

5-2018

Improving Information Alignment and Distributed Coordination for Secure Information Supply Chains

Omar Eldardiry
Purdue University

Follow this and additional works at: https://docs.lib.purdue.edu/open_access_dissertations

Recommended Citation

Eldardiry, Omar, "Improving Information Alignment and Distributed Coordination for Secure Information Supply Chains" (2018). *Open Access Dissertations*. 1720.
https://docs.lib.purdue.edu/open_access_dissertations/1720

This document has been made available through Purdue e-Pubs, a service of the Purdue University Libraries.
Please contact epubs@purdue.edu for additional information.

IMPROVING INFORMATION ALIGNMENT AND DISTRIBUTED COORDINATION FOR SECURE INFORMATION SUPPLY CHAINS

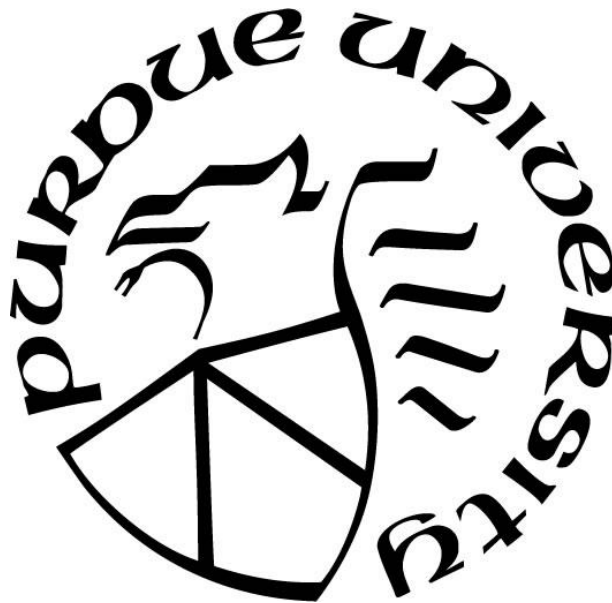
by
Omar Eldardiry

A Dissertation

Submitted to the Faculty of Purdue University

In Partial Fulfillment of the Requirements for the degree of

Doctor of Philosophy



School of Industrial Engineering

West Lafayette, Indiana

May 2018

THE PURDUE UNIVERSITY GRADUATE SCHOOL
STATEMENT OF COMMITTEE APPROVAL

Dr. Barrett S Caldwell, Chair

School of Industrial Engineering

Dr. David S Ebert

School of Electrical and Computer Engineering

Dr. J. Eric Dietz

Department of Computer and Information Technology

Dr. Yuehwern Yih

School of Industrial Engineering

Approved by:

Dr. Abhijit Deshmukh

Head of the Graduate Program

To my beloved wife

ACKNOWLEDGMENTS

I would like to express my sincere gratitude to my dear advisor, Barrett Caldwell, for his impact on my academic achievement is hard to describe in words. I thank him for teaching me the art of doing research, his active involvement in every aspect of my graduate career, and for the incredible collaborative lab environment he created for all his students.

Only because of that environment was I able to learn so much from my dear lab-mates. Thank you for every member of the lab for what I learned from you and the fun memories we shared throughout our journey.

My deepest gratitude goes to my beloved wife for her endless support and patience days and nights while I worked on my degree. I could not have done it without you. I can never thank you enough Safaa!

I want to express my greatest appreciation to my dear father for cultivating my passion for the field of industrial engineering, and for his inspiration and guidance throughout my industrial engineering career.

A huge thank you to my mother for raising me to value education and empowering me to be the best I can be. I am also very lucky to have my wonderful siblings. Your encouragement through the downs and cheering through the ups were both priceless.

Last but not least, many thanks to my Jon Boney, for helping me expand the impact of my research work by inspiring me to apply it in real-world business settings.

TABLE OF CONTENTS

LIST OF TABLES	viii
LIST OF FIGURES	ix
ABSTRACT.....	x
Introduction.....	12
Information Technology Advancements	12
Information Systems Threats on Businesses	14
IT Challenges.....	15
Cyber Physical IT Networks Vs IT Applications	17
IT System Emphases.....	18
Information Supply Chains.....	19
Research Overview	19
LITERATURE REVIEW	22
Information Display in Dynamic Event Driven Environments	23
Network Security Situation Awareness	24
System Architecture and Usability of COP	25
Human Cognition Elements of Information Processing and Task Analysis	26
Team Collaboration	27
Knowledge Capture and Organizational Capability	27
IT Deployment in Operations	28
Enterprise Systems Integration	29
Research Organization.....	29
METHODS AND INITIAL FINDINGS	30
Layer 1: External Entities	31
Layer 2: Liaison between the user and provider	31
Layer 3: The User	31
Project 1: Security and Network Operations	32
Data Collection and Analysis.....	32
Data Collection: RSA Security Conference Interviews	34

Case Study: Security Operations of a Global Manufacturing Organization	38
Project 2: Distributed Supply Chain Network Operations.....	43
Project 2 Background.....	43
Data Collection	46
Definition	47
System Design	50
Interface Design	52
Testing.....	56
Tool Deployment	57
OVERALL RESULTS.....	58
Project 1: Security and Network Operations	58
Tool 1: Information Alignment and Team Situation Awareness	58
Tool 2: Management of Team Performance	59
Tool 3: Operational Knowledge Referencing and System Teaching.....	59
Project 2: Distributed Supply Chain Network Operations.....	60
Interview Results	61
Integration	63
Business Impact	64
Cost Reduction.....	67
Security Operations and Impacts Beyond Operations and Finance	68
DISCUSSION	70
Processes of Implementation and Advancement for Distributed Information Supply Chains .	71
UX Research: Corporate Systems Vs Consumer Applications	72
Impact on Business Acquisitions	75
End to End Visibility	76
Research Limitations	77
CONCLUSION.....	79
REFERENCES	84
APPENDIX A. RSA Conference.....	90
INTERVIEWS SCRIPT	90
DATA COLLECTION	91

Participant 1	91
Participant 2	92
Participant 3	93
Participant 4	94
Participant 5	96
Participant 6	97
Participant 7	98
Participant 8	99
APPENDIX B. SOC CASE STUDY	101
DATA COLLECTION	101
Primary Findings.....	102
Secondary Findings.....	103
INTERVIEW RESPONSES	104
Participant 1 (Team Lead).....	104
Participant 2 (level 1 analyst)	107
Participant 3 (level 3 analyst)	109
Participant 4 (level 2 analyst)	112
Participant 5 (level 3 analyst)	114
Participant 6 (Area Manager).....	116
APPENDIX C. PROJECT 2	119
INTERVIEW RESULTS (ROUND 1)	119

LIST OF TABLES

Table 1 Interview Participants from 4 Distribution Centers	52
Table 2 Associate’s User Profile.....	53
Table 3 Supervisor's User Profile	54
Table 4 Operations Manager’s User Profile	54
Table 5 Plant Manager’s User Profile.....	54
Table 6 Senior Management’s User Profile.....	55
Table 7 HR Manager’s User’s Profile	55
Table 8 Project Manager’s User Profile.....	55
Table 9 Plant Controller’s User Profile	56
Table 10 Interview Results Highlights – Project 2 Phase 1	62
Table 11 Examples of Permission Rights in the Organization	69

LIST OF FIGURES

Figure 1 Cloud Computing Infrastructure (Marston et al., 2011).....	13
Figure 2 Network Security Situation Awareness Model (Onwubiko, 2009).....	25
Figure 3 Research Methodology	30
Figure 4 Human Factors Engineer's Role in Enterprise Systems Deployment	32
Figure 5 Methodology Progression.....	34
Figure 6 Interview Participant's Drawing of a Bank's Network	35
Figure 7 Interaction Between Junior and Senior Analysts.....	41
Figure 8 Management Hierarchy Involved in Project Implementation	44
Figure 9 All Methodology Phases Applied to Project 2	47
Figure 10 Functional Teams' Interaction During Planning Phase.....	51
Figure 11 task variation across shifts.....	65
Figure 12 labor utilization across plants	66
Figure 13 Organizational Hierarchy	71
Figure 14 Slide 1 - Supervisors Reports Mockup.....	119
Figure 15 Slide 2 - Functional Managers Reports Mockup.....	120
Figure 16 Slide 3 - Inventory Control Manager Reports Mockup.....	120
Figure 17 Slide 4 - Plant Manager Reports Mockup	121
Figure 18 Slide 5 - North America Executives Reports Mockup	121

ABSTRACT

Author: Eldardiry, Omar, M. PhD

Institution: Purdue University

Degree Received: May 2018

Title: Improving Information Alignment and Distributed Coordination for Secure Information Supply Chains.

Major Professor: Barrett Caldwell

Industries are constantly striving to incorporate the latest technology systems into their operations so that they can maintain a competitive edge in their respective markets. However, even when they are able to stay up to speed with technological advancement, there continues to be a gap between the workforce skill set and available technologies. Organizations may acquire advanced systems, yet end up spending extended periods of time in the implementation and deployment phases, resulting in lost resources and productivity. The primary focus of this research is on streamlining the implementation and integration of new information technology systems to avoid the dire consequences of the process being prolonged or inefficient.

Specifically, the goal of this research is to mitigate business challenges in information sharing and availability for employees and managers interacting with business tools and each other. This was accomplished by first interviewing work professionals in order to identify gap parameters. Based on the interview findings, recommendations were made in order to enhance the usability of existing tools. At this point, the research setting was shifted from network operations to supply chain operations due to the restrictive nature of network operations. The research team succeeded in developing a user-centered methodology to implement and deploy new business systems to mitigate risk during integration of new systems as the transition is made from the classic way of performing tasks. While this methodology was studied in supply chain operations, it enabled the identification of a common trend of challenges in operations work settings, regardless of the business application. Hence the findings of this research can be extrapolated to any business setting, besides the ones actually studied by the team. In addition, this research ensures that operational teams are able to maximize their benefit out of the technology available, thus enabling them to keep up with the rapidly evolving world of technology while minimizing sacrifices in resources or productivity in the process.

Traditionally, it has been more convenient, and thus more prevalent, for research in the areas of cognitive human factors, user research and UX principles to be conducted on consumer applications, as opposed to enterprise systems. The larger number of users of consumer applications and the research process being less complicated than it is in enterprise systems are contributing factors to this research trend. The result is that there is research available on every aspect of integrating new systems into consumer applications. Due to the need for research in these areas in enterprise systems research efforts have been on the rise. However, most of these focus on tool development rather than system deployment. This research team expanded the research arena by conducting UX research on the deployment of a system into an operations setting. Thus, the emphasis was on corporate systems, rather than consumer applications, and it was determined that the benefit of conducting research per user is higher in the corporate setting than in consumer applications, making such research efforts a worthwhile investment of resources.

INTRODUCTION

Today's businesses are capable of capturing large amounts of data about their operation. With continuous advances in computing technology, the challenge of collection and storage of data is diminishing. Today's real challenge is to analyze the large amounts of available data, and present it in an efficient and secure manner to the key decision makers in the business organization.

Investing to overcome such challenges can prove to be highly rewarding regardless of the business application or the level of organization. In recent years, information technology (IT) investment has accounted for more than 50 percent of all of the capital investments made by US corporations (Laudon & Laudon, 2012). Research and accredited education programs are renovating their curricula towards topics like visualization, machine learning, big data analytics, and other areas that supplement or enhance the benefits of large amounts of data available.

In the past, organizations were able to analyze data periodically to learn about evolving trends, hence make necessary adjustments. Today's competitiveness and fast pace forces organizations to make critical decisions continuously. Periodic analysis is no longer the solution. However, classic tools are still used today (such as spreadsheets) where data are manually processed and analyzed.

While spreadsheets and other manual tools might have been an effective approach in the past, it imposes great limitations with today's need for augmenting information generation. The classic approach takes longer time than may be available for decision making, requires analysts to perform repetitive steps to organize and clean up the data, and it does not allow to fully discover what data represents. It is crucial for businesses to have the capability to investigate data with more flexibility to advance their businesses and drive for efficiency and profitability.

Information Technology Advancements

The growth of IT industry is highly dependent on the digitization capabilities of creating, sharing and utilizing more digital data, information and knowledge. The IT business started with the first generation of giant digital mainframe systems used to process different transaction activities for different businesses, such as financial transactions, airline reservations and manufacturing production (G. Press, 2013)(G. Press, 2013).

The impact of computers was limited at the time since transactions were always bounded between a single machine and a small number of users. This rapidly evolved when Local and Wide area networks (LAN/ WAN) were established. It enabled multiple computers to communicate on site and between remote locations of organizations which expanded the amounts of stored data; and therefore, the availability, processing and use of this data.

The Internet, initially only available to military and educational institutions, established a significantly wider range of communications. Digital illegal activities were evolving side by side with advancements in the field. However, numbers of hackers and attacks tremendously increased when the internet or World Wide Web was made available for other organizations and individuals across the globe. The World Wide Web is the one event that has the greatest impact on the IT industry (G. Press, 2013). Cloud computing is seen by organizations as a great opportunity with a wide range of business applications and agility providing real time data at the fingertips of their employees. IT departments within these organizations, however, see this as a security threat to the business (Marston, Li, Bandyopadhyay, Zhang, & Ghalsasi, 2011).

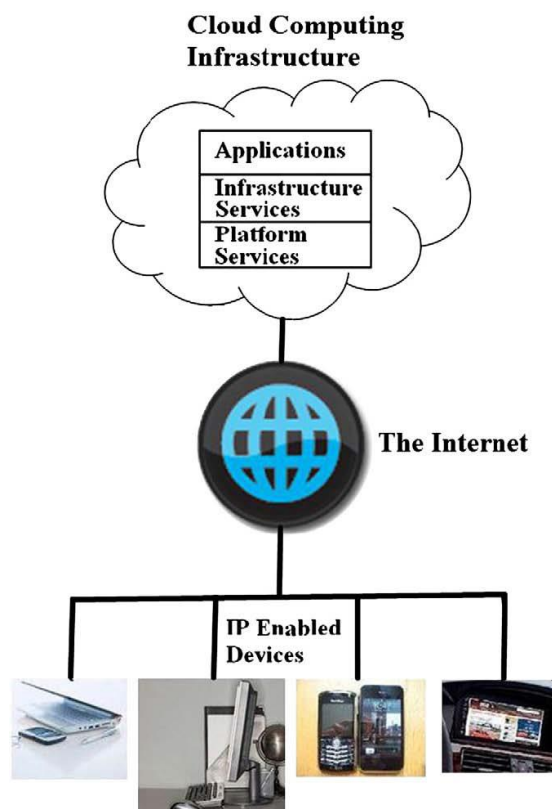


Figure 1 Cloud Computing Infrastructure (Marston et al., 2011)

The internet was designed to share information and not to protect it. As a result, digital crimes created more demand for IT employees. Since more people now have their personal and business information uploaded into “the cloud” (virtual internet-accessible storage) for various applications, the number of hacking attempts keeps rising, increasing the demand for cyber security.

Internet communications created new markets and more business opportunities. It amplified the demand of IT professionals. Demand of IT professionals is continuously increasing today especially with new technologies introduced such as smartphones, tablets, personal computers, and the increasing use for the internet of things and cloud computing applications.

Information Systems Threats on Businesses

IT applications are continuously growing in a wide variety of businesses. Aviation, banking, manufacturing, healthcare, education, energy, and other businesses rely on information technology and observe large amounts of new digital transactions and records on daily basis. Growth in and the technological advancement of cyber infrastructure networks create new challenges to maintain robust system performance. The cost of cyber breaches, data theft, and other hacking incidents continues to grow. Recovering from such incidents may take days, yet the effects last for long months or years in some occasions to regain the business’ integrity and reputation for security. Avoiding or at least taming the effects of those incidents is always of high priority.

Organizations are tempted to take advantage of new technological innovations. New technology opens new business opportunities to augment profits. IT professionals are often unable to cope with the fast pace of such technological advancements. Technology on the other side is also a tool misused in cybercrime by hackers. Technological sophistication represents another challenge to network and security IT organizations.

Businesses develop resilience strategies to face challenges that interrupt their functionality. Interruptions can happen due to machine failure, human errors, or lack of materials. Function loss also occurs due network malfunction that can be caused by external/uncontrolled events that greatly impact business processes. Examples of non-hacking incidents still demonstrate significant adverse effects on the organization, including the following illustrative examples.

- Information Technology at Purdue University (ITAP) group is responsible for IT operations and infrastructure for Purdue University Campus. ITAP reported damage due

to a tornado in November 2013. Damage hindered the operation to maintain its customers' expectations. Purdue webmail services were not functioning for most users for 48 hours.

- In November 2012, a computer breakdown in an United Airlines operations center for two hours impacted schedules of 250 flights and thousands of United Airlines customers (Associated Press, 2012). This caused failure of information delivery necessary to crew to be able to operate the flight. Even after the system was fixed the effect of breakdown had a ripple effect on operation. Such incidents can translate to customer disloyalty that takes years to restore.

IT Challenges

Organizations are challenged to maintain three attributes of IT network operation: (1) network security, (2) network health and (3) network performance. First, a clear understanding of different system components that affect those attributes must be available. Security teams cannot set the best protection strategies without knowing the most valuable organization data that need to be protected. Network teams similarly must have a clear definition of the critical assets that operations rely on and available alternatives and backups in case of damages that might occur.

Infrastructure, apps, data, security tools and personnel (employees, vendors, suppliers, and partners) are all part of this system and interact in different ways. Any of the components or link between them can act as a source of vulnerability or hinder the work operation. Information breaches or downtime always lead to customer dissatisfaction and impose costs to the organization. The larger the size of the organization, the more changes and transactions it performs in short periods of time. The failure to cope with this fast pace of activities also adds to the system's vulnerability.

Professionals must realize that uncontrollable system components will always exist. That means maintaining a 100% secured, fully operational process at all times is impossible. And so, increasing the level of security and productivity is obtained by focusing on the most valuable assets rather than equally protecting and monitoring all components.

IT operation is often separated into two distinct functions; Network Operation Centers (NOCs) and Security Operation Centers (SOCs). Both functions share multiple commonalities in how they operate with some differences in scope (depending on the organization). It is also common for some organizations to combine both functions into a single operations center. Other

organizations prefer to outsource the network management operations to external service providers. Combining and outsourcing decisions rely on the organization's size, business nature, privacy policy and sensitivity of the organization's information. The data collected in this dissertation covers both organizations types that separate or combine both functions.

Security Operation Centers (SOCs) manage organizations' network security related activities. Roles include any activities related to three critical aspects of an organization's information security: Confidentiality, Integrity and Availability. Network Operation Centers (NOCs) manage organizations' network health and performance. The roles in this case are related to network monitoring and control, troubleshooting, and incident response to physical adverse events such as power outage, memory shortage, system freeze or other similar failures.

NOCs and SOCs use large visual displays to deliver information to analysts that support their decision making. It is certain that the amount of information generated very highly exceeds the processing capabilities of human teams in SOCs/ NOCs. A key success to NOC/SOC teams is to provide the "needed" information to analysts at the "right" time. Failure of delivering the needed information to decision makers in a timely manner can create additional costs and time delays for the organization.

The ability to isolate the relevant information, present efficiently within the right context to the analyst expedites his responsiveness and improves the timeliness and quality of the decision-making process. It increases the level of Situation Awareness (SA) and performance of IT analysts and professionals (Onwubiko, 2009).

SA requirements for IT analysts must be determined and then materialized in information presentation to ensure accomplishing work goals in efficient manner. SA requirements for team leads and managers are also necessary, taken into consideration not only information about the network but also about team performance and work goals.

Similar to IT infrastructure network and security operations, Operational teams in other business applications encounter their own set of challenges. Each have their own set tools, information systems that support their operation. A security breach or network failure in a network operation requires analysts advanced tools to troubleshoot and mitigate. Similarly, supply chain analysts require other tools to track goods from raw material state until maturing a finished product delivered to the hands of the customer.

The research presented in this dissertation argues that implementing and deploying such tools in operations in most cases, is performed in a deficient way that hinders operational teams from integrating the tools into their daily work routine in a smooth way. While the research specifically focused on IT operations, and supply chain operations. The author argues that the method proposed applies to other operations teams attempting to integrate an information system.

Cyber Physical IT Networks Vs IT Applications

This dissertation studied two digital systems found in every global organization: security and network operations in cyber-physical networks, and business-oriented enterprise applications using those networks. Both digital systems are interconnected and supplement each other. From a systems perspective, the input of these systems is the set of digital transactions taking place within the workplace or interacting with an external entity. This includes sending an email, processing an ERP command to issue a work order, or compiling data to issue a financial report. The goal of teams working in this environment is to ensure the network is available and secured at all times to all business segments within the organizations. The environment is almost identical across organizations. The source of variation is mainly the size of the organization in terms of the number of employees and locations it possesses.

A change of focus to emphasize IT applications systems that business teams rely on to complete tasks helps to recognize the challenges of effective use of IT networks to achieve business goals. The input of these systems is related to the core of the business. The IT systems of a hair salon, airline carrier and a manufacturing firm are different due to the unique elements of the business itself. Information within a system must be presented to the user in a way that will allow them to their job efficiently.

Each system has its unique characteristics and priorities. For example, the pace of digital data generated from network activities is much higher than other physical based operations; yet they both share great commonalities when studying the supply chain of information (data generation, data collection, analysis, information presentation, knowledge sharing, decision making, and system feedback).

Organizations to manage and control activities require human intervention to monitor, investigate and resolve large numbers of transactions beyond its capabilities. Organizations often cannot

afford to hire enough employees, due to both expense and lack of qualified personnel available. Organizations therefore do not have a choice but to optimize their operations.

IT System Emphases

Trading your Honda for a Ferrari will not guarantee you arriving to work on time every day if you keep selecting the same busy route. In other words, having the most up to date/expensive tools can improve efficiency of operation but is not always the solution. Bad practices are never eliminated simply by acquiring new tools.

Project 1 in this dissertation, for example, shows how IT tools often generate large amounts of alerts that overwhelm analysts in network and security operations settings. An intrusion tool used by analysts in cybersecurity operations may show thousands of malicious IP addresses or other sources of “possible” threats. It is very hard to filter this large amount of transactions to prioritize the real/ most serious threats in this case. Critical information must be first isolated, before being presented to analysts within the right context to enable analysts perform corrective actions in a timely manner. The right context meaning gathering all related information to each incident in one location. Using different tools to investigate a malicious attack without integration impacts responsiveness.

Expanding on the incident response example, it is important to note the fact that hackers are aware of the available tools in the market, meaning that hackers can be a step ahead with respect to security teams. If motivated enough, a hacker will keep trying until he/she finds the way to intrude the system and acquires what he/she is looking for.

Beside tool limitations, the usability and deployment of IT tools used by a large team are two other great challenges discussed in detail in “Project 2”. Subject matter experts in physical operations applications do not necessarily possess a strong IT background similar to network operations analysts. Subject matter experts in this case are not qualified to select the analytical tools to be used or how to be integrated in their daily operation.

Business compliance to governmental and global regulations is best to be driven by advanced information systems where proof of activities can be documented. The specific application deployed in project 2 enabled a supply chain operation team of a global consumer goods brand to comply with the “Customs-Trade Partnership against Terrorism (C-TPAT)”, a U.S. Customs & Border Protection partnership with businesses that is designed to strengthen and improve overall

international supply chain security from point of origin to destination. This certification entails significant savings to the business when receiving and shipping containers of products through ports in the United States. This benefit will be further explained in the results section of this dissertation, and represents one significant gain achieved by business emphasis on “secure information supply chains” for managing physical goods, production processes, and materials information, as well as confidentiality, integrity, and availability of data and transactions.

