018). To improve operations and information security and reduce organizational risk, duplicate services should be evaluated for consolidation (Bell & Orzen, 2011; Whitman & Mattord, 2011). Organizational leadership should weigh the full cost of running duplicate services when evaluating consolidation proposals (Niemimaa & Niemimaa, 2017).

Lean's track record in manufacturing is well documented as a successful avenue to reduce overhead in production environments (Bell & Orzen, 2011; Tribelsky & Sacks, 2010). From a Lean perspective, effort and expenditures that do not provide value to an organization can be considered waste (Arunagiri & Gnanavelbabu, 2014). Lean methodologies that reduce waste can be applied to IT service management as a foundation of an argument for de-duplication of services (Bell & Orzen, 2011; Hicks, 2007).

Lean offers managers a view into IT operations from a minimalist perspective (Hicks, 2007). Lean strives for simplicity and rationalization of internal processes and external services (Bell & Orzen, 2011; Hicks, 2007). Risk management lends methods for calculating the likelihood of an incident and developing prioritization matrices for decision-makers (Benaroch, Lichtenstein, & Robinson, 2006 ; Cruz, Peters, & Shevchenko, 2015). Managers that use these tools can improve their teams, their services, and their organization (Cruz, Peters, & Shevchenko, 2015; Kouns & Minoli, 2010).

References

Alhuraish, I., Robledo, C., & Kobi, A. (2017). A comparative exploration of lean manufacturing and six sigma in terms of their critical success factors. *Journal of Cleaner Production, 164*, 325-337. doi:j.jclepro.2017.06.146

Arunagiri, P., & Gnanavelbabu, A. (2014). Identification of major lean production waste in automobile industries using weighted average method. *Procedia Engineering, 97*, 2167-2175. doi:10.1016/j.proeng.2014.12.460

Bell, S., & Orzen, Michael A. (2011). *Lean IT: Enabling and sustaining your lean transformation*. New York, NY: Productivity Press.

Benaroch, M., Lichtenstein, Y., & Robinson, K. (2006). Real options in information technology risk management: An empirical validation of risk-option relationships. *MIS Quarterly, 40*(4), 827-864. doi:10.2307/25148756

Camp, L. J., & Wolfram, C. (2004). Pricing security. In L.J. Camp & S. Lewis (Eds.), *Economics of information security advances in information security* (17-34). Boston, MA: Kluwer Academic Publishers.

Cruz, M. G., Peters, G. W., & Shevchenko, P. V. (2015). *Fundamental aspects of operational risk and insurance analytics: A handbook of operational risk*. Hoboken, NJ: Wiley.

Hicks, B. (2007). Lean information management: Understanding and eliminating waste. *International Journal of Information Management, 27*(4), 233-249. doi:10.1016/j.ijinfomgt.2006.12.001

Lean manufacturing (2018). In *Cambridge English Dictionary*. Retrieved from https://dictionary.cambridge.org/us/dictionary/english/lean-manufacturing

Straub, D. W., & Welke, R. J. (1998). Coping with systems risk: Security planning models for management decision making. *MIS Quarterly, 22*(4), 441-469. doi:10.2307/249551

Strebe, M. (2004). *Network security foundations*. San Francisco, CA: Sybex.

Taitsman, J. K., Grimm, C. M., & Agrawal, S. (2013). Protecting patient privacy and data security. *New England Journal of Medicine, 368*(11), 977-979. doi:10.1056/nejmp1215258

Tribelsky, E., & Sacks, R. (2010). Measuring information flow in the detailed design of construction projects. *Research in Engineering Design, 21*(3), 189-206.

University of Florida Center for Public Issues Education. (2014). *Evaluating information sources.* Retrieved May 18, 2018, from http://www.piecenter.com/wp-content/uploads/2014/08/evaluateinfo.pdf

Vacca, J.R. (Ed.). (2013). *Network and system security*. Rockland, MA: William Andrew.

Wangen, G. (2017). Information security risk assessment: A method comparison. *Computer, 50*(4), 52-61. doi:10.1109/mc.2017.107

Whitman, M. E., & Mattord, H. J. (2011). *Principles of information security*. Boston, MA: Cengage Learning.

Zimba, A., Wang, Z., & Chen, H. (2018). Multi-stage crypto ransomware attacks: A new emerging cyber threat to critical infrastructure and industrial control systems. *ICT Express, 4*(1), 14-18. doi:10.1016/j.icte.2017.12.007