Information Supply Chains

A key goal of successful supply chain management is providing end to end visibility of goods and services status starting at the supplier of raw materials all the way to the end user passing by all the chains of the network. The dissertation uses this analogy to highlight the significance of information availability within businesses. In “information supply chains”, the information is the critical resource being managed, not the goods or services being produced and sold. Sources of information generation, such as business transactions, market trends, shipment delays, and employee performance, become internal suppliers to the organization’s information supply chain. Customers of the information supply chain include operations managers, sales reps, demand planners and other professionals in the workplace that rely on information available to perform their daily tasks and meet their strategic goals. The roles of the human factors engineer and user experience (UX) practitioner are to ensure that the information (product) delivered to the employee (customer) is presented in a manner that aligns with his/ her tasks and decision making needs based on their hierarchy and responsibility within the organization.

Exploratory data collection for this research started in cyber network and security operations settings. Then based on results and lessons learned, research continued in supply chain operations settings to deliver a fully operational workforce analytics integration with a manufacturing organization’s ERP system. Methods Chapter shows in details how primary (operations team) and secondary (HR, Finance) system users were involved in an early stage of the implementation to ensure ROI of the tool is maximized.

Research Overview

The focus of this dissertation is on the information flow aspects of cyber-physical systems that support business operations. It considers both digital (cyber) and material (physical) components

within a production enterprise, and considers a common information flow that describes their joint performance in the organization.

The dissertation initially focused on security and network operations (Project 1). This project was funded by the Purdue Center for Education and Research in Information Assurance and Security (CERIAS). The project allowed the author to address existing business gaps focused on cybersecurity operations. Network and security analysts are lacking tools necessary to understand the status of their network in a timely manner. This is essential to support incident response, team collaboration and preparedness to respond to both internal and external potential threats.

With further exposure to business operations settings, in work environments outside network and cyber security operations, the author noted that the challenge exists across different business settings with different implications. Operations teams, regardless of the application, tend to have similar struggles interacting with complex business systems and with each other when executing critical time-sensitive decisions. A new opportunity (Project 2) enabled the author to expand on Project 1 findings to fully implement a tool that enabled a global consumer goods organization to integrate an automated system of measuring and managing performance of their workforce in the North American distribution network.

The initial purpose of this dissertation was to serve the goal of ensuring delivery of shared information in networks in a secured way. The challenge is to (1) manage the tremendous amount of continuous information flow supported by current and future networks, (2) ensure information delivery by managing network assets, health and performance; and (3) securing information against growing motivated intelligence of illegally accessing personal and business information. The purpose evolved to put together a user-centered systematic approach to allow operational teams in a variety of business contexts to integrate information systems tools in an efficient manner with minimal interruption to their routine operation. A step necessary to enable businesses utilize technological advancements, industry 4.0, and internet of things.

The next chapter presents relevant research focused on information technology systems design, evaluation and implementation in complex cyber- and cyber-physical operations settings. Issues of information integration, presentation and visualization, and concepts of situation awareness, are discussed in the context of enhancing interaction with professionals in the workplace with systems driving their tasks and goals. Chapter 3 describes Project 1 methods and initial findings, as well as additional discussion of Project 2 methods. Chapter 4 presents results of the full system

implementation and outcomes in Project 2, while Chapter 5 includes a broader discussion of issues and contexts of information technology system implementation in cyber-physical operations, including issues of technology acquisition and integration. Chapter 6 provides a conclusion and suggestions for additional work in this area.

LITERATURE REVIEW

Information Visualization and User Experience (UX) tools designers often follow a user centered-designed approach to be able to build tools for users working in specific environments. This ensures they can be equipped with tools that fit their needs and help them fulfill their unique tasks and work goals. Designers start with defining the tool characteristics based on user input and description of his/her work goals and what information is relevant to these goals or tasks on hand. The designer then develops a prototype and goes back to the user for testing. This process keeps reiterating until the user is satisfied with the final product and his/ her feedback addressed (Endsley, 2012).

The challenge in cyber physical operation centers is that users (in this case IT analysts) may not have a clear definition of the system. It is hard to quantify the different processes in cyber-physical network operations performed by analysts in this event driven environment. Also, it is important to note that, in many cases, the system customer is not necessarily interested in the cyber system itself but the physical components sitting on top of it. Recalling the airline dispatch example, the customer only cares about the planes leaving and arriving on time.

Network operation centers are event driven systems that carry lots of distraction to teams of analysts. The high variation and multi-tasking nature of analysts' responsibilities add another layer of complexity to network monitoring and management. Continuous system logs and events produce a high rate of data flow to the operations centers. Automated processing and algorithmic scans of network operations data are intended to filter out irrelevant information. However, visualization of information after processing remains a challenge, and still exceeds human cognitive processing capability.

This chapter presents literature regarding design methodologies of information visualization such as common operational pictures and user center design that are previously implemented in complex dynamic work environments such as IT operations. It also highlights previous research about human sense making, situation awareness and team collaboration in complex event driven working environments. This research summary is followed by an overview of techniques implemented in data collection and analysis of the research such as operational knowledge referencing, goal directed task analysis and heuristic usability evaluation. The chapter finally presents the impact

of IT investment and analytics on global organizations' productivity of operations and knowledge sharing among their distributed teams.

Information Display in Dynamic Event Driven Environments

Common operational picture (COP) types of displays were built to assist operational efficiency in military settings (M. D. McNeese & Brown, 1986). COP facilitated teamwork for military operations enabling remote teams and the command hierarchy creating collaborative platform (Brewer & McNeese, 2004). COP concepts have expanded to other fields such as civilian crisis management (Mcneese et al., 2006), utilities management such as the power grid (Blais, Goerger, Richmond, Gates, & Willis, 2005) and traffic incident management (Steenbruggen, Nijkamp, Smits, & Grothe, 2012).

COP also serves collaborative information seeking processes, especially across teams with different functions and responsibilities within the organization. Cyber operations possess similar characteristics, especially in multinational organizations with operations in multiple, physically distributed locations. Today's networks rarely exist to only serve one location, but often connect multiple infrastructures across the globe in different time zones. Network functions remain vital for business success on continuous basis, even though the possibility of intelligent threats, natural disruptions, or physical infrastructure failures also exist at all times. A common operational picture in such cases helps maintain successful monitoring and management of networks.

COP design relies on team Situation Awareness (SA) concepts. There are multiple definitions for SA. Endsley (1995, p36) defines human's SA in complex dynamic environments as "the perception of the elements of the environment within a volume of time and space, the comprehension of their meaning, and the projection of their status in the near future." According to this definition, there are three levels of SA: perception, comprehension and projection. A fourth level, resolution, was then added to this definition by other researchers (McGuinness & Foy, 2000). While the SA levels presented do not belong to a specific application, SA concepts were applied in different domains such as aerospace missions, air traffic control, and military operations to help professionals achieve their working goals and improve the quality of their decision making. An important distinction of three characteristics of dynamic environments addresses: (1) situation awareness, (2) decision making and (3) performance of professionals within those environments (Endsley, 1995). The three characteristics are highly inter-related. Part of this dissertation

attempts improving IT analysts' SA and consider how enhanced SA can improve the two latter characteristics.

Network Security Situation Awareness

Discussions of network security situation awareness (NSSA) extend the SA concepts described above (Onwubiko, 2009), and is shown in Figure 2. The model entails the four levels of SA (perception, comprehension, projection and resolution) (Onwubiko, 2009) and are described as follows:

1. ***Perception***: analysts being aware of network elements.
2. ***Comprehension***: analysts' methods to determine the relevance of perceived information.
3. ***Projection***: ability of analysts to predict future state based on comprehension.
4. ***Resolution***: necessary action required to address a network situation when it occurs.

The complete model developed is shown in **Error! Reference source not found..** It describes the interrelation between the 4 SA levels, analyst roles and NSSA attributes: dynamism and complexity, automation, real-time processing, multisource data fusion, heterogeneity, security visualization, decision control, risk assessment, resolution, forecasting and prediction.

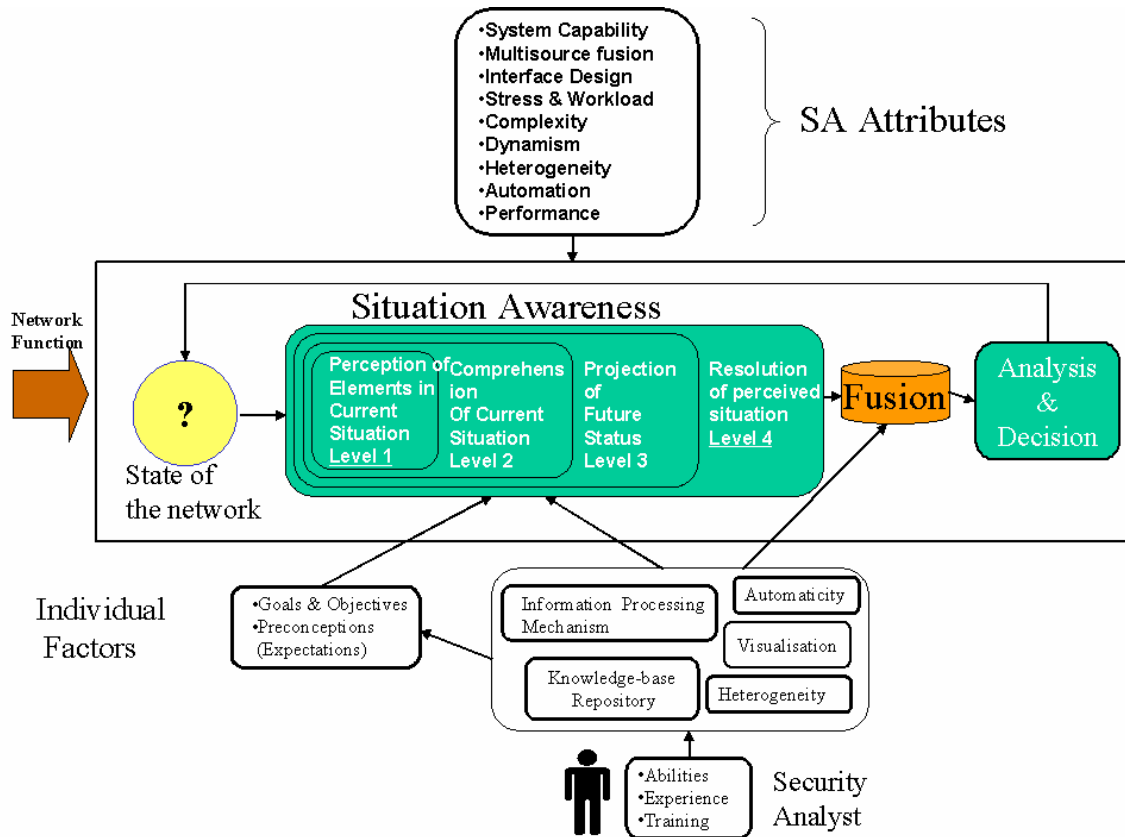


Figure 2 Network Security Situation Awareness Model (Onwubiko, 2009)

The literature that studies situation awareness in network and cyber security operations is very limited. Existing tools help analysts gain a level of SA that support their continuous decision making process. However, there are multiple gaps that exist in effective information presentation and knowledge sharing in cybersecurity and network operations.

System Architecture and Usability of COP

Recent research efforts have demonstrated the need to successful enterprise systems integration with individualized modern tools that target a user with specific goals within the organization. Relatively limited research is presented, however, on detailed steps to achieve the system integration focusing on interpersonal needs of the users and teams of users: domains considered include military command and control, logistics, disaster management and supply chain operations (Agre, Kramer, & Vassiliou, 2011) (Boukhtouta & Berger, 2014) (Kroculick, 2014) (Taylor & Arthanari, 2017) (Widera, Lechtenberg, Gurczik, & Bähr, 2017). Command and Control in military has been a great focus of the situation awareness, usability and IT research communities.

This is due the high value of return on investment of saving lives in combat. While the research continues to progress in this field, and opportunity for improvement still exists in providing a more comprehensive situation awareness of cyber common operating picture (CCOP)_ (Conti, Nelson, & Raymond, 2013); there has been a noticeable effort of adapting achievements in COP to the civil supply chain and logistics community (Tatham, Spens, & Kovács, 2017).

Systems engineering and design focuses primarily on technical system integration and architecture (Laaperi & Vankka, 2015). While this is important to team success working in this environment, it must be followed with system implementation methodology that ensures ease of use and information alignment with human decision making (Rummukainen, Oksama, Timonen, & Vankka, 2014). The research recognizes the criticality of integration on the system level. This dissertation combines UX research methods that have demonstrated success in the consumer market applications and products, with goal directed task analysis to improve performance of distributed operations teams in a global manufacturing organization.

Human Cognition Elements of Information Processing and Task Analysis

Algorithmic defense network scanning provides security analysts with data about potential threats and attacks. As of 2018, the information security product market includes a variety of software packages and tools to conduct network operation and intrusion scans. Despite technological advancements, algorithmic automated defense is not yet perfect. False alarms, incomplete information and other limitations of data provided require continuous human involvement. The system continues to rely on human to identify the real threat using automated scans data. A human is needed to isolate meaningful data, search for other related information and understand the full picture in the right context. However, security operators are often overloaded with information processing tasks (Sawyer et al., 2014).

Goal directed task analysis (GDTA) techniques are used to capture how experts and novices perform complex tasks. Monitoring of and response to various events presents a large portion of analysts' workload and critical decision making. Designers need to be aware of workload and its effect on operators' performance. Sawyer and colleagues' research results also considered event rate and signal probability effects on performance. These necessary features and constraints must be addressed in order to define important features to maintain and optimize the analysts' SA. GDTA helps translate the cognitive needs of analysts monitoring the network into design features

of technology in use to support their response action and decision making in complex environments (Endsley, Bolstad, Jones, & Riley, 2003). GDTA is an appropriate tool to be used in such complex environments with disruptive events (Bailey & Iqbal, 2008).

Team Collaboration

Network operations in complex information technology environments reach levels of complexity that are cognitively beyond individual capabilities. Team collaboration is necessary to accomplish work objectives. McNeese and colleagues (N. J. McNeese, Reddy, & Friedenber, 2014) showed the effect of collaborative information seeking (CIS) on team performance and team decision making. CIS is defined by Foster (2006, p330) as “*the study of the systems and practices that enable individuals to collaborate during the seeking, searching, and retrieval of information*”.

Many of today’s businesses own databases for knowledge referencing about challenges out of the regular working routine. Such databases are created to keep track of such challenges, their root causes and how the working team was able to successfully overcome those challenges. This is very valuable in case similar incidents happen in the future. It saves time and efforts spent on investigation, development and testing of alternative solutions, and minimizing the risks associated with delayed or missed event responses. Fewer organizations value or systematically enable the referencing of operational experience. Garrett and Caldwell (Garrett & Caldwell, 2002) defined the “operations to reference cycle” as *the period of time that it takes for this operational knowledge to become a reference source*. Their research studied capturing and referencing knowledge developed during NASA’s Mission Control Center operations. The success of this process enables dynamic operational environments to make of its previously generated knowledge in future similar situations which advance organizations development and responsiveness in dynamic event response environment.

Knowledge Capture and Organizational Capability

The classic meaning of the word foraging is “to search for food or provisions or to search for what one needs or wants” (Webster, 1960, p. 564). Foraging theory is utilized in different fields such as animal ecology (Winterhalder, 1981), human anthropology (Shennan, 2002), library science (Sandstrom, 1994) and information foraging in internet and computer system environments (Mantovani, 2001) to help human grasp seek knowledge they need to be able to achieve their work

goals. The foraging theory definitions were expanded to address the work of professionals working in an event driven environment (Garrett & Caldwell, 2006). The benefit from the new definition is to help complex operational environments such as healthcare delivery teams or spaceflight mission controllers to capture and make use of generated knowledge during operation. The new definition distinguished between (1) reactive foraging, in response to a current situation and (2) proactive foraging, in preparation for future forecasted system states. It also stated that resource foraging in dynamic environments occurs at an individual level or at group level. The same research explained practice of resource foraging in spaceflight operations and healthcare delivery as two dynamic, largely event driven environments.

Literature studying knowledge referencing techniques applied this theory to build systematic ways for multi-disciplinary experts share their knowledge while working on the same project (Garrett, Caldwell, & Collins, 2009; Rejab, Noble, & Allan, 2014). Real time knowledge sharing is also very critical for success of projects that rely on the diversity of expertise of team members. One example for such projects showed how to make use of theory (Garrett et al., 2009) to build a meta-knowledge bank for multiple experts to help them share and make use of their expertise for agile software development (Rejab et al., 2014).

Since challenges of effective search and use of relevant information (and expertise) exists in network and security operations centers, foraging theory can be applied to help minimize the effects of this challenge. However, the context of information technology deployments in ongoing operational settings must be considered, as explained in the next section.

IT Deployment in Operations

In the past decade, business analytics has become one of the four major technology trends (Chen, Chiang, & Storey, 2012). A survey conducted by the state of business analytics (Bloomberg Businessweek, 2011) indicated that 97% of companies with \$100 million or more of revenue use some form of business analytics.

Literature has shed the light on the lag between IT implementation and the benefits associated (Devaraj & Kohli, 2000; Kohli & Devaraj, 2003). For that reason, immediate firm performance return on investment (ROI) assessment (Ravichandran & Lertwongsatien, 2005) or financial ROI estimates (Ravichandran, Liu, Han, & Hasan, 2009; Tang, 2006) are not ideal ways of measuring IT solutions success. Digital solutions have been shown to provide a positive impact on the

organization for extended period of time (Chang & Gurbaxani, 2012; Santhanam & Hartono, 2003).

Enterprise Systems Integration

The Enterprise Resource Planning (ERP) industry continues to grow among medium and large corporations (Mahmud, Ramayah, & Kurnia, 2017). These companies rely on ERP systems to manage key processes of its businesses on daily basis. However, SAP, the ERP market leader, and other Enterprise Systems providers are unable to make significant advancements in enhancing the user experience (Kepes, 2013).

Li (2015) claims that despite the multiple discussions available by researchers for user experience pertaining software design and testing, research is limited when it comes to UX limitations related to the user's work perspective on enterprise systems. ERP providers are struggling to offer users an easy to use system compared to other modern individualized software system providers are able to offer. Success rate of ERP deployments have not exceeded 49% worldwide due to user resistance in changing work routine (Mahmud et al., 2017), and due to lack of training and poor information presentation (Wong, Veneziano, & Mahmud, 2016). The complexity of ERP systems' design and information presentation have resulted in employee frustration, including failures of ERP deployment resulting in billions of dollars' worth of law suits with market leading corporations such as Vodafone, Target, Hershey, Nike and others (Fruhlinger & Wailgum, 2017).

Research Organization

The workforce analytics system presented in this research provides productivity, and labor management insights to a targeted user, the distribution operations team of a global manufacturing organization, that cannot be presented with classic productivity modules of SAP or other ERP systems. It is based on a series of research phases, including interviews, participant observations, and embedded work tasks integrating both cybersecurity network operations and ERP enterprise systems implemented for professionals in the finance, sales and supply management of an organization. Descriptions of the first two phases of the research (known as Project 1), and initial findings, are presented in Chapter 3. Project 2, the third (and most complex) phase of the research, is described in Chapters 3 and 4. The workforce analytics tool that is at the heart of Project 2 was designed to provide insights to operations team in the distribution operations of the organization.

METHODS AND INITIAL FINDINGS

This dissertation research proceeded in several stages, and included data collection from multiple organizations and network operations work tasks associated with cyber-physical operations. Expert interviews were conducted at a major cybersecurity research conference to determine needs assessments for team-level information presentation and knowledge sharing in the field of cyber-physical IT operations. Based on these interview results, a case study was performed in a global manufacturing organization's HQ Security Operations Center. During the case study, the researcher collected data through attending team meetings, observing analysts at their stations, and interviewing analysts and managers individually. The initial data collection and the case study (described here as Project 1) focused on network and security operations. Findings from Project 1 formed the basis of the third phase of research (described as Project 2), where the author performed an iterative assessment, design, and implementation of an enterprise-level supply chain information management system. The author was also able to apply user experience (UX) and user research techniques while designing dashboards for a workforce performance management tool deployed for a supply chain operations team of a global consumer goods organization.

Project 2 spanned over a longer period during which the author was involved in development and implementation of an IT application deployment in a supply chain/ distribution work setting. Methods in that stage included user research, interviews, usability and interface design and testing. The methodology used during the projects is presented in **Error! Reference source not found..** the approach is an adaptation of a systems engineering implementation / system design process utilized in other industries (NASA, 2007) The figure illustrates the phases that any enterprise system integration/ enhancement should follow in order to deliver a usable tool that can drive efficiency and boost employees' performance. The phases are explained in detail later in this chapter.



Figure 3 Research Methodology

Error! Reference source not found. describes three layers where most of interaction occurs, once a system implementation project is approved and funded.

Layer 1: External Entities

This layer includes **two** entities, it also includes connections with entities external to the organization getting ready to adopt or enhance the usability of an existing enterprise system: **(1) the system provider**, the company that builds, sells and offers technical support services to the system; and **(2) the integration consultant** hired by either the provider or the user to facilitate integration of the new tool in the user's systems portfolio.

Layer 2: Liaison between the user and provider

Typically, the project manager (part of the customer's organization) acts as liaison between the provider and the system's user. The primary goals of the project manager are to keep up with the project's timeline and ensures work is done to the best interest of the organization.

Layer 3: The User

The last layer represents the customer, the organization procuring the enterprise system. This includes but not limited to operations and functional teams which are the focus of this dissertation. In addition to the project management portion, the methods presented in this research requires the early involvement of a Human Factors (HF) engineer that can work side by side with the project manager with the same goals described in layer 2. For this to materialize, the HF engineer must be a subject matter expert of the business processes, must be an internal member of the customer's organization and have the skillset that ensures the best interest of organization is accomplished. Later in the results section, a comparison between the workforce analytics system implementation (Project 2) and another implementation that was executed prior to Project 2 will show direct benefits of the HF engineer involvement.

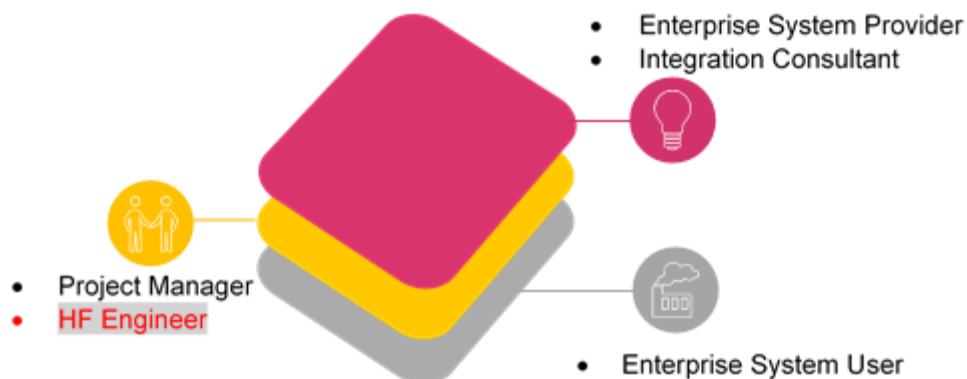


Figure 4 Human Factors Engineer's Role in Enterprise Systems Deployment

Project 1: Security and Network Operations

Data Collection and Analysis

The first phase of this research included exploratory, interview-based subjective data collection to answer three initial research questions regarding cybersecurity analyst tasks and challenges: (1) what are the primary gaps in analyst sense making process? (2) What visualization features are useful in mitigating these gaps? (3) what gaps exist in sense making and presentation of analyst team performance? An overview of the initial and ongoing research questions is presented here, followed by more detailed descriptions of research methods for each phase of the dissertation (including research already completed). The author of this dissertation participated as a primary member of a multidisciplinary research team addressing information needs and task coordination processes for security and network analyses, initially funded by the Purdue Center for Education and Research in Information Assurance and Security (CERIAS).

The data collection started with an initial interview study (IRB Protocol: 1402014480). The author (I) conducted on-site interviews with eight professionals attending the RSA 2014 security conference (see Section 3.1.2). Participants were based on a convenience sample (contacted during breaks and after technical sessions) in an open setting during the conference. Their experience in the field varied between 10 and 30 years covering a variety of businesses (financial, manufacturing, military, and commercial). Another set of interview questions were developed seeking more detailed information about cyber operations. These questions evolved from the initial interview study results.

Following these interviews, the author (I) conducted a case study in a security operations center of a global manufacturing organization (see Section 3.1.3), including attendance at team meetings, shadowing of analysts and interviewing an entire operations team, their team lead and the SOC manager.

This methodology supported the definition and initial system design phases of information technology system implementation (see Figure 5) and provide valuable input for designing a next generation software tool for use in network & security operations. The results were communicated to project sponsors and published in the Institute of Industrial & System Engineers Annual Conference (IISE) (Eldardiry & Caldwell, 2015).

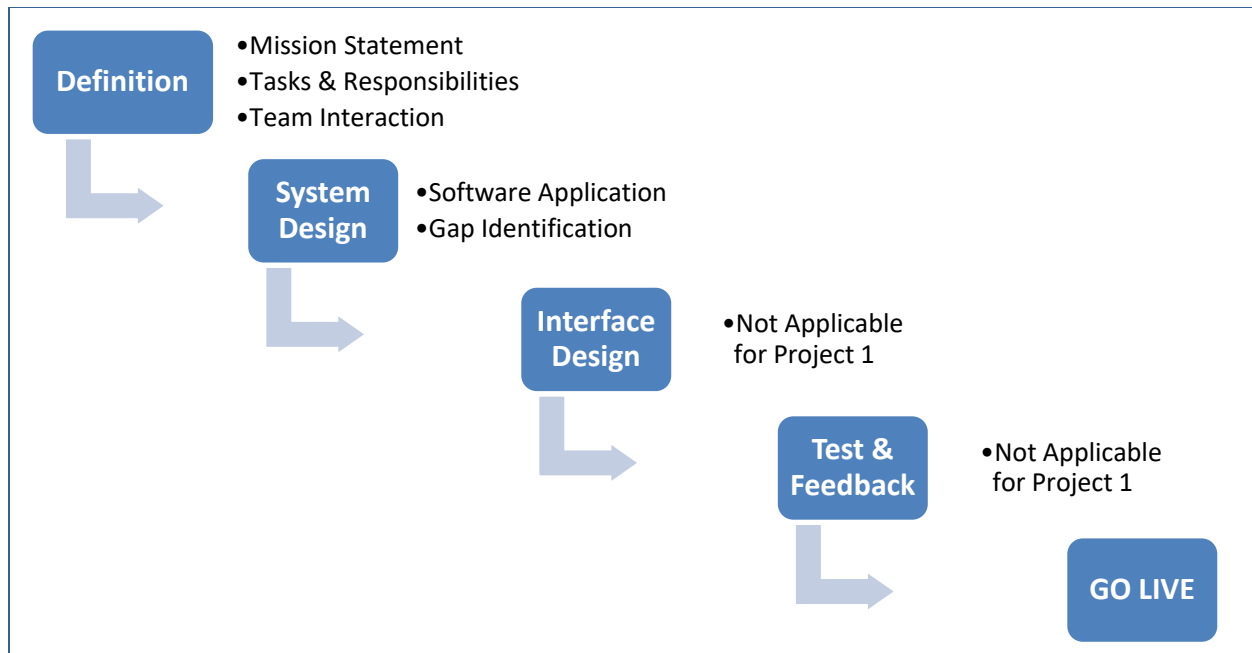


Figure 5 Methodology Progression

Data Collection: RSA Security Conference Interviews

This study was conducted during RSA security conference, February 2014 in San Francisco, CA with eight field professionals. Participants were selected and approached in an open setting during the conference during breaks and after technical sessions. Their experience in the field varied between 10 and 30 years. They come from different business backgrounds (financial, manufacturing, military, and commercial). Participants were a mix of professionals that work either in a network operation center or security operation center.

This initial data collection was an attempt to understand how network and security operations analysts at different managerial levels perform their tasks to meet their goals as well as their daily challenges of acquiring necessary technical information to fulfil their daily tasks. The semi structured interview technique was chosen to allow the capturing of analysts' and managers' ways of thinking in the sociotechnical NOC and SOC context.

Interview questions helped collect data about the working behavior of analysts, as well as the nature of the work environment. The interview protocol started with quick introductory questions to understand the experience level of the interviewee, team size he/she works with, the nature of the working environment, and how technical tasks are divided among analysts.

participants also focused on system vulnerabilities as the main challenge either internally or externally. Another discussed challenge is isolating relevant information from false alarms. The amount of time analysts waste investigating false alarms degrade their work efficacy and hinders them from responding to serious items in a timely manner. This is strongly tied with the challenge of appropriate task prioritization.

A NOC senior leader was frustrated from the quick turnover rate of junior analysts. They are constantly seeking higher positions and running away from 12 hour and overnight shifts, he said. One other participant, with over 30 years of experience in both NOC and SOC settings, especially identified the lack of understanding system components, structure and valuable assets with higher priority to protect as a great challenge to most analysts.

Network vs. Security Operations

Interviewees had different business backgrounds. In addition, their IT application had two different flavors, focusing on either network or security operations. This part of the pilot study findings focuses on similarities and differences between both applications.

Network operation centers are mainly concerned with the network's Health and Performance. Analysts in this case look at the network architecture: the pathways (up time, down time, bandwidth, etc.), the hosts (IP addresses, RAM, etc.) and users (log information).

Network health and performance can degrade due a breakdown, limitation in storage capacity, or system crash/freeze. In most well-defined and recognized cases, if the analyst is familiar with the type of event, a standard procedure can be followed, and problem can be resolved. Physical damage can take longer to fix but still, the amount of loss can be easily predicted, and an accurate time plan can be developed and shared for the organization to work around. Junior analysts often deal with more routine tasks and also get undesirable (night time) shifts. However, more complex or unexpected incidents (such as solar flares, storms, underwater cable cuts, or users' / administrators' bad practices) are often handled by senior analysts. Exceptional incidents happening during night shift require junior analysts to call in and seek help (a process known as "escalation").

Security related problems represent a different pattern of time sensitivity and business risk than health and performance type of problems. Security attacks have a higher level of sophistication. They are a product of human intelligence rather than a storm or power outage. Skilled network

attackers try to sneak into the target system in a smooth unnoticeable manner without raising any red flags. As a result, analysts focus on complex anomaly detection procedures required to detect such breaches before proprietary information resources are lost or compromised. Security analysts need to have a higher level of skills and always be up to date. Part of the security analysts' role is to create profiles of top attack signatures and most persistent attacking groups to be shared with the team and built into their detection system. It is believed that having the right tools and expertise often speeds up the problem-resolution process, so that malicious behavior and its source are often identified earlier and more accurately.

Work Behavior

Lack of collaboration between network analysts was repeatedly mentioned by interview respondents. Most agree, however, on its vital importance. The five who claimed to have collaboration at their NOCs, only really have it in a limited way, in the form of receiving, passing information (from juniors to seniors, from outside sources (e.g. weather info), or to external people (e.g. application users, whose apps are running on the network server). It is important to note that this is very hierarchical and informative, rather than collaborative form of communication. This is an especially prevalent concern (by the interviewees' account) in SOC's where experts tend to be technical specialists who often take responsibility for all event phases from identification to evaluation and resolution (to normal status). Two participants expressed that a great benefit of sharing breach incidents across organizations (such as IP's and threat profiles) would significantly reduce the possible spreads of internal and external threats.

One participant mentioned Root Cause Analysis as a tool to document operational experience from start to resolution being performed after each incident. The participant admitted, however, that while such information repositories are on hand, analysts rarely made use of it. It was acknowledged that people usually try by themselves first, then seek input from the more experienced colleagues, and only thereafter try to use the knowledge base when they are more desperate.

Case Study: Security Operations of a Global Manufacturing Organization

Based on data analysis of the initial interview results, the author developed a new interview protocol for more detailed data collection and participation in a single organization as a case study. This case study was performed in a global manufacturing firm's security operation center.

Background

The firm is a Fortune 500 manufacturing company with over 10,000 employees across four different business segments. Each segment manufactures a different set of products and competes in a different market. IT within the company is separated into three separate functions: (1) *Network* (backup, network power, hardware and other tasks related to network health and performance); (2) *Security* (Intrusion Prevention, data loss prevention, hacking, vulnerability, and other security related tasks); and (3) *Systems* (system upgrades installation, configuration, troubleshooting, and other tasks related to maintaining the IT system). A team from each function exists for each segment. In addition, there one more team for each of the three functions on the corporate level connecting all teams together.

The systems teams are the only 24/7 operating teams. Problems that arise after business hours are reported by the systems teams to the security and network teams to be processed the following day. Depending on the urgency of the problem, security or network employees can be called in after business hours. Different segments own manufacturing operations in eight different U.S. states as well as Australia, Canada, China, France and several European countries. The company also owns offices in multiple locations in Europe, the Middle East, Brazil, and India. The multiple sites existing at different time zones are adding to the complexity of the IT teams' mission.

Case Study Layout

Two business days were spent at the company's headquarters in the Midwest United States, with the corporate level IT security team conducting data collection efforts (while the author was engaged in a multi-week work internship). The case study can be divided into three main project activities. First, the researcher could attend daily team meetings. Meetings were spent in reviewing incidents status using a management tool called Remedy. During the meeting the team distributes new incidents to analysts based on expertise or nature of the problem that aligns with

analysts' responsibilities. The team also discusses priority items, ongoing projects, and investigates pending delayed items with the manager.

The second activity of the case study analysis involved shadowing of IT analysts. Four analysts from the team were shadowed as well as their team lead. During the shadowing process, each team member provided an introduction to the nature of tasks assigned, the different tools and software packages in use and the daily challenges the analyst is facing. Each analyst, lead and manager shadowed also completed an interview focused on how IT professionals at different levels of operations see their roles, what is the nature of the assigned tasks, the decisions need to be made, the types of tools used, the level of satisfaction using the tools, the level of collaboration between different members of the team, and finally, the challenges and areas of improvements.

Case Study Summary

The IT security team perceives their mission statement as to protect the system's CIA - Confidentiality (unauthorized disclosure of data), Integrity (unauthorized change of data), and Availability (system functions are accessible to the right people/ security controls).

Security operations require multiple software tools to cover a variety of tasks. The SOC IT team where the case study was performed used the following software packages in their daily operations:

- ***Remedy***: a software tool used for IT service, allow analysts to manage, prioritize, and track the progress of "IT tickets" created by the network users (organization employees)
- ***QRadar***: a software tool used primarily for Security Information and Event Management (SIEM) applications
- ***RSA Security Analytics***: a software tool used for investigation, detecting patterns and increase the SOC vigilance to external threats
- The SOC team utilized a data loss prevention custom made tool
- The SOC manager was in the process of building an IT Performance Management tool with the purpose of tracking the performance of the different tasks as well as the individuals within his team

There is a necessity for the different tools to efficiently communicate at both human and data structure levels. For example, the outputs of some tools act as input to others. It is preferred that all tools are packages of the same software vendor to facilitate this communication (for example Microsoft Word, Excel and PowerPoint are packages of the Microsoft Office Suite). However, it is found that IT security analysts sometimes choose to use tools from multiple vendors because of the features each is offering.

Software companies attempt to provide advanced technological solutions and tools to assist IT analysts in their attempts to accomplish tasks to protect their organizations' confidentiality, integrity and authenticity. However, some critical or company-specific elements are often overlooked or misaligned with analyst tasks and understanding. Respondents addressed three categories of gaps that need to be investigated.

The first category contains features that exist in tools but never used. This is because they are not needed, needed but hard to use, or it is not known to the user (IT analyst) that they exist in the first place. The second category contains desired features that are missing. This is because the miscommunication between the users and designers or lack of designing capabilities. The third and last category presents the set of features that not only do not exist but also beyond the user's capability to define. This is the time when the IT professionals are frustrated with specific tasks vital but do not know what is the best systematic practice to approach them. Here, an imperative step that must precede design of any IT tool is to better understand the user and the work environment.

Junior IT analysts are primarily responsible of network monitoring and other miscellaneous routine processes. There is a high turnover of junior analysts; after 1-2 years of work experience, they start seeking advanced positions (continuing to work 12-hour night shifts is not the best work layout). It is not hard to find other positions, as the field has very high demand for analysts with work experience. The repeated hiring of junior analysts requires ongoing training. It also means that there is always a fresh employee on board developing expertise. Entry level and junior analysts interact extensively as shown in **Error! Reference source not found.** with senior analysts to expedite their learning curve. They also tend to escalate more assignments at their early time of employment due to their limited expertise. This disruptive/ distracting work environment degrades work quality of senior analysts.

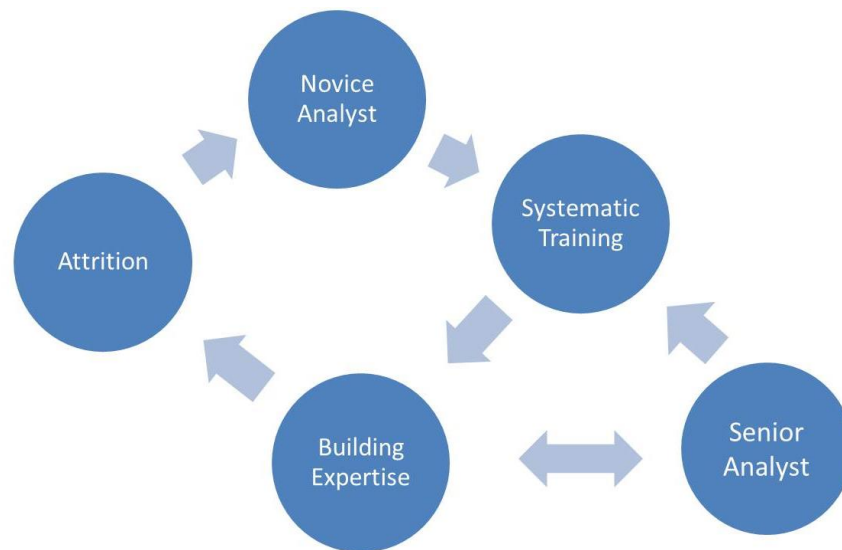


Figure 7 Interaction Between Junior and Senior Analysts

Senior analysts and team leads tasks are divided into two main categories. First, risk management involves strategic planning that is beyond monitoring or response to specific incidents to be able to proactively detection of possible threats (what can happen), the sources of threats and vulnerabilities (how a threat can happen). For that they need better status tools/ displays of the current state of the organization. While developing the appropriate metrics to monitor the system behavior is a challenge, finding the right tool to collect data and display it to managers is even a bigger struggle. It was found that the team leads primarily rely on spreadsheets and Word document files performing such tasks, based on their need of a flexible (and inexpensive) tool that is easy to customize, do basic computations (like percentages), and create graphical presentations of data.

The second category of tasks that fall under team leads' responsibilities is team performance management. There is a desperate need for tools that can track team performance status. The desired tool must be able to map the actual status of analysts, and mapping actual project status to planned/ ideal status. Tool designers must consider the development of performance measures and embed them into the tool that can reflect the actual performance status of the organization. IT security professionals often rely on traditional production measures (based on routine production efficiency measures) that are easy to understand yet do not provide meaningful evaluation of work

contribution. Lack of adequate tools presents a challenge for team leads and area managers communicating their teams' performance status to senior managers beyond the CISO office.

Another task performed by analysts is to classify the organization's information. Dedicated members of the IT operations team work on defining all organizational information level of sensitivity, where it stored, people that can access, whether they are authorized or not. Understanding this structure is vital to prioritize protection on critical functions of the organization. For example, securing blue prints for the firm in hand or its employee's personal information is not the same as data of last month's raw material purchases.

Another finding from the case study is the inaccurate framing of the challenge facing the IT operations. Developing solutions from a purely technical IT perspective (rather than business/strategic perspectives) often cannot translate to other core organizational priorities. Lack of adequate communication between IT and other segments affect business success. For example, during the author's shadowing sessions of the employees, there was an ongoing discussion with engineering R&D senior engineers on a potential \$X million engineering technology purchase. The purchase decision was already made based on a 3-month feasibility study of this technology's impact on sales, productivity ...etc. The finance division already approved the purchase and the engineering team executed the purchase. The security team was only involved at time of implementation. The team was never notified in advance or included in the buying decision. Failure in communication and failure to include security risk in cost benefit analysis led to the selection and attempted implementation of an inappropriate tool. Poor needs / tool alignment compounded the challenge of significant additional work load imposed on the security team to secure a new platform to be implemented across a company with operations spread across four continents.

Initial findings from the Project 1 interviews and case study yielded a number of useful insights regarding challenges to effective identification, development, and implementation of tools to support effective NOC / SOC coordination with other business operations. However, these challenges themselves also limited the feasibility of implementing a full system implementation as shown in Figure 5. Coincidentally, the author was able to participate in a separate opportunity that allowed for a full system implementation building on the initial findings from Project 1. This effort to support network operations for distributed supply chain management will be described in the following section as Project 2.

Project 2: Distributed Supply Chain Network Operations

This project was completed in a different manufacturing organization than the “Security & Network Operations” project or Project 1. The implementation occurred in the North American distribution network of the organization that is composed of four distribution centers in the United States and Canada. The organization, in business for over 150 years, has its headquarters in the east coast of the United States and runs manufacturing, distribution and service operations in six continents.

In addition to the definition and system design phases accomplished in Project 1, the main differentiation between both projects is that in Project 2, the research team was able to complete a full cycle of the research methodology and present a usable tool to the manufacturing organization. The research team was able to overcome limitations that did not allow a full implementation in Project 1.

In Project 1, data was collected at a conference (eight interviews) and a team of analysts in a security operations center (1 site). In Project 2, data was collected from engineers, managers, supervisors and executive management, with 26 employees working in 4 locations participating in the project.

Manufacturing, supply chain and distribution operations in the United States and across the globe still depend on a significant participation by a human workforce. In this company, workforce salaries are the highest expense, presenting around 50% of total operational expenses. The focus of the effort was the deployment of an IT tool to manage and track the performance of workforce in the North American distribution network of a \$15 billion global manufacturing organization.

The next section presents the challenges in the planning and implementation phases of the project. It starts with describing the hierarchy of management and associates who are intended to use the new system, their responsibilities and the impact of the system on their work routine and on the business.

Project 2 Background

The tool is intended for use by shift supervisors, managers and executives within the organization. Noting the organization’s management hierarchy is essential for setting the ground on how data

was collected and ensuring that the design is executed in a way that meets the needs of the entire team.

The organization owns manufacturing and distribution plants across four continents. The scope of the project at hand lies in the North American (NA) distribution network with three Distribution Centers (DC) in the United States and one in Canada. Project participants are spread in five hierarchical levels (two through six) as shown in **Error! Reference source not found..** Level 1 employees (“associates”) perform many DC tasks with data collected and analyzed by the tool, but were not expected to be active users of the tool.

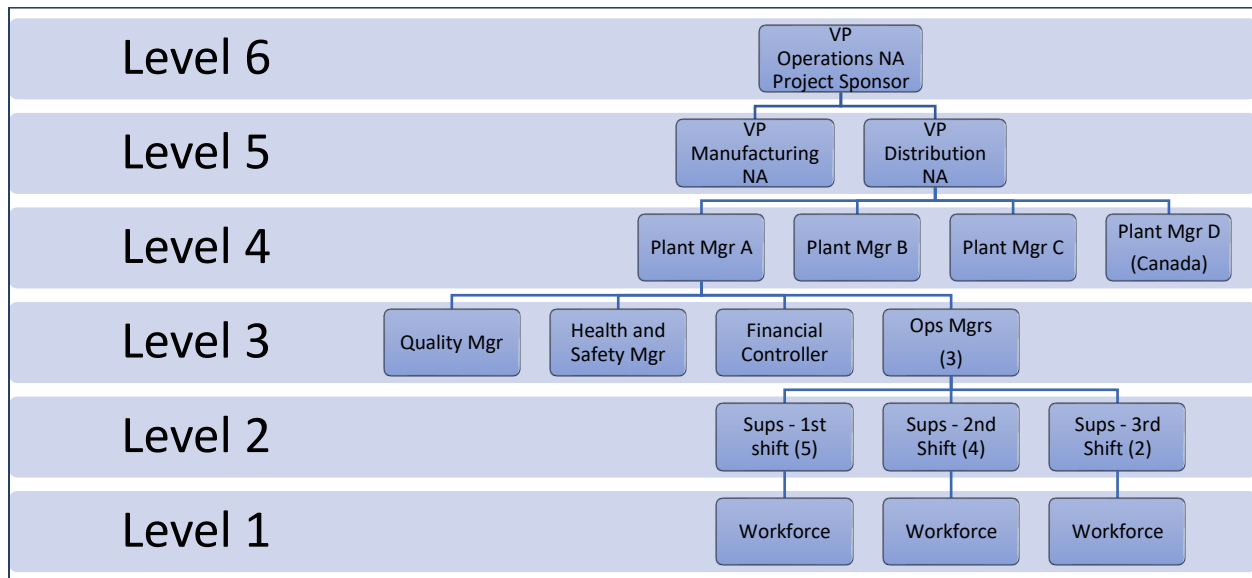


Figure 8 Management Hierarchy Involved in Project Implementation

Level 2 - Supervisors

A supervisor manages a team of associates in a specific functional area. Work responsibilities include the following tasks:

1. Leading the team members in completing the work for the day
2. Ensuring timely accurate processing of daily tasks
3. Focusing on standards and safety & quality requirements
4. Optimizing resources and processes and controlling variables that influence the workflow

The tool in discussion is vital for supervisors to be able to efficiently manage daily tasks. Also, the tool provides historical trends and work standards empowering supervisors to define and complete

tasks, and mitigate risk associated with unplanned incidents affecting workflow (task 4). Overall department performance is passed to functional managers in level 3 described below.

Level 3 – Functional Managers

1. *Quality Manager:* Maintains quality excellence and ISO requirements across the plant. Part of the business quality team to ensure quality goals are aligned within the company. Investigates internal quality problems, customer complaints and rejects. Assists with establishing positive corrective action.
2. *Inventory Control Manager:* Sets long term strategies to optimize storage and retrieval of goods. Manages inventory audits and cycle counts inside the plant and inventories in remote warehouses.
3. *Distribution Operations Manager:* A key user of the workforce management tool in discussion. Manages the supervisory team and responsible for the entire operation across shifts. Responsible for creating a productive work environment and motivating the different teams on the floor. Performs analyses and identifies opportunities for optimizing the operation, minimizing waste of resources and material.
4. *Manufacturing Operations Manager:* A key user of the workforce management tool in discussion. Similar responsibilities to those of the DC operations manager, but in an assembly functional area responsible for (1) building product sets (for example a pan is made in Thailand, its lid is made in Mexico and are both shipped to the DC and assembled into a set before shipping to the customer) and promotional items (for example, buy two pans and get a free kitchen utensil). The department is physically a part of the distribution center, but the manager reports directly to the corporate director of manufacturing operations.
5. *Financial Controller:* Guides financial decisions by establishing, monitoring, and enforcing policies and procedures. Protects assets by establishing, monitoring, and enforcing internal controls. Monitors and confirms financial state by conducting audits, providing information to external auditors. Heavily involved in project budgeting, planning. The controller utilizes the system to measure financial savings.
6. *Environmental, Health and Safety Manager:* promotes a work environment that prevent injuries, illness sources; assists the organization to comply with safety laws; performs audits to eliminate hazards from the workplace.

In addition to information pushed from supervisors about productivity (typically summarized in a weekly report per department per shift), managers at this level rely on performance measurement to plan for staffing (and budgeting for staff) necessary to support business capacity at peak seasons (workforce for this specific team exceeds 70% of operational cost, which is typical for distribution operations). Finally, productivity targets and improvements set by senior management in strategic

plans is a key metric that level 3 managers work on towards achieving their yearly goals. Such tool facilitates an accurate evidence of achieving such goals.

Level 4 – Plant Managers

The plant manager represents the DC at the organization's executive team, composed of other distribution and manufacturing plant managers within the organization in North America. The plant manager provides leadership and strives for excellence in safety, quality, delivery, and associate development, and has facility-wide responsibility for all traditional plant operating functions. The plant manager establishes and communicates the plant's vision to all associates and ensures its realization through strong personal leadership.

Level 5 & 6 – Regional Directors and Vice Presidents

These senior leaders are part of the North American and corporate executive team. They are responsible for making strategic decisions and setting of long term plans, potentiating the competitive edge of the business and delivering the highest value to the customer. Senior management set goals to ensure continual improvement of operations. They do not periodically review performance of workforce but analysis of work improvements and trends are discussed in details in operational reviews presented by managers in levels 3 and 4 on quarterly basis.

Data Collection

The project passed through four milestones from start to completion. **Error! Reference source not found.** introduces the full methodology proposed by this dissertation. It also summarizes the main tasks performed during each of the four phases (definition, system design, interface design, testing) before the new tool was fully launched.

Prior to the project start, the author performed many of the distribution center tasks to understand the workflow experienced by level 1 associates. Activities included receiving products from suppliers (manufacturing plants of the organization); order picking & processing, product sets assembly; shipping deliveries to the customer (home owners and retail businesses); and other inventory auditing activities. Some activities (such as transporting products with a forklift truck) were not performed due to safety constraints and lack of training. Nonetheless, this experience helped the author understand work processes and challenges faced by the associates on the floor

and provided experience-based contributions to all phases of the IT implementation. The steps included the Project 2 effort are shown in the following sections, and follow the implementation process stages shown in Figure 9.

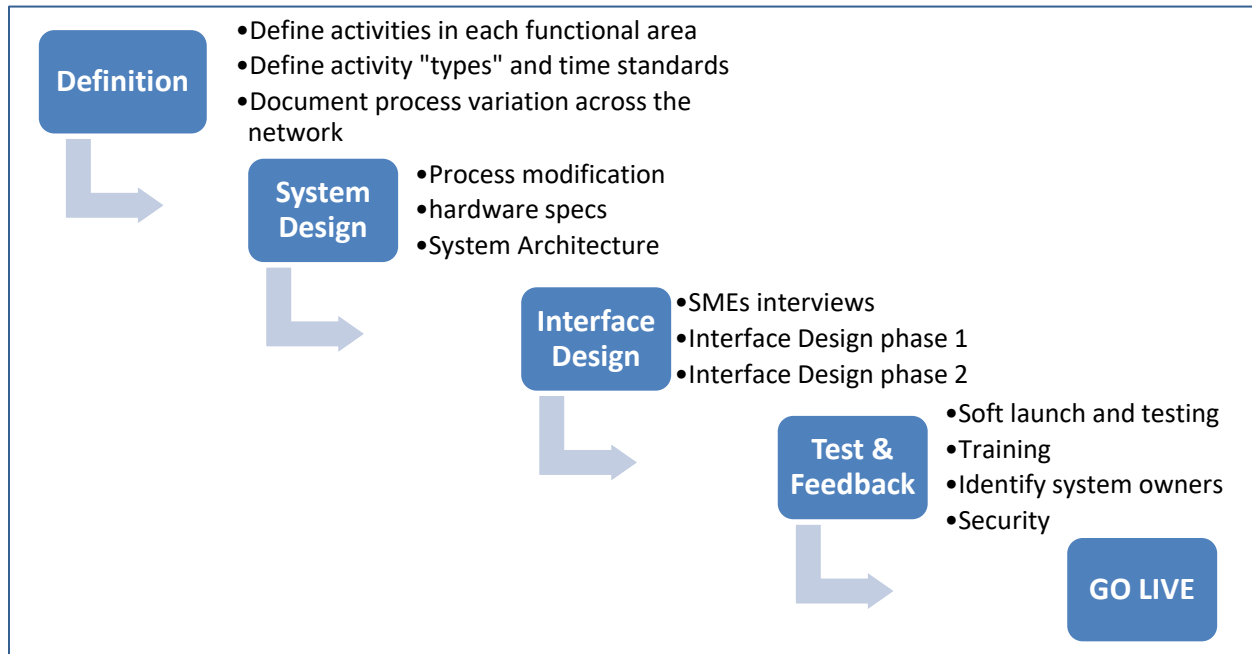


Figure 9 All Methodology Phases Applied to Project 2

Definition

Step 1: Site Survey

During the definition exercise, the author designed templates to allow for a standard procedure of data collection across the distribution network. All teams in each of the four distribution centers were asked to use the templates to provide the following:

1. Define the work scope of each functional area in the DC
2. Populate a list of activities performed in each area
3. Separate the list into two types, value added (direct) activities and non-value added (indirect activities).
4. Compute a standard time for all value-added activities, this step involved motion time studies led by the author in distribution center A.

Step 2: Work Breakdown Structure

The workforce analytics work breakdown structure was developed during a series of meeting sessions, integrating information from site surveys and existing process map diagrams. The implementation is focusing on performance management of value added activities by level 1 Associates; as a result, support departments that represent a fraction of the workforce on the floor (such environmental health and safety, maintenance, and facilities management) were excluded from this exercise.

It has been found that a typical distribution center provides value to the customer through five key operational departments that contribute to performing a direct activity function as follows:

1. *Receiving/ Inbound Department.* This department is responsible of unloading trucks (domestic) and containers (overseas shipments) of product and store them into the distribution center storage locations. In addition to the physical placement of goods, the department is also responsible of processing necessary transactions for the warehouse management system to recognize the quantity and location of each item received. This allows customer orders to be placed against received items.
2. *Order Processing Department.* Order processing is by far the largest department in a distribution center, especially those that support e-commerce orders and not limited to retail customers. In order processing, work performed includes order picking, repacking, and labeling of customer orders.
3. *Shipping/ Outbound Department.* This department includes palletization of customer orders, order presentation (arrangement, wrapping), documentation (bill of lading generation), loading orders on trucks (full truck loads, less than a truck load or parcel shipments).
4. *Inventory Control Department.* A key department that maintains product cycle count compliance, unit of measures for new items, and storage location configuration.
5. *Value Added Services Department.* This department was a major source of variation between distribution centers within the network, entails building promotional displays, execution of customer specific customization, limited rework of non-conformance product and building product sets.

Step 3: Key Metrics

As mentioned in the site survey steps, activities performed on the floor are split into two main categories, direct and indirect. An example of a direct activity is moving product from the receiving dock to the storage locations. An example of an indirect activity is changing the battery of a forklift truck. All metrics identified during the study are tied to two key metrics: (1) workforce productivity and (2) workforce utilization.

1. *Workforce Productivity* Direct activities present labor productivity and work efficiency.

The goal for an associate is to work to 100% of the standard time of a given direct activity. The efficiency is improved by process change to reduce standard time of a given direct activity.

$$Productivity = \sum_1^D \frac{quantity\ completed\ x\ standard\ time}{direct\ time\ worked} \times 100\%$$

2. *Workforce Utilization* Time spent on direct activities ratio to total worked hours represent labor utilization. The goal is to maintain a 90% of labor utilization not including support functions such as maintenance which is considered 100% of indirect work nature.

$$Utilization = \sum_1^I direct\ time\ worked \times \frac{1}{total\ worked\ time} \times 100\%$$

Step 4: Site Variation

Subject Matter Experts were invited to participate in a series of meetings with the goal to eliminate unnecessary variations between locations as applicable, then to capture variations that cannot be eliminated with root cause documentation. Root causes of variation between locations were found to be related to a variation in one of the following items:

1. Customer Requirements
2. Automation/ Equipment
3. Product
4. Storage Locations/ Racking Type

The variation is only documented if creating a unique activity to a specific location an associate must perform on the floor while working towards fulfilling a customer order. Or if a similar activity is performed but with a different time standard.

System Design

Step 1: Integration Impact on Business Operation

This phase started with assessing the feasibility of standardizing how the tool is to be used across the network, as well as defining the impact on the business daily operation once the tool is integrated. The goal was to come to an agreement of the tool purchase, and determine the system architecture. The researcher presented to the operations team in a series of meetings continued for several weeks.

A great challenge in the definition phase of Project 2 (see **Error! Reference source not found.**) was the involvement of distributed teams in each distribution location. However, all teams involved were internal teams with the same background discussing mainly topics related to operations. This challenge was magnified significantly in the system design phase. Parties involved included the project team, members of the finance team, a dedicated IT team, and two external parties: the tool vendor, and the consultant firm that works in partnership with the tool vendor. The system boundaries in this phase included the following:

1. Interactions with external teams
2. Interactions across functions within the company (project management, operations, IT, Legal, finance) as shown in Figure 10
3. Budget constraints

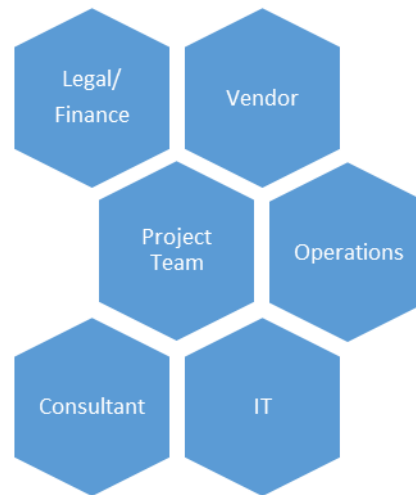


Figure 10 Functional Teams' Interaction During Planning Phase

An important note in this phase was each party had its own goals by nature other than agreeing on the system structure. Financial controllers were focusing on the budget, legal focusing on what is being shared with external parties. And that, from the researcher's perspective was the greatest challenge in this phase.

Step 2: Determine Permission Rights

A separate series of sessions were held with a smaller group of key people during the system design phase to determine permissions structure for the internal team (users). Permissions rights has two components: read and write. Each user or group of users possess a different level of access to information processed and presented by the workforce management tool. Examples of responsibilities include the ability to modify report content and format, edit users' profiles, update activity standards, and access reports generated from one or multiple locations. A limited number of Level 1 associates were technically qualified to modify elements within the system.

Another security component is to use the tool to investigate/ track a specific shipment, and identify associates who worked on the shipment. This specific functionality of the system introduces a new dimension to the project. The distribution centers in the North American are supply chain security certified facilities. This project supplements the "Customs – Trade Partnership against Terrorism" (C-TPAT) certification process. Both security components and their implications are discussed further in the results section of this chapter.

Interface Design

The goal of this task phase was to make sure the system design agreement is satisfying the internal teams' requirements, and to collect SMEs input of their expectations on what to get out of the system. This step overlapped with the system design step.

Step 1: User Research

Individual interviews were conducted with 26 employees across four Distribution Centers. A, B, C and D. In distribution center A, the entire management team, and shift supervisors, were interviewed. The project was conducted mainly in location A over a three-month period. Three interviews were conducted via teleconference at Distribution Center D; the author traveled to Distribution Centers B and C, to conduct on site interviews. The number of interviews by location / level and job title of each interviewee are summarized in Table 1 below.

Table 1 Interview Participants from 4 Distribution Centers

DC	Participant Count	Executive	Plant Manager	Dept. Manager	Supervisor 1st shift	Supervisor 2nd Shift
A	14		1	5	5	3
B	4		-	2	-	1
C	3		1	1	2	-
D	3		1	2	-	-
Other	2	2				
TOTAL: 26		2	3	10	7	4

Interviews were conducted in two rounds. During the 1st round, interview questions were open ended. For example, “what kind of information you are looking to get out of the system?” “What decisions you will be making based on the displayed information?” “How do you obtain necessary information to make such decisions today?” “How would you like the information to be presented?” “In what format (tables, charts, etc.)?”

During the 2nd round of interviews, Interface mockups (Appendix C) were built based on Results from round 1 interviews. The mockups were displays via Microsoft PowerPoint to the users to allow additional feedback. Weekly team meetings were conducted (10 weeks) to brainstorm and agree on the system functionalities to be implemented. The interviews resulted in (1) adjustment and feedback to system design architecture, (2) format and content of the presented information

about the workforce performance, (3) frequency of pushing information updates to SMEs and system users.

Step 2: Creating Personas

User profiles or Personas (a term commonly used in UX research in consumer applications) were developed to represent generic needs of the workforce tool system users. Profiles were given fictitious names to facilitate the discussion within the implementation team.

Primary Users: Operations Team

The system was built around the primary users' needs. The associates performing work on the floor is not user per se of the system, however, a great focus during implementation was not to disrupt or introduce additional steps that the associates must perform for data collection. A great success was to use existing data points to deliver implementation goals. Other primary users are shifts supervisors, operation managers, and plant managers. A presentation of the user profiles, representing primary and secondary users, are presented below in Tables 2-9.

Table 2 Associate's User Profile


	<p>Jim</p> <p>I work on the floor to fulfill customer orders. The less steps I need to do, the more productive I am. I like to be recognized when I do a good job.</p>
<p>Occupation: Hourly Floor Associate</p> <p>Education: GED</p>	<p>Tool Use: not a user, but provides most of transactions that create data points to the workforce analytics tool</p>
<p>Characteristics: Paid by the hour, appreciates high pay rate during overtime, too much overtime increase attrition risk.</p>	

Table 3 Supervisor's User Profile


	Connie I manage labor on the floor, I hold daily kick-off meetings to review performance. I succeed by motivating my team members.
Occupation: Shift Supervisor Education: BSc Degree	Tool Use: I need to review performance with my team on daily basis. Assign work to associates according to their skillset
Characteristics: tactical role, management by exception.	

Table 4 Operations Manager's User Profile



	Anthony I oversee all operations departments across shifts. My job is to ensure customer orders are fulfilled on time with minimum cost possible.
Occupation: Operations Manager Education: BSc / Advanced Degree	Tool Use: Set efficiency goals on weekly and monthly basis for the facility.
Characteristics: minimum 3-5 years of experience. Focus on labor management, and customer order fulfillment. Frequent interaction with other functions	

Table 5 Plant Manager's User Profile

	Mary I am responsible for all aspects of the business within the 4 walls. I need to show trends of improvements for senior management.
Occupation: Plant Manager Education: MBA/ Advanced Degree	Tool Use: Aggregate performance of departments per quarter. Evidence of performance improvements trends.
Characteristics: 10+ years of experience. Frequent interactions with transportation, sales, supply chain and other corporate teams. Strategic Decision Making.	

Secondary User: Senior Management & Support Functions

The workforce system was acquired to support the production operations team. Other users who are found to benefit from the system outside the operations team are identified as secondary users. Secondary users are those who were included in the scope of work at a later stage. They are employees indirectly related to the production operation. While senior management involved are

part of the operations team, due to lower frequency of using the system, they are considered secondary users.

Table 6 Senior Management's User Profile


	Steve Part of the executive management team. I work to set and support execution of strategic goals. Optimize distribution network to best serve the customer.
Occupation: Director of Operations Education: MBA/ Advanced Degree	Tool Use: Overall network performance. Metrics per distribution center location. Set productivity goals for the year.
Characteristics: Minimal or no interaction with the tool. Analytics insights pushed to the user via direct reports.	

Table 7 HR Manager's User's Profile


	Daniela I work to create opportunities for employee engagement, and maintain a desirable work environment for the team.
Occupation: HR Manager Education: Advanced Degree	Tool Use: Quantitative metrics to use for employee recognition, and employee accountability.
Characteristics: Limited technical knowledge about business processes	

Table 8 Project Manager's User Profile

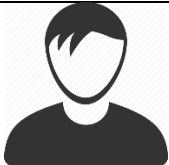

	Richard Introduce new methods, new technology to continually improve work efficiency and minimize cost.
Occupation: IE/ Project Manager Education: BSc Degree	Tool Use: Analysis to identify opportunities for improvement
Characteristics: technical oriented, focus on project implementation and report on ROI, empower workforce to utilize new resources.	

Table 9 Plant Controller's User Profile

	Cynthia Responsible for all operations financial transactions. Work closely with operations and corporate finance. Make sure labor, assets are justified and used to meet goals.
Occupation: Plant Controller Education: BSc Degree	Tool Use: Report on labor utilization, budget justification
Characteristics: Number oriented, control spend for all direct and indirect costs.	

Testing

The organization's IT team along with the vendor design team launched a "test environment" for the tool. The test environment is identical to the real tool except it does not affect critical functions such as payroll, absenteeism, or actual production decisions. The tool was introduced to the teams in all four locations. The author developed training materials and held training sessions for all locations. These sessions resulted in bug identifications and modification requests that I communicated to the vendor's design team to be addressed before the actual deployment date. I had the opportunity to negotiate additional costs requested by the vendor in relation to requested modification.

User Acceptance Testing

The author designed test scripts with detailed steps on how the system is used. Test scripts covered topics including:

1. Productivity Reports
2. Utilization Reports
3. Associate Performance Reports
4. Activity Performance Reports
5. Creating Interactive Dashboards
6. User Profile Setup
7. Automated Email Configuration
8. Exception reports
9. Creating New Metrics

10. Modify Existing Metrics

In addition to being reliable references for training purposes, the scripts are also evidence for user testing to ensure verification and validation (the system can perform the tasks for which it was built). This exercise also provided a formal channel for system users to communicate additional feedback for the author to enhance overall usability of the system.

Tool Deployment

This section reviews decisions driven by information made available by the performance management tool. It provides information to distribution operations, engineering, human resources, and finance.

Operations supervisors, as primary users of this tool, obtain real time information on work progress on the floor and react with moving associates around to avoid process bottlenecks. They can identify associates with lower levels of productivity, in other words identify candidates for additional training. Supervisors and managers can identify high performers and dedicate them to train their peers and work with lean facilitators and engineering to improve work methods.

Based on these outcomes, the engineering team can identify work areas needing process design enhancement/ automation as a step to increase overall process efficiency and labor utilization. The human resources department, in coordination with operations management, can access data showing performance trends per individual, per department, and per shift allowing human resources to motivate associates through different incentive and accountability programs.

Finally, for finance and controllership, reports tailored towards labor capacity in addition to other systems providing business projection can be used to allocate budgets for labor expenses. This has been key to controllership; for example, being able to figure out additional workforce needed proactively alongside with business expansion rather than a shot in the dark approach in the past. Previously, decisions were made on how many to hire with no quantitative data to back it up. This performance management tool has definitely filled this gap.

OVERALL RESULTS

Project 1: Security and Network Operations

As previously discussed, Project 1 involved two stages of data collection. The first stage included interviews of eight participants attending the RSA cybersecurity conference; the second stage was a “case study” where the author interviewed and shadowed a SOC team consisting of an SOC manager, team lead, and four analysts. Project 1 interviews and job shadowing identified three critical operational gaps affecting NOC / SOC analysts in cybersecurity operations. Information technology tools, described below, can help address these gaps, including support for improved information alignment and knowledge sharing, team status determination, and more efficient capturing of operational experience into reference documentation. Such tools can improve the responsiveness of analysts to APTs and other threats, reduce mental workload on senior and junior analysts, and facilitate communication between analysts at various levels, their managers, and other professionals in the organization outside the security segment. The remainder of this section provides an overview of each of the three tools and potential benefits to the industry.

Tool 1: Information Alignment and Team Situation Awareness

Typically, junior analysts work on results from algorithmic network scans, big data analytics results and apply their training to highlight cues of potential threats. This is then passed to higher level analysts that first investigate and separate actual attacks from false positives then apply necessary defense mechanisms when needed. Senior analysts often perform redundant steps already executed by junior analysts to reach their state of knowledge about the current state of the problem.

This tool targets visualization improvement for algorithmic scan results when displayed to analysts to help identify potential threats faster. It also empowers junior analysts to transfer their knowledge to senior analysts efficiently when attempting to escalate a specific incident. Escalation is frequently needed when dealing with a case beyond junior analysts’ technical knowledge. This will reduce the total number of steps analyst need to go through and expedite the response time to stop the threat. Further results in this context can introduce new features and functions on existing tools in the market.

Tool 2: Management of Team Performance

SOC managers and team leads are often confronted with requests to define and measure their network and team status; they are often not capable of communicating the value of their work to others outside of the technical realm of NOC / SOC professionals. A team performance management tool should help managers quantify their team performance and network status, with two important outcomes. The first outcome is to be able to track their operations and identify weaknesses; the second outcome is to be able to communicate performance quantitatively that provide understandable justifications of budgets and benefits to organizational units beyond the CISO office. Such a tool is most needed to maintain an efficient operation and assist team leads in operation and project management, as well as to enable feasibility studies of strategic projects and other managerial roles.

Tool 3: Operational Knowledge Referencing and System Teaching

IT operations centers experience a high turnover of novice analysts as those analysts acquire skills enabling them to advance in their career. The job market is such that skilled analysts are always in high demand and multiple opportunities exist for IT professionals to excel and advance. Many analysts also seek better jobs to avoid long and overnight shifts needed to maintain a 24/7-hour operation. This is a phenomenon that requires continuous training of new analysts. Besides standard training, development of expertise and acquiring skills necessary to perform required tasks is also necessary. Transfer of organizational knowledge to novice analysts efficiently is a vital process to maximize the organization's capabilities at all times (Grant, 1996).

Experts in other work environments are able to perform a standard process of operations to achieve a successful knowledge referencing and documentation. Turning operational experience into shared and accessible reference documents has been shown to improve work efficiency in other domains such as healthcare, spaceflight mission control (Garrett & Caldwell, 2006). However, IT professionals report a lack of similar processes allowing them to perform an efficient transfer of knowledge and expertise to analysts at early stages of their careers.

In preliminary interviews, network managers and team leads stated that they are unaware of tools that will allow them to document work procedures and cases to be used as a resource for novice analysts. They express frustration from the need of their continuous involvement in operational

level tasks that interrupt their managerial tasks. Interruption affects productivity and reduces the quality of end work results (Foroughi et al., 2014).

Senior analysts are always encouraged to detect and recognize unusual or novel patterns that could represent new types of cyber threats. This is vital to be able to keep up with continuous evolving complex threats from professional attackers and hacking organizations. By contrast, junior analysts are expected to take care of more structured routine tasks.

This tool aims at helping senior analysts grasp repetitive tasks leverage their skills to (1) teach the system and automate such tasks or (2) transform these escalated tasks to routine tasks and teach junior analysts how to deal with them in case tasks cannot be automated and need human sense-making.

There are multiple challenges that hinder designers develop such tools. First, analysts tend to prefer solving the problem on hand and move on without realizing the order of magnitude of potential improvement impact on their future workload. Second, even with seeing the benefit of eliminating repetitive time consuming tasks, analysts cannot dedicate needed time to teach the system or developing a knowledge reference guide for junior analysts. Without prior demonstrations of success, it may be hard to convince organizations to invest in such tools.

The next steps at this point of research were to utilize goal directed task analysis (GDTA) to capture tasks, information and SA requirements of network analysts. Then, use collected data to build visual prototypes for testing purposes. Instead, a change of direction occurred; research was pursued in a different work environment, the research methods were still pursued but for supply chain operations teams rather than network analysts. The research was taken a step further with a full system implementation validating the impact of the research in business settings. The next section gives more details on results from the supply chain implementation.

Project 2: Distributed Supply Chain Network Operations

The author worked with a distribution operations team managing supply chain and production information across four North American distribution centers to deploy a workforce analytics and management tool. This section focuses on results and benefits of developing and managing a well-defined, user-focused approach during the implementation.

This section also covers the impact of the tool on the overall operation of the production organization. It is important to note the impact of integrating the tool into the team's operation. A

typical implementation where a consultant company focus on system testing and not user testing would have not empowered the user (distribution team) to fully utilize the tool capability in such a short period of time. Further, the results of Project 2 efforts (based also on Project 1 findings) addresses information security aspect of this implementation, a key learning point that enabled a smoother transition to utilize the workforce analytics tool.

Interview Results

Supervisors

Supervisors need to track performance of their departments on a daily basis. Without report automation, a supervisor must wait until the end of the shift and start pulling data from the system, significantly adding to work hours and delaying the timely use of the information. Automated access and integration of activity performance data as work is being performed on the floor is necessary to provide supervisors with performance reporting they need in a timely manner.

Measuring daily operation evolves around three key factors: (1) worker performance, (2) value added (direct) activities performance, and (3) non-value (indirect) added activities. Four daily reports were automated and sent to each supervisor. Before the beginning of their shift, the supervisor receives reports attached to an email summarizing all the previous day's achievements. The supervisor only needs to print or display reports in order to share with their team in the daily startup meeting. This new routine had a great impact on associates' motivation, awareness, and accountability.

Operations Manager

The operations manager, working closely with supervisors on process improvement and increasing productivity, initially requested daily reporting that can provide an overview of activity performance by department and by shift. Two weeks after the tool was implemented, the operation manager realized that this was too much information to track at the granularity initially requested. He adjusted to weekly and monthly tracking with the ability to drill down to a daily level of detail, or obtain exception reports for poor performance if necessary. The reports allowed the functional area managers to identify improvements opportunities, and set realistic yet challenging goals for the team that would result in stable and productive operations.

An important lesson learned was noted from the interaction with functional area managers. “More data is not always the right answer”. Excessive data, regardless of accuracy, can be overwhelming and degrade the value originally intended. Aligning data pushed to the user with their decision frequency is vital. It is key in operation to determine data “grain size” (the level of detail of information presented) and frequency presented to system users. For example, it is valuable to present performance metrics per individual for a supervisor managing a team of 20 associates. This can be overwhelming for an operations manager responsible for 400 associates across three shifts. It also overwhelming to push this data to the operations manager on daily basis; optimal frequency must be determined. Grain size comparison across managerial levels is shown in Table 10 below. Column definitions are as follows:

1. *SME*: Subject Matter Experts receiving the data
2. *Content*: level of detail needed. A supervisor needs to see employee names, operations manager needs one average value for each supervisor, plant manager needs one metric for the entire department (one department has three supervisors, one for each of the three 8-hour shifts)
3. *Comparison*: A way to benchmark performance against similar teams. A supervisor can compare his teams’ performance to a different shift within the same department. A plant manager can compare to other plants within the network.
4. *Other Attributes*: Data presented in a specific format assists user to have a faster interpretation, make better decisions. A supervisor wants to recognize top performers every Monday in kick off meetings asked for a report sorted in descending order based on performance.

Table 10 Interview Results Highlights – Project 2 Phase 1

SME	Content	Comparison	Frequency	Other attributes
Supervisors	Employee Activity	Shifts	Daily Weekly	Descending order
Operations Manager	Supervisor Activity	Shifts, Departments	Weekly Monthly	%, actual hours
Plant Manager	Departments Plant	Other North America DCs	Weekly, monthly	Charts, Cumulative
Senior Management	Departments plants	Manufacturing plants, European DCs, Asian DCs	Monthly, quarterly	Charts, Cumulative

Senior and Executive Management

Managing workforce and operational goals on the floor is out of scope for executive management. Therefore, reports sent to senior executives in levels 5 & 6 show high level information including 5-10 data points per plant per quarter. However, executive management have access to interactive dashboards that help them discover trends and areas of weaknesses, strengths and work culture within the business.

Integration

The organization where Project 2 was performed also implemented multiple system implementations and enhancements outside of the project scope of the workforce analytics tool, and beyond the scope of this dissertation. One outcome of this dissertation research was the demonstration of an information technology implementation process supporting a smoother transition while adopting the new system. The main accomplishment was the execution of the implementation with minimal interruption to daily operation, and maximizing the utilization of the system capabilities to best serve the user.

A year prior to this project, operations teams involved in this implementation experienced another information technology system implementation where business IT led the implementation. The goal was to standardize the Warehouse Management System (WMS) for the North American distribution network. The team expressed several concerns to the author regarding their desire to avoid difficulties similar to those experienced during the WMS implementation. Interaction with the team during the various phases of the workforce analytics system implementation allowed the author to understand the failure in previous implementation from a user experience point of view. The prior implementation did not take into consideration business variation in different locations. The operations team in location A lost system functionality that used to exist in the WMS system. This caused the team to alter processes to align with system capabilities when ideally the system is created to support the process. This was considered during the site variation step explained in details in section 0.

The operations teams also suffered from challenges related to interface design. The transactions sequences driven by interface layouts do not align with business process and decision making. The interface design caused users to work through application screens in repetitive and inefficient

ways, when compared with the flow of other work-related tasks. This misalignment has been minimized in Project 2, especially based on results of the user acceptance testing phase (see Section 0). User Acceptance Testing is frequently used in consumer-based interface design efforts; however, the application of these techniques to in-house enterprise software development is less frequent. Thus, the use of User Acceptance Testing to improve information technology system design to handle business operations is a relative innovation in this organization (as defined by Rogers in the discussion of diffusion of innovations: see Rogers, 1995). The integration process was not presented as UX research, but the interviews, training, and implementation / integration efforts had the impact of effective UX and user acceptance testing outcomes.

Business Impact

The ability to track workforce performance in real time provided several additional benefits and positive impacts for business operations. This section highlights the direct benefits to operations after the workforce analytics deployment was completed. Not all positive outcomes directly link to individually quantified returns on investment. However, a more direct and specific measure of productivity (amount of actual work done compared to industrial engineering standard time measures) was developed during the definition phase of the project. This productivity measure provides an accessible key performance indicator (KPI) for distribution operations as a whole; this tool enabled the first available assessment of a critical organization KPI. Other business impacts include the following:

Benchmarking

Information Visualization allowed for comparison of workers performing the same task within the same team, and across shifts. Figure 11 below shows the productivity (%) vs the number of hours worked in a week period for a specific task. Each circle on the graph represents one worker. The blue color indicates a 1st shift worker, the red is used for 2nd shift. The operations manager's target is to push as many circles to the top right corner.

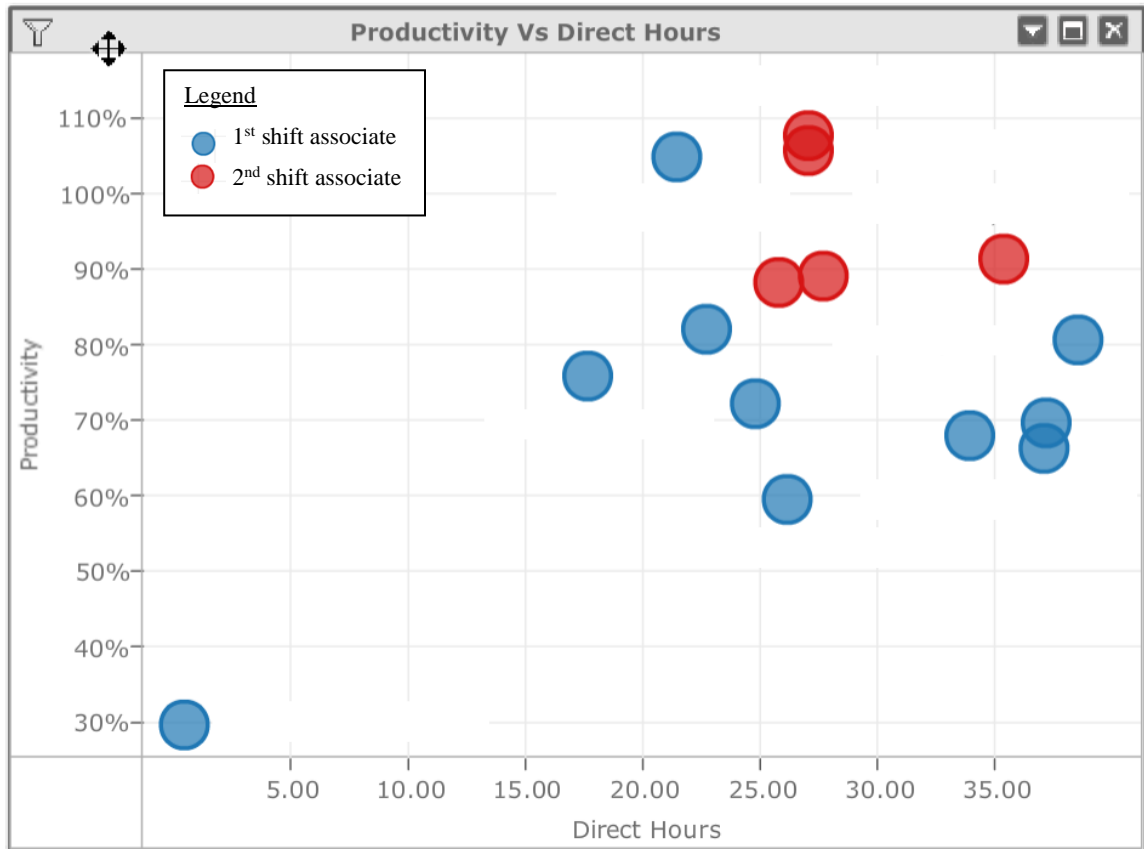


Figure 11 task variation across shifts

Goal Setting

Experienced workers, because of job-based learning, can easily meet (and exceed) the performance standard as defined by industrial engineering time study. However, there is also a high level of turnover among Level 1 associates. Thus, newer members of the team are often not capable of meeting the time standard. The system acts a reliable tool to divide workers in virtual groups and embedding their expertise in the goal setting function.

Hourly Tracking

Supervisors use similar dashboards with smaller time intervals, reviewed during the day that help them recognize slow performers during the day and investigate root causes on the floor.

Sharing Best Practices

As shown in Figure 11 above, 2nd shift workers demonstrate a higher average hourly productivity than 1st shift worker; similar findings were observed across plants. (It is important to note that these findings were not known to distribution center (DC) managers prior to the implementation of the tool. Thus, the tool was used to initiate further investigation and a determination of best practices among the higher performance 2nd shift employees. In Figure 12 below, each color indicates a unique work activity, and each bar presents the cumulative work performed by a single employee. The chart compares task spread in a department across plants. The graphs indicate that the organization of direct value-added tasks among associates differs between DC A and DC B, leading to more efficient labor utilization in DC B.

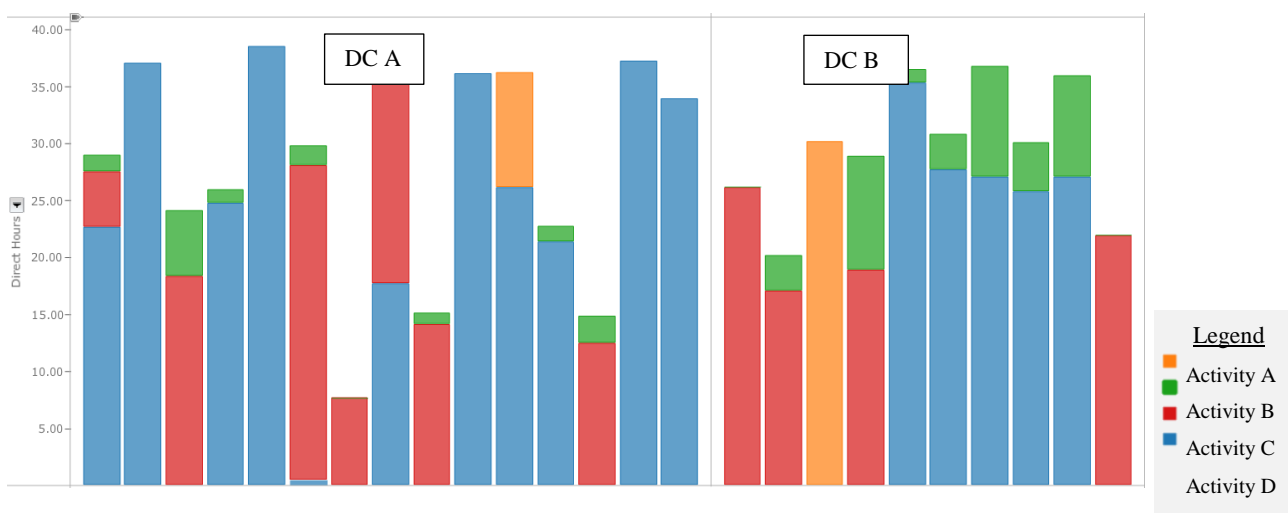


Figure 12 labor utilization across plants
Direct hours worked (Y-axis) per associate (X-axis) per activity

Overtime Reduction

Improved productivity, a well-managed workforce, embedding expertise to enhance standard work measures, and sharing best practices are all factors that combined to reduce missed performance goals and the need for overtime. Financial controllers were able to use dashboards to achieve a significant reduction in salary spend, especially in peak demand seasons (national holidays and summer).

Strategic Planning

A great analytics tool used to support strategic decision making. The workforce analytics tool, and dashboards provided at different levels of granularity, provided the supply chain operations teams a structured approach in determining workforce needs and allocations to support business growth. Productivity information also helped engineering teams prioritize, for the first time, activities for job redesign or automation support and resulting labor savings.

Cost Reduction

For this organization, labor costs in the North American distribution network is 47% of total operating cost; overtime is 12% of the labor cost. Labor is therefore the largest cost driver in the organization; supplies and materials are second, at 12% of total operating costs. Within the first 12 months of workforce analytics tool implementation, the distribution network has seen a 15% reduction in labor costs, as measured by shipped goods to hours worked. (The overall volume of business is expanding, with an overall increase in absolute numbers of employees.) The availability of a tracking system enables team leads and supervisors to review performance with their associates periodically, increase constructive competitiveness across shifts, and create transparent accountability measures (the first time that such empirical productivity metrics have been available). These features have motivated improved performance from associates and others, and created additional evidence to prioritize, support, and fund of new automation and job redesign projects.

The workforce analytics tool implementation also supports HR employee reviews, with granular analyses and dashboard summaries that quantifying individual, team, shift, and distribution center performance. These capabilities help provide more transparent justification of decisions such as yearly raises, promotions, accountability. In addition, it is used by the Environmental, Health and Safety team as an investigation tool to define root causes of product or equipment damage incidents, or even worker's compensation justifications and other safety issues, as the tool connects employee IDs to tasks performed and work exposures.

Security Operations and Impacts Beyond Operations and Finance

Permission Rights

As described previously, and elaborated in Section 0, cybersecurity SOC teams have a mission obligation to protect an organization against threats related to its Confidentiality (unauthorized disclosure of data), Integrity (unauthorized change of data), and Availability (system functions are accessible to the right people/ security controls). Permission rights falls under the integrity portion of that mission. The author's Project 1 experience focused on security operations allowed for early involvement of NOC and SOC team perspectives in Project 2. For the distribution centers, Integrity and Availability operations are critical to ensure adequate "read" and "write" access is appropriately granted according the functionality needed for each user of the system.

Based on the feedback from system design and implementation, the level of access and permission rights does not necessarily correlate with employee's seniority. Phase one of the implementation showed that full access given to senior management for editing reports, employee data and other functions, resulted in confusion and performance losses. The testing phase of the project helped the IT implementation team realize this problem and develop a feasible resolution. The resulting recommendation was to limit senior management's "editing" permission rights, and create a list of "specialized" employees that can perform other tasks upon request. Some examples of the permission rights assignment in the organization are presented in Table 11.

Table 11 Examples of Permission Rights in the Organization

	Employee Title	Access	Initiated by
1	Operations Manager	Edit Activity Definitions	
		Create a New Activity	A Change in Standard Operating Procedure (SOP)
		Terminate a Current Activity	A Change in SOP
		Update Activity Standards	Equipment Enhancements, Employee Training
2	HR + Payroll	Manage User Profiles	hiring, firing, promotion, department change
3	Supervisors Area Managers	Create Reports, Edit Report Contents (access limited to their department)	
		View Performance of Similar Departments, create comparison charts (high level, anonymous employee details)	
4	Super-User	Complete Access to the system	promotions, employee transfer to different departments
		Edit Users' Access Levels (permission rights)	
		Create Custom Reports to Senior Management including performance data from multiple plants	one time requests from senior management

C-TPAT Supply Chain Security Global Certification

Customs-Trade Partnership against Terrorism (C-TPAT) is a U.S. Customs & Border Protection partnership with businesses that is designed to strengthen and improve overall international supply chain security from point of origin to final destination. Two main objectives of this program are to (1) Prevent terrorist attacks and flows of illicit goods in global supply chain businesses and (2) Facilitate the flow of legitimate cargo (Department of Homeland Security, 2016).

Employees working in distribution settings are encouraged to report suspicious activities such as partially loaded but unattended containers/trailers, or finished goods left open and unattended. It is the responsibility of the security team on site to prevent unauthorized access to the facility, to the product containers & cargo areas. The tool tracks employee names who worked on a given shipment, creating a record trail of people involved. Such historical records assist in certification compliance, and help to demonstrate organizational commitment to developing and maintaining secure supply chain operations.

DISCUSSION

Network and security operations' scope of work is significantly different from that of industrial and systems engineers focusing on supply chain operations. SOC teams work diligently to protect the confidentiality, integrity and availability of the organization's network and information. NOC teams focus on the health and performance of the same network. Multiple organizations are found to have one team with both goals due to the great overlap and similarity of work routine.

By contrast, supply chain operations is often composed of multiple teams with both physical and functional distributions across the organization. Supply chain operations functions include supply planning, raw materials purchasing, storage and distribution, manufacturing, demand planning, transportation and customer service. Some organizations include channel marketing and sales operations under the supply chain operation umbrella. The supply chain operation teams' scope of work focus on physical goods and workflow of materials to fulfil customer orders.

While the scope of work is different between both work environments, the process of managing a complex supply chain consisting of both goods and information has overlaps and similar real-time monitoring and operations requirements. Supply chain management is looking at adverse events and incident response at the physical level of providing goods or service or to the end customer. Extreme weather conditions affect fuel cost, goods prices and lead time. Similarly, a power outage that impacts the network health and performance to its users in the digital world requires similar information sharing and presentation needs.

This discussion addresses parallels and cross-functional overlaps at three levels of analysis. The first parallel is within the operations teams. Figure 13 shows the similarity of the organizational levels and information exchanges between NOC/SOC and supply chain management functions. In an ideal world, when a junior analyst is unable to mitigate the effect of a reported cyber infrastructure incident, the escalation of that incident to a senior analyst would involve similar procedures (and links to other operations teams) that a team lead would receive from an operations manager when faced with unusual circumstances on the shipping dock.

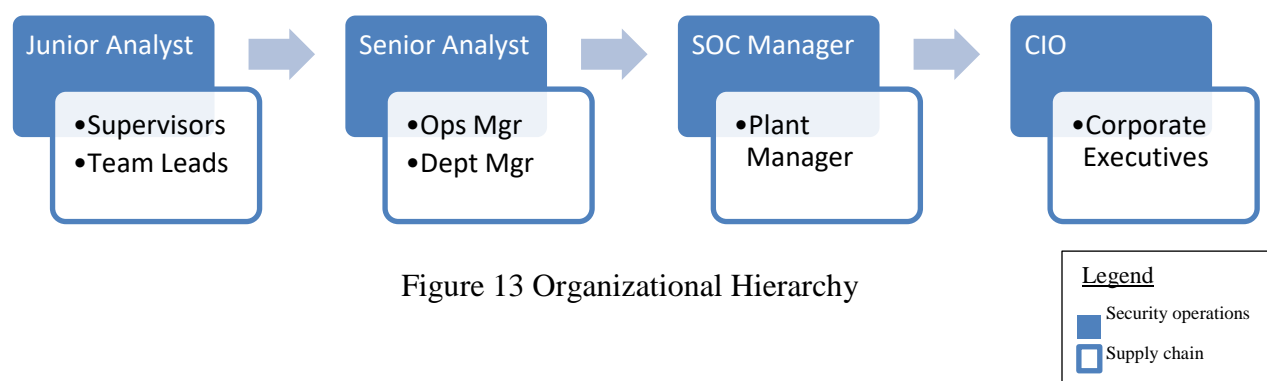


Figure 13 Organizational Hierarchy

The second area of parallels and overlaps addresses interactions with other teams within the organization. Both supply chain operations and security operations are specialized functions that require coordination and justification of priorities with cross-cutting organizational functions such as human resources, finance and long-term planning. Budget approvals, hiring, recruiting and other business transactions mandates interactions to be performed in the same fashion. Third, the interaction with groups outside the organization, such as external customers, suppliers, service providers and competition, have strong parallels between physical and information supply chain operations, as shown in this dissertation. Thus, secure information supply chain management can be a joint function addressing the flows of both physical goods and critical information in the distributed production organization.

There are two key characteristics observed during this dissertation research that sets the SOC apart from supply chain operations in relation to organizational integration and support of secure information supply chains. One is the technical nature of work performed in cyber operations, not seen as a source of profit or return on investment, that makes it hard to communicate budget justifications to non-technical groups. And the other is the attitude of limited communication of specific SOC processes and procedures (justified by minimizing organization vulnerability), which limits insight by other functional roles into the work done in the SOC. Both characteristics will be discussed in depth in the section 0 (Research Limitations)

Processes of Implementation and Advancement for Distributed Information Supply Chains

Throughout this research effort, the author had the chance to interact with and observe network and security professionals starting at the analyst level all the way up to the chief information security officer. The author also interacted with cross functional teams of global manufacturing

organizations from finance, operations, application services, and business IT. Distribution operations employees involved in this research included the shop floor level, supervisors, operations managers, plant managers and senior executives. Despite linked goals and priorities, it was noted during this research that, due to lack of a common “language,” operations and finance teams struggle with communicating with technical IT teams during project implementation. For many supply chain information system projects, IT teams are forced to lead the implementation project with limited implementation process knowledge. It is critical that both information and operations teams agree on the benefits and priorities for implementing the new system, without distributed teams feeling compound obligations to (1) lead the implementation, (2) learn how to follow the new process, and (3) train their employees affected by the change while carrying out their daily work and responsibilities. The dissertation provides evidence that these challenges are general across organizations in diverse industries and sectors, whose functions may not include linked security operations centers, network operations center, and supply chain operations teams. The approach presented in this dissertation was intended to provide an example of mitigating the gap in communication between cross functional teams involved in deploying a new business system or launching enhancements to an existing one. It sets explicit responsibilities during the phases of implementation. It also aims at taming the levels of frustrations of the primary system user (operations) after the system is launched and ready to use. This is primarily achieved by including the user in the implementation process similar to the classic user center designed approach for home consumers (Abrams, Maloney-krichmar, & Preece, 2004). Completely excluding the user or asking the user to take charge are two extremes that must be avoided to achieve success.

UX Research: Corporate Systems Vs Consumer Applications

An unanswered question from Project 1 involves the design and implementation of a set of user-centered tools to support NOC / SOC analysts. Although not fully addressed in this dissertation, the successful implementation of a workforce analytics enterprise software tool in Project 2, integrating supply chain and security functions, suggests that additional tools to support NOC and SOC functions in an enterprise setting can be developed using a similar user-centered approach. Several research questions / hypotheses are to be addressed in future work beyond this research:

RQ1: Is the list of NOC / SOC improvement tools (described in Chapter 4) in the correct order of priority and feasibility for development?

RQ2: What elements and representations of NOC / SOC operations, and NOC / SOC teams, are most relevant to effective presentation of relevant network health and team performance in these tools?

RQ3: What is the feasibility of creating and implementing one or more these tools for operational implementation and/or sale in the network security industry?

However, these questions must be considered with a significant caveat regarding the processes and challenges of user experience (UX) research. The dynamics and impact of user experience (UX) research and design vary widely between the corporate (enterprise-level) and consumer (individual user) worlds. Corporate UX research presents distinct challenges and barriers compared to consumer UX research. Usability studies and updates to consumer apps available on a smartphone are more visible than new versions of enterprise software systems. The number of available applications, as well as the number of potential sales units for consumer applications, helps highlight the UX function in application design. It is easier to model the knowledge base of the consumer rather than the enterprise system user. Applications designed for consumer use, such as bank applications, YouTube, Fitbit, or Google Maps, require little training or domain expertise for a user to master the various functions. The same is not true for systems, such as Kronos (labor management) and EPIC (electronic healthcare records system), utilized by corporations that are intended for specialized users.

Furthermore, the simplicity of the tasks being accomplished in the consumer application helps reduce the barrier required for the UX *designer* to effectively develop consumer-level products. Since consumer applications are predominantly used to perform activities that would be considered basic to an average individual, minimal background knowledge and training are required for the UX designer to understand the application, user needs and develop ways to improve it.

By contrast, some enterprise-level systems are aimed towards specialized users who have knowledge that an average individual would not possess without extensive training. This adds an additional layer of complexity to the UX designer and researcher, making it unfeasible to conduct research without obtaining background information on the area in question and mastering the dynamics of that system. For instance, a medical record enterprise system requires specialized training for qualified health professionals to integrate into an expertise-driven task (healthcare delivery). The need for this training associated with corporate systems complicates the corporate UX research route.

Aside from barriers to corporate UX research that pertain to the actual applications or systems, competition among consumer applications within a specific market segment prompts investment in UX research as a competitive advantage. For example, the presence of multiple large bank systems, such as Chase, Bank of America, and Wells Fargo, each with a mobile application that enables bank clients to perform a plethora of financial transactions from their mobile devices, creates an increasingly competitive arena for enhancing the consumer's experience with the mobile application. The bank whose application and online portal provides the most favorable user experience may be the ones that wins over the most clients. Conversely, only a few major players control the corporate system market. Companies such as Kronos (labor management), EPIC (healthcare system), SAP & Oracle (Financial and ERP business systems) and Red Prairie (Warehouse Management System) are leaders in their respective specialties with few to no competitors. This leads to less emphasis on competitive UX research to achieve advantages.

Not only is there limited competition in the corporate world that may de-prioritize UX research, there are potential limits to the availability of qualified participants. Consumer applications with potential user populations of millions of adopters may find significant test populations willing to volunteer their time, at no cost or for a small incentive, in order to participate in UX research aimed at improving a particular application. Enterprise systems for specialized users, on the other hand, may have challenges in recruiting research participants. This is further aggravated by specialized users who are working professionals with limited extra time to volunteer; in some cases, the employer may restrict participation in UX work, especially if such participation is seen as affecting a competitive bid or maintenance contract process.

Despite the complexities of corporate UX design for enterprise-level systems, there is one sense where it is the more cost effective area for return on investment (for the implementing organization). Corporate UX research can lead to higher avoided costs of failures to use the system properly as compared to consumer UX research. For example, if a user of the Chase bank mobile application is unable to navigate the application properly in order to deposit a check, his or her biggest loss will be a delay in the deposit of the money, and consequently a delay in the availability of funds to the user. In contrast, if an employee in a supply chain function is unable to perform a task in the corporate system that leads to perishables being left to spoil in the port, the company would suffer a profound monetary loss. Performing UX research on corporate systems on a regular basis would help offset such unnecessary costs.

Impact on Business Acquisitions

The results of this research effort are not only applicable to enhancing digital system deployment within an existing organization, but also to business acquisitions and mergers with decisions to be made regarding duplicative or incompatible information technology systems. It has become a common trend for business from diverse industries to acquire one another. Such was the case when Amazon acquired Whole Foods in 2017: a supply chain service and technology company acquired a grocery provider. With the great diversity in the types of businesses comes substantial challenges in integrating the businesses (and their information technology systems and cultures) and consolidating them under one ownership.

When a merger occurs, onboarding can be a lengthy process, lasting for weeks or even months, and extending beyond HR merging and explanation of benefits. However, in order for a merger to occur smoothly the acquiring business must employ an efficient approach for managing operations until all systems have been successfully merged and all employees have been successfully (re)trained on technologies and processes. Failure to do so would negatively affect the business since deployment of the acquiring business's systems and procedures in the acquired party may take some time.

Furthermore, timelines set for mergers are extremely critical in order for the acquiring business to realize the cost justification initially anticipated, and planned for, with the merger. It is inefficient and unfeasible, in the long run, for organizations to support multiple divergent systems, whether it be IT systems or others. As soon as planning for a merger begins, the clock begins ticking for how quickly the two entities become one as every day lost in alignment and coordination delays the return on investment of the acquisition and makes the cost justification for the merger less favorable. Leveraging existing resources becomes vital as does their effective allocation. For example, having two IT support teams available to provide assistance for two ERPs cannot be financially justifiable. It surely leads to the underutilization of personnel and an inefficient use of resources. Thus, upon acquiring a business, the enterprise must promptly share an infrastructure and information flow. The findings of research conducted by this team include methods that can be implemented during a merger to facilitate its timely cost justification.

The trend of businesses from diverse industries complicates the path of merging technology systems in the timeliest, most efficient fashion possible. The merging process is already a challenging one, even with both companies being competitors from the same industry. When the

companies are from completely different industries, there is an added level of complexity to the merger. In order to illustrate the challenges faced during mergers, the example of the Amazon acquisition of Whole Foods will be revisited. While Amazon is a supply chain service and technology (Kindle, Echo, etc.) company, Whole Foods was a provider of perishable, physical goods (fresh groceries). In addition to being from two completely different industries prior to the acquisition, each organization has its own supplier management solution, enterprise resource planning system (ERP), and finance management reporting tools, amongst other systems that represent the backbone of any successful business organization. Time sensitivity of the merger is not only about efficiencies in merging cultures, but in meeting the anticipated return on investment that was assumed during the merger negotiations.

The author's research introduces methods that enhance system learnability and implementation in a complex, distributed organization. In fact, the Project 2 organization, through organic growth as well as acquisitions, has the challenge of merging over 100 ERP systems. It is hoped that the processes and evidence-based outcomes from this dissertation can help with the integration and consolidation of many information technologies originally designed for distinct cyber operations and cyber-physical supply chain operations.

End to End Visibility

Management of change is a practice set in place to ensure health & safety regulations are controlled when a change is made within a facility. This procedure exists with different names with a similar check list to ensure changes made within a team or department are communicated to other parties that may be impacted by that change. Cross functional collaboration is a must to perform business efficiently; operating in silos leads to failure.

Competitiveness and the fast-paced nature of business today requires enterprises to go beyond management of change. Dealing with change is an ongoing process. End to end visibility is a must. Organizations such as the Project 2 distribution centers are forming "control towers" for their supply chain operations (Doesburg & Tholhuijsen, 2016) to provide the needed visibility. The control tower is a committee of subject matter experts from teams across the supply chain (purchasing, supply planning, demand planning, marketing, sales, customer service, manufacturing, distribution & transportation). One goal of these control towers is to develop and deploy information technology solutions that pull information internally from the organization's

systems as well as tapping external resources such as ports, transportation carriers, social media and weather forecasts to support subject matter experts in decision making and event response. The findings of this research can help control tower teams utilize the intelligent solutions provided similar to supply chain cyber system implementation discussed in the methods and results sections of this document.

Research Limitations

On an organizational level, there is often a technical barrier between SOC's and other departments, thus preventing members of those departments from recognizing the value of research aimed at enhancing SOC's. Members of other departments have limited access or technical training to understand the details, function, or value of a cybersecurity or network operations center in their organization. Risks and opportunities identified within the information security organization are not openly communicated with the rest of the organization. This leads to SOC being decoupled from the other operations teams and the rest of the organization. This decoupling is detrimental to the organization as it prevents cooperation within the organization, particularly when it comes to research initiatives that would further streamline SOC. On a financial level, cyber operations do not derive direct profit. As a result, organizational decision makers hardly see the value of investing in an organizational function that only avoids loss (and intangible loss at that).

Even if the stated challenges within an organization are addressed and a research project is initiated, another challenge quickly arises. SOC's are increasingly protective of their data, such that they are unable to provide research institutions with access that would allow research efforts to be fruitful for the SOC. This particular situation was encountered by the author and research team colleagues while working under a Purdue CERIAS (The Center for Education and Research in Information Assurance and Security) grant. Despite the project being structured and positioned in such a way that would minimize obstacles to deriving interventions that are implementable to the organization, the challenging nature of SOC access limited progress in the project. First, affiliation with a research organization, such as the Purdue CERIAS, was not always adequate to allow for sufficient access to data. Even after conducting preliminary interviews at a leading cybersecurity conference, further access to the organizations and broad economic sectors included in the interviews remained difficult.

The author was able to participate in an internship program to conduct a case study in the SOC of a manufacturing organization. The internship entailed temporary employment by the company, helping mitigate issues of resistance from SOC teams that had been encountered with other organizations. Valuable information was obtained during this case study; however, the author did not have permission to disclose much of the activity observed. As a result, Project 1 did not materialize in UX-based tool implementation in the SOC environment. It yielded valuable recommendations and identified a trend of challenges that could be extrapolated into other environments, making this project pivotal in the course of the author's progress as a foundation for Project 2 system design, implementation and deployment.

A shift from the cybersecurity environment to the cyber-physical operations environment did increase the ability and freedom of reporting on supply chain information visualization. The issues encountered in the cyber-physical operations environment mirror those in the cybersecurity environment. Amongst those issues, as identified by Project 1 conducted in the SOC environment, are challenges in information sharing and presentation; incident response; problem escalation; and performance tracking. While both environments share these issues, they differ in one key area. The cyber-physical operations environment is a more distributed, shared-access (intranet-based) information technology system where information can be more freely shared across departments within the organization. This shift enables research to be conducted at the level and scope that allows specific interventions to be discussed and implemented at an enterprise scale. Since insider threats are a concern in the SOC environment, cyber security teams only share general recommendations or descriptions of system analysis or implementation processes.

In conclusion, while the research experience in the security cyber environment was challenging due to issues inherent to this environment, it identified key points that facilitated the author's transition to the cyber physical operations environment. This effectively increased the researcher's flexibility in reporting on supply chain information visualization and allowed for the completion of the research.

CONCLUSION

In the technologically dynamic world of the early 21st Century, machine learning, data analytics capability, and computing power have yielded systems that are capable of a variety of actions based on data acquisition and integration. However, human teams within organizations are often unable to fully utilize these systems' advanced capabilities. Both organizational resistance and technology capability misalignments stand in the way of the use of more advanced systems and embracing technology in completing daily tasks and strategic goals.

This dissertation research is aimed at resolving this discrepancy, by demonstrating conceptual orientations and systematic processes that help improve the implementation of enterprise-level information technology systems. More specifically, this research focuses on facilitating the design, implementation, and deployment of new cybersecurity and cyber-physical operations systems, as well as the training of employees on how to utilize the advanced technology to enhance their daily operations.

This research focused on different work environments within a geographically and functionally distributed operations setting. These work environments included network operations, security operations, and supply chain and distribution operations. Within these settings, two key areas were examined. The first area studies interactions between human team members and the technology systems in use with the goal of improving information presentation and generating a more efficient process for team-level decision making and incident response. The second area pertains to interactions between individuals of different hierarchies within the organization. In the supply chain setting the different hierarchies, in order of increasing management authority, are shift supervisors, operations managers and senior management. In the cyber operations setting, which encompasses the security and network settings, the hierarchy, in order of increasing management authority, is analyst, senior analyst, and manager.

The research effort was comprised of two key projects. Project 1 was conducted with a focus on multiple cybersecurity IT operations setting, and was geared towards addressing means by which collaboration within and across teams in IT operations, and in cases beyond the CISO (Chief Information Security Officer) office, can be improved. Project 1 was ended at a pre-implementation state, such that recommendations were made to the organization, but they were not actually implemented to a work setting. Nonetheless, it yielded three key findings (1)

performance of novice analysts is limited by the usability of tools on hand, (2) performance of senior analysts is bound by limitations in the delegation of tasks to novice analysts and the availability of status/context tools, and (3) lack of information alignment, situation awareness, or team performance status in SOC is, per se, a NOC/ SOC vulnerability.

Due to limitations of the security environment hindering research progression due to its inherently protective nature (as described in section 5.5), the research shifted to the supply chain setting of managing flows of physical goods in an enterprise setting. Similar operational, team coordination, and cyber-physical challenges are faced by supply chain teams interacting with technology solutions in their work environments. Project 2 involved an actual implementation of the findings from Project 1 in a supply chain setting, allowing their team to design, implement and deploy a performance management cloud-based solution for an e-commerce distribution operation. Project 1 also laid the foundation for project 2, so that project 2 had a well-defined research question and did not require exploratory subjective data collection. During project 2, the author led all the steps in the transition from an organization not having a mechanism to track operational performance to the **implementation** of a fully automated performance management solution. Methods in that stage included user research, interviews, usability and interface design and testing. Benefits of the performance management solution were realized shortly after implementation.

Key **benefits** of the Project 2 implementation included

1. *benchmarking*- Information visualization enabled benchmarking, such that the performance of workers in the same team completing the same tasks could be compared within and across shifts;
2. *goal setting*- With the variation in worker expertise, due to factors such as high turnover in the workforce, the newly implemented system serves as a reliable tool to separate workers in to virtual groups while taking their expertise into consideration when setting goals;
3. *hourly tracking*-the newly implemented system provided with smaller time intervals reviewed throughout the day to aid in the identification of slow performers and investigate root causes on the floor;
4. *sharing best practices*- utilization of a performance management system enabled comparison of task spread across the different plants in the network;
5. *overtime reduction*-the performance management solution allowed for improved productivity, a well-managed workforce and standardization of work tasks, which led to a

reduction in the need for overtime labor and hence a significant reduction in salaries was observed.

Findings of Project 2 illustrated the potential impact that this research can have on streamlining the implementation of new information technology systems in distributed organizations.

A unique set of **constraints** stands in the way of corporations conducting the UX research necessary to enhance their operations. These constraints include the complexity and specialized knowledge to understand the scope of the corporate system, limited competition amongst corporate system providers, and potentially limited availability of expert participants for corporate system testing.

Furthermore, the author's interactions with individuals of varying hierarchies within their respective organizations, in the cyber physical and other diverse settings, including finance, global manufacturing and operations, demonstrated the effective implementation of user experience techniques in enterprise-level information system implementation. Additionally, the findings of this research demonstrated that the **challenges** faced by different industries, including cyber physical and supply chain settings, when introducing a recent technology, or an enhancement to an existing technology, are almost identical. The Project 2 implementation was able to demonstrate an information technology system implementation that achieved significant and fast-accruing benefits to the organization with minimal disruption to the overall workflow.

Aside from enhancing routine technological solution transitions within an organization, this research is highly impactful for streamlining the **successful completion** of a merger. Unique challenges arise when business acquisitions and mergers require the integration and consolidation of redundant or incompatible enterprise-level information technology systems. This research introduces methods for enhancing system learnability and implementation. Incorporating these methods into business acquisitions would aid in streamlining them and facilitate a smoother transition for all parties involved. While these methods were initially applied to cybersecurity, cyber-physical and supply chain operations, they are equally applicable to systems utilized in a wide spectrum of areas, such as auditing, HR, finance and customer service.

Another area where the findings of this research are becoming increasingly significant is **management of change** through the use of control towers (a committee of subject matter experts and decision makers from teams across the supply chain). Since dealing with change is an ongoing process, organizations resort to the use of control towers to provide for the necessary visibility.

Findings from this research can assist control tower teams in utilizing the intelligent solutions provided, as was discussed in the methods and results sections of this document regarding supply chain cyber system implementation.

Finally, it is crucial to note that the implementation of new technological solutions by organizations is not an optional endeavor. Failure to stay up to date with the most advanced methods of managing operations, and continuing to perform tasks the classic way, is extremely risky as it could quickly lead to bankruptcy. In a highly competitive technology environment, businesses that lack the infrastructure to revolutionize their procedures, based on market needs, often fall behind and struggle visibly. Therefore, investing resources in research, such as the one this team has conducted, becomes monumental for survival in today's fiercely competitive market. Of note is that fact that this research was initially conducted in the cybersecurity setting, which proved to be an inherently challenging area to yield research progress. Within an organization, there is often a technical barrier between the SOC and the remainder of the organization making it challenging for individuals outside the SOC to understand the potential value of investing on the SOC. Due to the nature of the information handled by SOC, findings of research are not likely to be openly communicated. The highly technical nature of SOC operations also makes it challenging for non-SOC executives to understand SOC data and operations to a sufficient degree that they are willing to support research initiatives. Therefore, SOC find it difficult to justify funding for research or strategic performance improvements to organizational executives since there is not direct profit of cyber operations.

While the research community tends to focus on physical supply chains of goods and services, it is crucial to highlight the need for research on information supply chains. In a physical supply chain, the primary focus is on a tangible good; an information supply chain (including that for services) focuses on the entire process of information creation, processing, and use, as well as the flow of tangible goods and production materials. Information is created from transactions, stored, analyzed, presented, and then used to support decision making and performance measurement. Considerable research has been conducted on classic supply chain optimization problem, however, there is minimal research to date in the area of information supply chains (particularly secure cyber-physical information supply chains). The manifestation of that is the lack of information alignment, deficiencies in information sharing and communication between different levels of the organization, inability to make informed decision to respond to adverse events, and absence of

mechanisms for tracking and management of performance. By integrating cybersecurity, network operations, and supply chain functions to improve secure information supply chains, organizations can benefit by increased organizational security, process integrity, and resource availability.

REFERENCES

- Abras, C., Maloney-krichmar, D., & Preece, J. (2004). User-Centered Design. In *Encyclopedia of Human-Computer Interaction* (pp. 1–14).
- Agre, J., Kramer, C., & Vassiliou, M. S. (2011). Collective C2 in Multinational Civil-Military Operations ". *16th ICCRTS*, (4), 55.
- Bailey, B. P., & Iqbal, S. T. (2008). Understanding changes in mental workload during execution of goal-directed tasks and its application for interruption management. *ACM Transactions on Computer-Human Interaction*, 14(4), 1–28. <https://doi.org/10.1145/1314683.1314689>
- Blais, C. L., Goerger, N. C., Richmond, P., Gates, B., & Willis, J. B. (2005). Global Information Grid services and generation of the mobility common operational picture. In *Fall Simulation Interoperability Workshop (SIW)*.
- Boukhtouta, A., & Berger, J. (2014). A Framework of Recognized Operational Support Picture for Asset Visibility. *Procedia - Social and Behavioral Sciences*, 147, 251–259. <https://doi.org/10.1016/j.sbspro.2014.07.168>
- Brewer, I., & McNeese, M. (2004). Expanding concept mapping to address spatio-temporal dimensionality. In *Concept Maps: Theory, Methodology, Technology. Proceedings of the First International Conference on Concept Mapping* (Vol. 1, pp. 101–107).
- Businessweek, B. (2011). *The Current State of Business Analytics : Where Do We Go From Here? Bloomberg Businessweek Research Services*. Retrieved from [busanalyticsstudy_wp_08232011.pdf](#)
- Chang, Y. B., & Gurbaxani, V. (2012). The impact of IT-related spillovers on long-run productivity: An empirical analysis. *Information Systems Research*, 23(3 PART 2), 868–886. <https://doi.org/10.1287/isre.1110.0381>
- Chen, H., Chiang, R., & Storey, V. C. (2012). Business Intelligence and Analytics : From Big Data To Big Impact. *Mis Quarterly*, 36(4), 1165–1188. <https://doi.org/10.1145/2463676.2463712>
- Conti, G., Nelson, J., & Raymond, D. (2013). Towards a cyber common operating picture. *International Conference on Cyber Conflict (CyCon)*, 1–17.

- Department of Homeland Security. (2016). US Customs and Border Protection
<https://www.cbp.gov/>.
- Devaraj, S., & Kohli, R. (2000). Information Technology Payoff in the Health-Care Industry: A Longitudinal Study. *Journal of Management Information Systems*, 16(4), 41–67.
<https://doi.org/Article>
- Doesburg, R. van, & Tholhuijsen, W. (2016). Clearing the fog around the control tower. *Expert Insights DSV*.
- Eldardiry, O. M., & Caldwell, B. S. (2015). Improving Information and Task Coordination in Cyber Security Operation Centers. In *Proceedings of the 2015 Industrial and Systems Engineering Research Conference* (p. 2015).
- Endsley, M. R. (1995). Toward a Theory of Situation Awareness in Dynamic Systems. *The Journal of the Human Factors and Ergonomics Society*, 37(1), 32–64.
<https://doi.org/10.1518/001872095779049543>
- Endsley, M. R. (2012). *Designing for situation awareness: An approach to user-centered design*. CRC Press.
- Endsley, M. R., Bolstad, C. A., Jones, D. G., & Riley, J. M. (2003). situation awareness oriented design: from cognitive requirements to creating effective supporting technologies. In *Human Factors and Ergonomics Society* (pp. 268–272).
- Foroughi, C. K., Werner, N. E., Hatcher, M. C., Lopez, a. J., Zafar, T. W., & Boehm-Davis, D. a. (2014). Do Interruptions Affect Content Production? *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, 58(1), 255–259.
<https://doi.org/10.1177/1541931214581053>
- Foster, J. (2006). Collaborative Information Seeking and Retrieval. *Annual Review of Information Science and Technology Definition*, (2003), 329–356.
- Fruhlinger, J., & Wailgum, T. (2017, July 10). 15 famous ERP disasters, dustups and disappointments. *CIO Digital Magazine*. Retrieved from
<https://www.cio.com/article/2429865/enterprise-resource-planning/enterprise-resource-planning-10-famous-erp-disasters-dustups-and-disappointments.html>

- Garrett, S., & Caldwell, B. (2002). Describing functional requirements for knowledge sharing communities. *Behaviour Information Technology*, 21(5), 359–364. Retrieved from <http://www.informaworld.com/openurl?genre=article&doi=10.1080/0144929021000050265&magic=crossref>
- Garrett, S. K., & Caldwell, B. S. (2006). Team resource foraging in event-driven task environments. In *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*. <https://doi.org/10.1177/154193120605001512>
- Garrett, S. K., & Caldwell, B. S. (2006). Team Resource Foraging in Event-Driven Task Environments. In *Proceedings of the Human Factors and Ergonomics Society Annual Meeting* (Vol. 50, pp. 1514–1518). <https://doi.org/10.1177/154193120605001512>
- Garrett, S. K., Caldwell, B. S., & Collins, S. T. (2009). Supporting Expertise Coordination in Multidisciplinary Project Teams. *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, 53(16), 1008–1012. <https://doi.org/10.1177/154193120905301602>
- Grant, R. M. (1996). Prospering as in Integration Environments : Organizational Capability Knowledge. *Organization Science*, 7, 375–387.
- Guralnik, D. B., & Friend, J. H. (1960). *Webster's new world dictionary of the American language (College ed.)*. “Cleveland, OH: World Publishing.”
- Kepes, B. (2013, December 17). Avon's Failed SAP Implementation A Perfect Example Of The Enterprise IT Revolution. *Forbes Tech*. Retrieved from <https://www.forbes.com/sites/benkepes/2013/12/17/avons-failed-sap-implementation-a-perfect-example-of-enterprise-it-revolution/#2fae7f7431a6>
- Kohli, R., & Devaraj, S. (2003). Measuring information technology payoff: A meta-analysis of structural variables in firm-level empirical research. *Information Systems Research*, 14(2), 127–145. <https://doi.org/10.2307/23011464>
- Kroculik, J. (2014). An end-to-end communications architecture for condition-based maintenance applications. *Open Architecture/Open Business Model Net-Centric Systems and Defense Transformation*, 9096(June 2014). <https://doi.org/10.1117/12.2053133>
- Laaperi, L., & Vankka, J. (2015). Architecture for a system providing a common operating picture of critical infrastructure. In *2015 IEEE International Symposium on Technologies for Homeland Security (HST)* (pp. 1–6). <https://doi.org/10.1109/THS.2015.7446228>

- Laudon, K., & Laudon, J. (2012). *Management information systems: managing the digital firm. MIS: Managing the Digital Firm* (Vol. 7). <https://doi.org/10.1590/S1415-65552003000100014>
- Li, H. (2015). “To shave or not to shave”. In *Enhancing User Experience of Enterprise Systems for Improved Employee Productivity: A First Stage of Case Study*. <https://doi.org/10.1007/978-3-319-20895-4>
- Mahmud, I., Ramayah, T., & Kurnia, S. (2017). To use or not to use: Modelling end user grumbling as user resistance in pre-implementation stage of enterprise resource planning system. *Information Systems*, 69, 164–179. <https://doi.org/10.1016/j.is.2017.05.005>
- Mantovani, G. (2001). The Psychological Construction of the Internet: From Information Foraging to Social Gathering to Cultural Mediation. *CyberPsychology & Behavior*, 4(1), 47–56.
- Marston, S., Li, Z., Bandyopadhyay, S., Zhang, J., & Ghalsasi, A. (2011). Cloud computing - The business perspective. *Decision Support Systems*, 51(1), 176–189. <https://doi.org/10.1016/j.dss.2010.12.006>
- McGuinness, B., & Foy, L. (2000). A subjective measure of SA: the Crew Awareness Rating Scale (CARS). In *Proceedings of the first human performance, situation awareness, and automation conference*.
- McNeese, M. D., & Brown, C. E. (1986). Large group displays and team performance: An evaluation and projection of guidelines, research, and technologies. *Security*.
- Mcneese, M. D., Pfaff, M. S., Connors, E. S., Obieta, J. F., Terrell, I. S., & Friedenber, M. A. (2006). multiple vantage points of the common operational picture: supporting international teamwork. In *PROCEEDINGS of the HUMAN FACTORS AND ERGONOMICS SOCIETY 50th ANNUAL MEETING* (pp. 467–471). <https://doi.org/10.1177/154193120605000354>
- McNeese, N. J., Reddy, M. C., & Friedenber, E. M. (2014). Towards a Team Mental Model of Collaborative Information Seeking during Team Decision-Making. *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, 58(1), 335–339. <https://doi.org/10.1177/1541931214581069>
- NASA. (2007). *NASA Systems Engineering Handbook. Systems Engineering* (Vol. 6105). [https://doi.org/10.1016/0016-0032\(66\)90450-9](https://doi.org/10.1016/0016-0032(66)90450-9)

- Onwubiko, C. (2009). Functional requirements of situational awareness in computer network security. *2009 IEEE International Conference on Intelligence and Security Informatics*, 209–213. <https://doi.org/10.1109/ISI.2009.5137305>
- Press, A. (2012, November 16). United Airlines' Flights Are Delayed by a Computer Failure. *New York Times*, p. B2.
- Press, G. (2013, April). A Very Short History of Information Technology (IT). *Forbes*. Retrieved from <http://www.forbes.com/sites/gilpress/2013/04/08/a-very-short-history-of-information-technology-it/>
- Ravichandran, T., & Lertwongsatien, C. (2005). Effect of Information Systems Resources and Capabilities on Firm Performance : A Resource- Based Perspective. *Journal of Management Information Systems*, 21, 237–276. <https://doi.org/10.1080/07421222.2005.11045820>
- Ravichandran, T., Liu, Y., Han, S., & Hasan, I. (2009). Diversification and Firm Performance: Exploring the Moderating Effects of Information Technology Spending. *Journal of Management Information Systems*, 25(4), 205–240. <https://doi.org/10.2753/MIS0742-1222250407>
- Rejab, M., Noble, J., & Allan, G. (2014). Locating Expertise in Agile Software Development Projects, 260–268.
- Rummukainen, L., Oksama, L., Timonen, J., & Vankka, J. (2014). Visualizing common operating picture of critical infrastructure. <https://doi.org/10.1117/12.2050231>
- Sandstrom, P. E. (1994). An Optimal Foraging Approach To Information Seeking And Use. *Library Quarterly*, 64(4), 414–449.
- Santhanam, R., & Hartono, E. (2003). Issues in linking information technology capability to firm performance. *Mis Quarterly*, 27(1), 125–153. <https://doi.org/10.1017/CBO9781107415324.004>
- Sawyer, B. D., Finomore, V. S., Funke, G. J., Mancuso, V. F., Funke, M. E., Matthews, G., & Warm, J. S. (2014). Cyber Vigilance: Effects of Signal Probability and Event Rate. *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, 58(1), 1771–1775. <https://doi.org/10.1177/1541931214581369>
- Shennan, S. J. (2002). Genes, memes and human history: Darwinian archaeology and cultural evolution.

- Steenbruggen, J., Nijkamp, P., Smits, J. M., & Grothe, M. (2012). Traffic incident management, a common operational picture to support situational awareness of sustainable mobility. *International Journal of Transport Economics*, 39(1).
- Tang, C. (2006). Perspectives in supply chain risk management☆. *International Journal of Production Economics*, 103(2), 451–488. <https://doi.org/10.1016/j.ijpe.2005.12.006>
- Tatham, P., Spens, K., & Kovács, G. (2017). The humanitarian common logistic operating picture: a solution to the inter-agency coordination challenge. *Disasters*, 41(1), 77–100. <https://doi.org/10.1111/disa.12193>
- Taylor, C., & Arthanari, T. (2017). Enabling Disaster Relief Supply Chain Visibility (SCV) and Supply Chain Coordination (SCC). In *Americas Conference on Information Systems* (pp. 1–10).
- Widera, A., Lechtenberg, S., Gurczik, G., & Bähr, S. (2017). Integrated Logistics and Transport Planning in Disaster Relief Operations. In *14th ISCRAM Conference* (pp. 752–764).
- Winterhalder, B. (1981). optimal foraging strategies and Hunter-Gatherer Research in Antropology: Theory and Models.
- Wong, W. P., Veneziano, V., & Mahmud, I. (2016). Usability of Enterprise Resource Planning software systems: an evaluative analysis of the use of SAP in the textile industry in Bangladesh. *Information Development*, 32(4), 1027–1041. <https://doi.org/10.1177/0266666915585364>

APPENDIX A. RSA CONFERENCE

INTERVIEWS SCRIPT

Hi, I am Omar I am a graduate student at Purdue University. I am working on a research project and currently trying to understand how network operations center analysts use information from visual displays and dashboards.

Do you mind if I ask you some questions regarding my project? It should not take more than 15-20 minutes!

Do you mind if I record your answers for note taking purposes only? Saving time and will be destroyed right after it is written. I will not include any information that may identify you or your organization.

1. My name is Omar Eldardiry, the Principal investigator is my adviser, Dr Barrett Caldwell. You can reach him at bscaldwell@purdue.edu for further questions/information about this research.
2. I will be recording this interview for note taking purpose only. Your information is confidential. So, the collected information will not be related to you or your organization.
3. Your participation is voluntary and you may skip any questions
4. You must be at least 18 to participate

List of Questions:

1. How long have you been working in the field, how long with your current organization?
2. How big is your organization in terms of number of employees, how many are involved with cyber security?
3. What are the 5 or 10 main types of information cyber network analysts need in order to fulfill their job requirements?
4. What types of events generate this information and how can these events affect the network?
5. What other sorts of internal/external manifestations that can interrupt the regular work routine for an analyst, overload or crash the network? What additional information that an analyst would wish to have to tame the effect of such unexpected incidences?
6. How do analysts divide work and network monitoring among each other? Based on technical functions/ physical separations/ expertise ...etc.
7. Do analysts work independently or collaborating?

DATA COLLECTION

Participant 1

Background

Years of experience: 12 years.

Years in current organization: 12 years

Size of company: less than 100

Number of employees involved with security: all

What are the main types of information needed?

1. Users IP addresses
2. Destination of malware
3. Spread of malware around the organization
4. The source of malware and
5. How it intruded the system and found its way into the organization

The best status of analysts is to do nothing, if you have the right set of tools and security products the company will always be able to get the right results in the right time. Otherwise delays occur. Some companies just do not have the right set of tools, something to do with forensics not the real time problem they are facing. (examples of tools: ecut – netwitness) “problem of supplies”

How analysts divide work?

It depends but for the company I work for it is a physical separation and also level of expertise of analysts. For example, dealing with threats generated inside the organization (information leakage) is easier and requires fewer skills than malware attacks and threats from outside.

Do analysts collaborate?

Unfortunately, they do not. But it would be more efficient to share knowledge about occurring incidents. Sharing data about different customers is valuable, for example, if an IP is found to be bad then other analysts should be aware. Also, sharing expertise will allow analysts to learn about new threats that their co-workers dealt with.

Participant 2

Background

Years of experience: 16 years

Years in current organization: 5 years

Size of company: 70,000 employees

Number of employees involved with security: 150 employees

What are the main types of information needed?

This is more operational, I work in the governmental side of the company

APT (Advanced Persistent Threat) is a constant threat in my defense contracting company.

Threat vectors to analyze. Common attack signatures. Profile the threat actors, top 10 groups that keep trying to intrude our network, so we have profiles built on them and all this is built in into our detection system. IP address, etc.

Compiling common threat analysis that can be shared across the company.

What other manifestations can break the work routine?

The attackers are professionals that plan for months looking for vulnerabilities, they slowly sneak in trying not to raise red flags and show that there is an attack.

The containment interrupts the workflow and all efforts go towards defending the network.

A challenge is when you have millions and millions of alerts and limited number of staff. What to look for and where to find it becomes really hard.

It's a mature network, so maybe things breakdown here and there but that is not considered a security issue and does not cause lots of problems.

How analysts divide work?

Not really sure how the team is organized, but I know that the skillset plays a big role. Junior analysts go to the basic architecture things while more advanced analysts help create and set profiles of threats

Do analysts collaborate?

They have to collaborate, they always share profiles of threats.

Participant 3

Background

Years of experience: more than 15 years.

Years in current organization: 13 years

Size of company: 21,000 employees

Number of employees involved with security: 130 employees (only 4 are fully dedicated to security!)

What are the main types of information needed?

Information relevant to generated alerts, threat vectors

For example: a suspicious change in the system: an administrator escalated a privilege at 2 am. That is an alert

Analysts are responsible to analyze the event correlation. Computing power is not enough, human correlation is needed in addition. Relevant information would be in this case: login information, IP address involved, login time, who logged in, where is he/she located.

What other manifestations can break the work routine?

Initial response: I do not understand the question. For example, if a system failure takes place?

This is not the greatest challenge. From the operations perspective, defining the cause and fix it will take care of such incidents. When a JVM for example runs out of memory it is easy to spot and fix.

However, if a criminal causes a failure of the system then he is dumb. When a failure happens, everybody is checking the logins and scanning the network to define the source of problem.

A certain procedure is followed to solve the problem. On the other hand following procedures cannot fix more complex problems

How analysts divide work?

Working is separated by technical functions and also depending on the area of expertise of each analyst. Some analysts happen to work better with DBA, JVMs, JBOSS, Routing, or Linux.

Do analysts collaborate?

Analysts work independently; most analysts do the same set of activities. After spending a period of 30 to 90 days they are familiar with majority of incidents. After that, most events are predictable, randomization drops greatly.

From a different perspective, analysts are always juniors. Once they reach a certain number of years they seek higher positions especially to avoid working at bad shifts and aiming at higher salaries. And so, analysts rarely have the right set of skills to deal with more complex unstructured problems as mentioned before. If such complexity occurs at night shifts, an analyst need to report to senior admins and a sense of collaboration would take place at this point.

Seniors trying to avoid receiving phone calls at 2 am or on weekends from analysts, they attempt to standardize work. Develop more work procedures for analysts to follow. (if you see this, this and this then you need to do the following).

Participant 4

Background

Years of experience: 29 years

Years in current organization: 10 years

Size of company: 8,000 employees

Number of employees involved with security: 30 employees (described as a large group)

What are the main types of information needed?

In the NOC you are heavily focused on networking and telecommunication and computer science (initial response, the interviewee thought I am asking about the analysts' background)

NOC is a set of tools that monitors the health of the environment. So looking at up time, down time, turnaround time (time to live): when you ping something how long does it take to go there and come back. Focused on that bit level, so if time to live is high there might be something that clogs the network or something down, I need to go and see and what is going on. This is a lot of what they see on the screen, statistics stuff, if things are healthy or not. Of course if there is something that does not work, they would call in and see what's going on.

Also, load balancing, how I better distribute the load and traffic to get the best speed and maximum efficiency.

What other manifestations can break the work routine?

1. If they get no reply, sometimes you cannot access the webpage. A typical cause would be servers hang/freeze (especially Microsoft servers, UNIX are more robust).
2. Another cause is the VMware, a lot of people use virtual environments. In those environments you might hit a glitch of VMware.
3. You run out of storage space, maybe because of many log records that eats up the storage space or many users using the system and you did not know about it.
4. Hardware malfunction, this is rare.
 - a. A lot of errors, error messages, fail to connect, user cannot access the app when I click on it nothing happens, user calls the app manager and the app manager calls the NOC
 - b. NOC usually can see the network and can see for example which servers went down or so. They know what apps are running on this server and should link to the app managers, notify them that the server is down, and the app is down.

How analysts divide work?

It depends on the organization. In our environment the NOC runs the firewalls, the load balancers, the remote access devices, the routers, the connections and backup connections to the internet, and the switches

There is a mix on how they divide work. They are all looking, one might be very good at Cisco and Palo Alto and Juniper, another one might be good at checkpoint whatever firewall you have and maybe the switches. So maybe by expertise

Do analysts collaborate?

They have to collaborate. You got to talk to your neighbor when you run into a problem. At the end of each incident they do RCA, what happened how it was fixed and how it should not happen again, so this is always debatable in knowledge base.

They are not very good at retrieving the case from the knowledge base if a similar incident is happening, usually they start troubleshooting and if it is getting more complicated they will start asking have you ever seen that before. And then will start going into the knowledge base.

Other Comments

NOTE: [the relationship between SOC and NOCs] you want to ensure that staff from NOC and SOC work closely together, when SOC running into some detection or even antivirus check, they should be able to go talk to NOC and say hey I got these IPs or machines detected can you tell me what they are? NOC should be able to provide more information.

NOC if they have a DDOS (distributed denial of service) attack; a NOC will be the one saying hey we are getting hammered our bandwidth is coming down this looks like a DDOS attack; the SOC will be the one going on the internet and find out if there is any DDOS going on that we should know about it. And gets the NOC information, this is what we are seeing.

Participant 5

Background

Years of experience: 10 years

Years in current organization: 18 months

Size of company: 120,000 employees

Number of employees involved with security: 2,000 employees

What are the main types of information needed?

1. They need to know what are the valuable assets that they are protecting
2. What is the architecture of the existing information system within the company
3. Understand who and how is impacting them
 - a. Data points about intrusions
 - b. What is abnormal, so they need to first understand and define what is normal
 - c. Be able to determine real and false positives to focus their resources on real positives
 - d. Prioritize problems, because resources is always a limitation

What other manifestations can break the work routine?

APT, DOS or DDOS

In any network there some attributes like: bandwidth, latency, and data transfer rates

For these attributes you should know what normal for them and what is abnormal for two segments of the network: internal network, external connections

For abnormal there are two types: genuine and malicious that can cause spikes

Example: 1. DDOS for external connection, malicious 2. Server failure, genuine

SISO (senior information security officer) and security management teams can be involved for malicious abnormalities

Other examples: cut of intercontinental cable, solar flares (rare), network grids failure

The maturity of processes, skills and tools in other words capability of the company makes it easy or hard for the company to differentiate between malicious and genuine abnormalities and easily detect them

How analysts divide work?

Most popular segregations are by expertise: experts in network security, firewall, performance issues, routers, etc.

Sometimes there are some generalists that keep looking at the screens and move problems to more experts in level 2 or 3 that filter false positives and work on fixing issues

Do analysts collaborate?

Work environment is collective, quick group thinking, looking at different tools. Work has to be collaborative.

Participant 6

Background

Years of experience: 10 years

Years in current organization: 10 years

Size of company: 1,000 employees

Number of employees involved with security: 50 employees

What are the main types of information needed?

Based on rules, assets, system events, correlation of events,

What other manifestations can break the work routine?

DDOS, system failures, patching problems; such problems can slowdown the network or unavailability

How analysts divide work?

Security operations looking at monitors detecting red flags, then problems are moved to level 2 where teams will check the correlation of data whether or not it is a false alarm, level 3 that is more specialized and work on solving the problem trying to bring things to normal status

Do analysts collaborate?

Collaboration happens at all and between the three levels

Participant 7Background

Years of experience: 19 years

Years in current organization: 5 years, 2 years in the current position

Size of company: 14,000 employees

Number of employees involved with security: between 200 and 300 employees

What are the main types of information needed?

1. The applications running in the environment
2. The users, user identities and users spread within the organization

Side note: North-South means flow of data to and from the organization. East-West means flow of data within the organization (less priority)

3. State of applications, alerts from applications being compromised (attacked) assuming that policies are set.
4. Different groups of users using different applications. For example: sales personnel use these applications.
5. Compromised servers.
6. Guest operating terminals (end points). An analyst should be able to stop traffic if a guest terminal is compromised.
7. Setting Policies around a particular event. For example: guest is compromised, policy is stop traffic. (even if malware is treated an analyst should not trust and block the traffic)

Less important information

8. Threats that are coming up so that the analyst can be ahead of the game (maybe displayed on a side scree)

What other manifestations/events can affect the work routine? (source of generated information)

Source: Malware attacking the service

Operating system crashed

Hardware crashes. For example: switch malfunction,...etc.

Effect/result: application failure or compromise

Rare to happen but Is it easy to identify and solve hardware crashes?

It is relatively easy most of the time. Suddenly, no traffic from this endpoint, a report is generated

Also, all systems are compliant with regulations. Companies use software products to scan the system regularly to ensure the system is compliant.

How analysts divide work?

Dividing the network can be done in different ways depending on the size of the network and analysts expertise.

Do analysts collaborate?

They have to collaborate. Also, there are collaboration efforts between network admins, security admins and storage admins where I work. This is vital to solve in common problems.

Participant 8

Background

Years of experience: 32 years

Years in current organization: 6 months

Size of company: less than 5,000 employees

Number of employees involved with security: 35 employees

What are the main types of information needed?

1. Visualize the whole network: every location, circuit, links between locations. One of the operators' tasks is to monitor all these elements
2. Drilling down to every switch, device and wire. Not the host/infrastructure but the routers and more detailed elements
3. The analyst also should understand the host where the primary computing is at.

ATM is the host. Branches have multiple hosts. All connected by infrastructure (see drawn map in notebook)

What other manifestations can break the work routine?

1. Computer going in a loop, a process sending a lot of transactions saturating the line
2. Atlanta snow Jam: large numbers of people reaching ATMs to get cash, high demand
3. Attacks: DDOS on the website, *surge* in demand
4. Breaking a link: AT&T network was down because a farmer was digging a whole to bury his dead cow in the early 1990s
 - a. If carrier has good sensors, it can determine the damage location
 - b. If redundancy is available it can switch information flow to other tracks

How analysts divide work?

Work is divided by what needs to be monitored. Multiple NOCs report to a central NOC.

Do analysts collaborate?

Juniors are looking at yellow/red pop-up in the map. Medium expert analysts making decisions switching to alternate routes, senior experts architecting changes and improving the maps

Senior experts also work on solving more complex problems

They 100% collaborate, constant discussions, must work in the same room.

Figure below shows a diagram drawn by research participant 8 as an example of network components of a national bank need to be managed by a Network Operations Center (NOC) team.

APPENDIX B. SOC CASE STUDY

DATA COLLECTION

During the month of August 2014, a visit was made to a fortune 350 manufacturing company with around 13,000 employees. The company owns 4 different business segments. Each segment manufactures a different set of products and competes in a different market.

IT within the company is separated into three separate functions: (1) Network (backup, network power, hardware and other tasks related to network health and performance) (2) Security (Intrusion Prevention, data loss prevention, hacking, vulnerability, and other security related tasks) and (3) Systems (system upgrades installation, configuration, troubleshooting, and other tasks related to maintaining the system). A team from each function exists for each segment. In addition, there one more team for each of the three functions on the corporate level connecting all teams together. The system teams are the only 24/7 operating teams. Arising problems after business hours are reported to the security and network teams to be processed the following day. Depending on the urgency of the problem, security or network employees can be called in after business hours. Different segments own manufacturing operations in eight different U.S. states as well as Australia, Belgium, Canada, China, France and Romania. The company also owns offices in multiple locations in Europe, The Middle East, Brazil and India. The multiple sites existing at different time zones are adding to the complexity of IT teams' mission.

During the visit to the company's headquarters in the Midwest of USA, the researcher had a chance to spend time with the corporate level IT security team. Tasked accomplished were as follows: daily team meeting, reviewing Remedy (a tool used to keep track incidents' status), discussing priority items, ongoing projects, investigating unsolved delayed incidents, assigning new incidents to analysts in the team based on expertise and nature of the problem.

Researcher shadowing four analysts from the team as well as their team lead, during the time of shadowing he was introduced to the nature of tasks assigned to each member of the team, the different tools and software packages the team is using and the daily challenges the analysts are facing.

Researcher interviewed the four analysts that participated in the shadow session, their team lead and the area manager. This document highlights the findings from the interviews. The interviews are then listed in the order where they were conducted.

Primary Findings

1. The goal of any IT security team is to protect the system's CIA - Confidentiality (unauthorized disclosure of data), Integrity (unauthorized change of data) and Availability (system functions are accessible to the right people/ security controls)
2. Security operations require multiple software tools to cover the variety of tasks. IT service (Remedy), SIEM - Security Information and Event Management (QRadar), investigation (RSA security Analytics), data loss prevention, and IT performance Management. There is a necessity for the different tools to efficiently communicate. For example, some acts as input to others. It is highly recommended to have these tools as packages of the same software vendor to facilitate this communication. However, it is found that IT security operators sometimes prefer to use tools from multiple companies because of the features each has to offer. (think of a mac user that prefers an android phone over an iphone that can better sync with his personal computer)
3. Junior IT analysts deal with standard processes, goal directed task analysis can be helpful to map the "ideal" state of the analysts to their actual state. While senior analysts deal with more complex tasks and need to work on improving their execution of investigation
4. Team leads have a variety of responsibilities:
 - (1) Risk management, looking beyond monitoring or response to specific incidents like other analysts are doing to proactively detection of possible threats (what can happen), the sources of threats and vulnerabilities (how a threat can happen). For that they need better status tools/ displays of the current state of the organization. While developing the appropriate metrics to monitor the system acts as a challenge, finding the right tool to collect data and display it to managers is even a bigger struggle. It has been found that the team leads use spreadsheets for that purpose. And that is mainly because the need of a

flexible tool, easy to customize, do basic computations (like percentages), create graphical presentations of data and avoid buying other expensive IT management tools.

- (2) Team performance, for this there is another need of status tools/displays for the activity of the security team. Where they are (actual status) in comparison to where they need to be (planned status)
5. In this regard, a part of the area managers' responsibilities is to report both security status of the system and status of the IT teams to non IT senior managers for multiple reasons like justifying their budgets or reporting their progress
6. At various levels IT employees still use spreadsheets for tracking and other purposes. This shows either missing features of tools in use, lack of software tools in the market or inadequacy of the available tools

Secondary Findings

7. It is possible for companies to retain a security operations team only during business hours rather than a 24/7 operation. This highly depends on the nature of the business rather than the size. However, members of the security must always be available to be called in by other 24/7 IT teams when necessary.
8. Combining the NOC and SOC to be managed by the same team is possible and depends mainly on the size of the organization
9. Team collaboration in security operations centers is vital. It must happen (1) on the team level at least on daily basis (2) between analysts to collaborate on non-repetitive/unstructured incidents and to share new lessons learned and (3) across levels to escalate challenging issues and status of projects in progress.
10. While analysts tackle incidents of different nature, each one still specializes in a specific topic (for example data loss prevention, employee termination, investigation, etc.) to develop some expertise and make improvements to this domain. This is partially considered as a proactive approach where collaboration does not take place as efficient as in reactive or incident response contexts.

INTERVIEW RESPONSES

One on one interviews performed were audio recorded. Answers are highlighted in yellow below. Recordings were destroyed after all answers were captured and documented.

Participant 1 (Team Lead)

1. What general industry do you work in?

☐ Banking
 ☐ Aviation
 ☐ Medicine
 ☐ Telecommunications
☐ Energy
 ☐ University / Research
 ☐ Other: **Manufacturing**

2. What area(s) of network and / or security operations are your job responsibilities focused (select all that apply)?

☐ Security Awareness
 ☐ System Management
 ☐ System Audit
☐ System Architecture
 ☐ Operations
 ☐ Hacking
☐ Forensics
 ☐ Incident Response / Recovery
 ☒ Generalist
 ☐ Other

3. What term best describes your level of activity and responsibility in your organization?

☐ Analyst
 ☒ Team Lead
 ☐ Area Manager
 ☐ Executive

4. On a 1-7 scale (1 – not at all important, 7 – very important) would you say each of the following goals is for your operations center?

(7) Security (internal and external threats)
 (1) Network performance and efficiency
(1) Network health
 (4) Network recovery (for example, after a storm outage)

5. Lots of different contributors to network downtime or degraded system behaviors can be described as an “adverse event”. (For instance, a corporate website may be taken offline due to a severe storm with tornadoes, an accidental deletion of a critical file, or an organized denial of service attack, as well as due to other causes.) Which types of adverse events do you focus on in your position?

Any Adverse events that affects the Confidentiality, Integrity and Availability (CIA) of the system
Confidentiality: unauthorized disclosure; Integrity: Changing of Data; Availability: The system functions are accessible to the right people

6. What are the main daily decisions you need to make? Do you primarily focus on a) monitoring (tracking) network and system performance before an adverse event), b) response to an event, or a c) combination of both? If both, can you estimate the percentage of time you spend (per day, per week) on each?

(b) Response on higher level, decision making related to new and ongoing projects

7. What types of information do you need most to complete your tasks, and what sorts of tools and / or displays do you use to get that information? How often does the information need to be updated for you to feel confident that you are looking at helpful information to complete your tasks?

The role of the team leader is more of risk management. The concerns are primarily: threats (what can happen) and vulnerability (how the threat can occur)

Situational Awareness about threats and sources of threats, for example: an inactive account of a retired employer that is still not terminated - buying/installing new software/technology – employees uploading data to clouds which increases the risk and magnifies the complexity of keeping the data secured

Information needed comes from awareness of the new threats and from all departments within the organization

8. Do you frequently use the same combinations of information in the same way when completing your tasks across different days, or do you need to create new combinations of information for different situations or events?

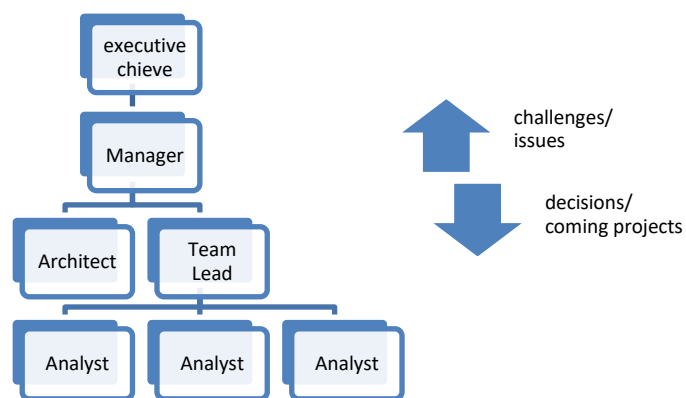
No, it is always different based on projects in progress

9. What are the biggest challenges to knowing and getting access to what you need for the presentation of information to complete your tasks?

Data from other departments is not fed to IT security team. For example an engineering team bought a \$200,000 package of software without prior notice to the security team. Then, the team contacted us seeking help for the installation process. As a result, the security team had to work on creating a secure environment when it was best to be aware 3 months earlier when it was possible to alter the purchase decision or at least do ensure the necessary work can be done prior to the purchase transaction.

10. Do you normally collaborate with other people when completing your tasks? What sorts of information do you receive from other people (either vertically or horizontally in the organization)? What information are you expected to pass on to others (either vertically or horizontally in the organization)?

Very collaborative, both vertically and horizontally, daily 8:30 am meeting to setup priorities and daily goals



11. What types of tools and information presentation would you like to have to complete your tasks, but are currently difficult or confusing to get and use? Have you seen an example of this tool or information presentation that seems to do well at what you want?

Currently working on KPIs/ summary Metrics for different Segments to be able to identify the owner (segment and network/security/systems)

Using spreadsheets: customizable, flexible, easy to do basic percentage calculations to compare planned with actual, low cost compared to expensive IT management packages in the market,

Examples for Metrics:

1. Network Access Control (NAC) Deployment - A setting on routers checks certain measures to identify level of trust for hardware connected (plugging laptop to the network, it checks the domain, if antivirus on laptop is up to date, safe to let it access the network) a CISCO tool is used for NAC
2. System Patching
3. Anti-Virus Health

Participant 2 (level 1 analyst)

Background

Translate incidents into Remedy tickets; respond to majority of recurring incidents/tickets

2. What area(s) of network and / or security operations are your job responsibilities focused (select all that apply)?

☒ Security Awareness ☐ System Management ☐ System Audit
☐ System Architecture ☐ Operations ☐ Hacking
☒ Forensics ☒ Incident Response / Recovery ☐ Generalist ☐ Other

3. What term best describes your level of activity and responsibility in your organization?

☒ Analyst ☐ Team Lead ☐ Area Manager ☐ Executive

4. On a 1-7 scale (1 – not at all important, 7 – very important) would you say each of the following goals is for your operations center?

☒ Security (internal and external threats) ☒ Network performance and efficiency
☒ Network health ☒ Network recovery (for example, after a storm outage)

5. Lots of different contributors to network downtime or degraded system behaviors can be described as an “adverse event”. (For instance, a corporate website may be taken offline due to a severe storm with tornadoes, an accidental deletion of a critical file, or an organized denial of service attack, as well as due to other causes.) Which types of adverse events do you focus on in your position?

Website compromises - Domain control issues - Network failure - System crash - Huge outage
(team does not get involved in minor outage recovery)

6. What are the main daily decisions you need to make? Do you primarily focus on a) monitoring (tracking) network and system performance before an adverse event), b) response to an event, or a c) combination of both? If both, can you estimate the percentage of time you spend (per day, per week) on each?

c) Combination, translating new incidents to tickets

Respond to assigned incidents - 60 to 70% response

7. What types of information do you need most to complete your tasks, and what sorts of tools and / or displays do you use to get that information? How often does the information need to be updated for you to feel confident that you are looking at helpful information to complete your tasks?

Information from Remedy-daily team meetings-security analytics- Qradar

Other tools: excel (tracking), ipvoid.com (check ip address), iana.org (port#), Google search

- I must have Q-radar open at all times.

8. Do you frequently use the same combinations of information in the same way when completing your tasks across different days, or do you need to create new combinations of information for different situations or events?

It depends on the assigned ticket. Set standard filter combinations for regular incidents.

For non-recurring I have to work out a new filtering route (5-10% are non-recurring)

9. What are the biggest challenges to knowing and getting access to what you need for the presentation of information to complete your tasks?

Analyst did not have an answer for this question since he is novice (6 months working experience) and most of tasks assigned are well structured

10. Do you normally collaborate with other people when completing your tasks? What sorts of information do you receive from other people (either vertically or horizontally in the organization)? What information are you expected to pass on to others (either vertically or horizontally in the organization)?

Very collaborative, both vertically and horizontally, daily 8:30 am meeting to setup priorities and daily goals

11. What types of tools and information presentation would you like to have to complete your tasks, but are currently difficult or confusing to get and use? Have you seen an example of this tool or information presentation that seems to do well at what you want?

Analyst did not have an answer for this question since he is novice (6 months working experience) and most of tasks assigned are well structured

Participant 3 (level 3 analyst)

Background

- RSA Security Analytics, investigating sharing classified files in emails, malware, and other security related to network traffic
- RSA Security Analytics does not feed input of data rather than a tool to investigate highlighted incidents from QRadar and other sources that acts as data input
- Employee termination

2. What area(s) of network and / or security operations are your job responsibilities focused (select all that apply)?

☐ Security Awareness ☐ System Management ☐ System Audit

☐ System Architecture ☐ Operations ☐ Hacking

☒ Forensics ☒ Incident Response / Recovery Generalist

☒ Other investigation

3. What term best describes your level of activity and responsibility in your organization?

XXX Analyst __ Team Lead __ Area Manager __ Executive

4. on a 1-7 scale (1 – not at all important, 7 – very important) would you say each of the following goals is for your operations center?

(7) Security (internal and external threats) (2) Network performance and efficiency

(2) Network health (1) Network recovery (for example, after a storm outage)

5. Lots of different contributors to network downtime or degraded system behaviors can be described as an “adverse event”. (For instance, a corporate website may be taken offline due to a severe storm with tornadoes, an accidental deletion of a critical file, or an organized denial of service attack, as well as due to other causes.) Which types of adverse events do you focus on in your position?

DDOS attacks, compromised sites, security breach

In case of security breach I drop whatever I am working on and focus on this specific incident

6. What are the main daily decisions you need to make? Do you primarily focus on a) monitoring (tracking) network and system performance before an adverse event), b) response to an event, or a c) combination of both? If both, can you estimate the percentage of time you spend (per day, per week) on each?

Combination 50-50

7. What types of information do you need most to complete your tasks, and what sorts of tools and / or displays do you use to get that information? How often does the information need to be updated for you to feel confident that you are looking at helpful information to complete your tasks?

Log events – metadata – Qradar (time lag between event and information displayed is less than 15 minutes) – Security Analytics (time lag is around 15 minutes) I check Qradar and Security Analytics at least every hour

8. Do you frequently use the same combinations of information in the same way when completing your tasks across different days, or do you need to create new combinations of information for different situations or events?

5-10% new incidents, but other that I use the same combination of information for example phishing I know exactly what to do and sometimes it takes just few seconds to fix a phishing incident.

9. What are the biggest challenges to knowing and getting access to what you need for the presentation of information to complete your tasks?

Giving access to employees – approval requests often do not provide sufficient information

10. Do you normally collaborate with other people when completing your tasks? What sorts of information do you receive from other people (either vertically or horizontally in the organization)? What information are you expected to pass on to others (either vertically or horizontally in the organization)?

Talking to peers for unusual incidents to brainstorm or to update the team. Interact frequently with other teams discussing or seeking more details about tickets initiated by other teams from different segments or functions

11. What types of tools and information presentation would you like to have to complete your tasks, but are currently difficult or confusing to get and use? Have you seen an example of this tool or information presentation that seems to do well at what you want?

Agreeing with point made on software combining different tools only if having eligible characteristics. For example, QRadar is more Robust SIEM than others. Similarly, RSA Security Analytics for metadata allow the user drill down and have more information accessibility.

In other words, the company can pay to activate an additional module of the RSA software to replace QRadar SIEM tool. The analyst believes that this will facilitate his job, however the company decided not to do so since analysts agreed that QRadar is a more robust SIEM tool.

Side Note from analyst: 6 years ago the security team did not exist and was part of the Network Team

Participant 4 (level 2 analyst)

Background

- Intrusion detection system (IDS) one of the most mature security products in the market
- Source fire acts a sniffer, it detects everything over network, hook it up on te network and does all the matching and capture by itself. It follows vulnerability rules created by vulnerability detection teams
- Instant Response to detections, team is trying to be more proactive
- This tool, source fire, feeds into the log aggregation tool QRadar(SIEM) – Qradar acts as a storage media and correlates data from different tools
- Analysts prioritize and read through incidents appearing at QRadar

2. What area(s) of network and / or security operations are your job responsibilities focused (select all that apply)?

☒ Security Awareness ☐ System Management ☐ System Audit
☐ System Architecture ☒ Operations ☐ Hacking
☒ Forensics ☒ Incident Response / Recovery Generalist ☐ Other

3. What term best describes your level of activity and responsibility in your organization?

☒ Analyst Team Lead ☐ Area Manager ☐ Executive

4. On a 1-7 scale (1 – not at all important, 7 – very important) would you say each of the following goals is for your operations center?

☒ (7) Security (internal and external threats) ☒ (1) Network performance and efficiency
☒ (3) Network health ☒ (1) Network recovery (for example, after a storm outage)

5. Lots of different contributors to network downtime or degraded system behaviors can be described as an “adverse event”. (For instance, a corporate website may be taken offline due to a severe storm with tornadoes, an accidental deletion of a critical file, or an organized denial of service attack, as well as due to other causes.) Which types of adverse events do you focus on in your position?

Outage - Network failure - System crash- (sharing of classified documents)

6. What are the main daily decisions you need to make? Do you primarily focus on a) monitoring (tracking) network and system performance before an adverse event), b) response to an event, or a c) combination of both? If both, can you estimate the percentage of time you spend (per day, per week) on each?

Combination; 30-40% Response, some weeks are busier than others!

7. What types of information do you need most to complete your tasks, and what sorts of tools and / or displays do you use to get that information? How often does the information need to be updated for you to feel confident that you are looking at helpful information to complete your tasks?

Assigned ticket details from Remedy, Monitoring Qradar, project updates from team leader or manager, awareness from arstechnia.com

8. Do you frequently use the same combinations of information in the same way when completing your tasks across different days, or do you need to create new combinations of information for different situations or events?

Around 15% of incidents are none recurring

9. What are the biggest challenges to knowing and getting access to what you need for the presentation of information to complete your tasks?

Working with other IT teams in remote location, for example their response time might be different than ours and so we could not deliver to the customer in a timely manner as we are used to.

10. Do you normally collaborate with other people when completing your tasks? What sorts of information do you receive from other people (either vertically or horizontally in the organization)? What information are you expected to pass on to others (either vertically or horizontally in the organization)?

Same answer as other analysts

11. What types of tools and information presentation would you like to have to complete your tasks, but are currently difficult or confusing to get and use? Have you seen an example of this tool or information presentation that seems to do well at what you want?

No Answer.

Participant 5 (level 3 analyst)

Background

Data loss prevention: File integrity tool, recover lost files, control employees access to files, inactive users do not need access, what folders, files were created by who at what time.

2. What area(s) of network and / or security operations are your job responsibilities focused (select all that apply)?

☒ Security Awareness ☐ System Management ☐ System Audit
☐ System Architecture ☒ Operations ☐ Hacking
☒ Forensics ☒ Incident Response / Recovery ☐ Generalist ☐ Other

3. What term best describes your level of activity and responsibility in your organization?

☒ Analyst ☐ Team Lead ☐ Area Manager ☐ Executive

4. On a 1-7 scale (1 – not at all important, 7 – very important) would you say each of the following goals is for your operations center?

☒ (7) Security (internal and external threats) ☒ (2) Network performance and efficiency
☒ (3) Network health ☒ (1) Network recovery (for example, after a storm outage)

5. Lots of different contributors to network downtime or degraded system behaviors can be described as an “adverse event”. (For instance, a corporate website may be taken offline due to a severe storm with tornadoes, an accidental deletion of a critical file, or an organized denial of service attack, as well as due to other causes.) Which types of adverse events do you focus on in your position?

Compromised Systems, websites, workstations or servers

6. What are the main daily decisions you need to make? Do you primarily focus on a) monitoring (tracking) network and system performance before an adverse event), b) response to an event, or a c) combination of both? If both, can you estimate the percentage of time you spend (per day, per week) on each?

75% monitoring and 25% responding to incidents from Remedy

7. What types of information do you need most to complete your tasks, and what sorts of tools and / or displays do you use to get that information? How often does the information need to be updated for you to feel confident that you are looking at helpful information to complete your tasks?

Log – more data to correlate with a certain log makes a great difference, the more related and up to date information to a specific incident is available the easier it is to get the job done

8. Do you frequently use the same combinations of information in the same way when completing your tasks across different days, or do you need to create new combinations of information for different situations or events?

Most of the time combines new sets of tools and information due unstructured nature of incidents I am dealing with

9. What are the biggest challenges to knowing and getting access to what you need for the presentation of information to complete your tasks?

Diving into a new tool set, getting access, culture of the company (classified documentation), the fact that I have different goals

10. Do you normally collaborate with other people when completing your tasks? What sorts of information do you receive from other people (either vertically or horizontally in the organization)? What information are you expected to pass on to others (either vertically or horizontally in the organization)?

Lots of collaboration

Information I get is “who – what – why – when” all possible raw data can be used to help

Information I pass to the team is lessons learned, how the incident happened and how to react to it.

11. What types of tools and information presentation would you like to have to complete your tasks, but are currently difficult or confusing to get and use? Have you seen an example of this tool or information presentation that seems to do well at what you want?

Our office lacks large screens that can help save time instead of digging in different windows

Needing to reach out for other employees during investigation due to limited access

Participant 6 (Area Manager)

Background

All other analysts report directly to area manager

2. What area(s) of network and / or security operations are your job responsibilities focused (select all that apply)?

☐ Security Awareness ☐ System Management ☐ System Audit
☐ System Architecture ☐ Operations ☐ Hacking
☐ Forensics ☐ Incident Response / Recovery ☒ Generalist ☐ Other

3. What term best describes your level of activity and responsibility in your organization?

☐ Analyst ☐ Team Lead ☒ Area Manager ☐ Executive

4. On a 1-7 scale (1 – not at all important, 7 – very important) would you say each of the following goals is for your operations center?

(7) Security (internal and external threats) (3) Network performance and efficiency

(6) Network health (2) Network recovery (for example, after a storm outage)

5. Lots of different contributors to network downtime or degraded system behaviors can be described as an “adverse event”. (For instance, a corporate website may be taken offline due to a severe storm with tornadoes, an accidental deletion of a critical file, or an organized denial of service attack, as well as due to other causes.) Which types of adverse events do you focus on in your position?

Virus outbreaks, internal/external hacking, DDOS attacks, Websites failures, Theft of IT equipment, IT related investigations

6. What are the main daily decisions you need to make? Do you primarily focus on a) monitoring (tracking) network and system performance before an adverse event), b) response to an event, or a c) combination of both? If both, can you estimate the percentage of time you spend (per day, per week) on each?

70% monitoring, ensure new tools are operational/ functional

7. What types of information do you need most to complete your tasks, and what sorts of tools and / or displays do you use to get that information? How often does the information need to be updated for you to feel confident that you are looking at helpful information to complete your tasks?

Progress Reports, summary reports (how many open tickets/ incidents,
I use QRadar SIEM, Remedy, and reports from team lead

8. Do you frequently use the same combinations of information in the same way when completing your tasks across different days, or do you need to create new combinations of information for different situations or events?

New combinations is always needed

9. What are the biggest challenges to knowing and getting access to what you need for the presentation of information to complete your tasks?

Manipulating the data and understanding what information you are looking for. Relying on the skills of the team

10. Do you normally collaborate with other people when completing your tasks? What sorts of information do you receive from other people (either vertically or horizontally in the organization)? What information are you expected to pass on to others (either vertically or horizontally in the organization)?

Collaboration happens all the time. Vertically on the project level for example: recent project of removing windows XP from the network, what needs to be done, who is doing what and so on

11. What types of tools and information presentation would you like to have to complete your tasks, but are currently difficult or confusing to get and use? Have you seen an example of this tool or information presentation that seems to do well at what you want?

Interviewee had to leave for another meeting. I Did not have the chance to ask the question

APPENDIX C. PROJECT 2

INTERVIEW RESULTS (ROUND 1)

The figures in this section are examples of the mockups presented to SMEs in round 2 of the interviews based on data collected in round 1. Associates' names listed are not real and used to capture the format requested by the tool users, specifically functional area supervisors.

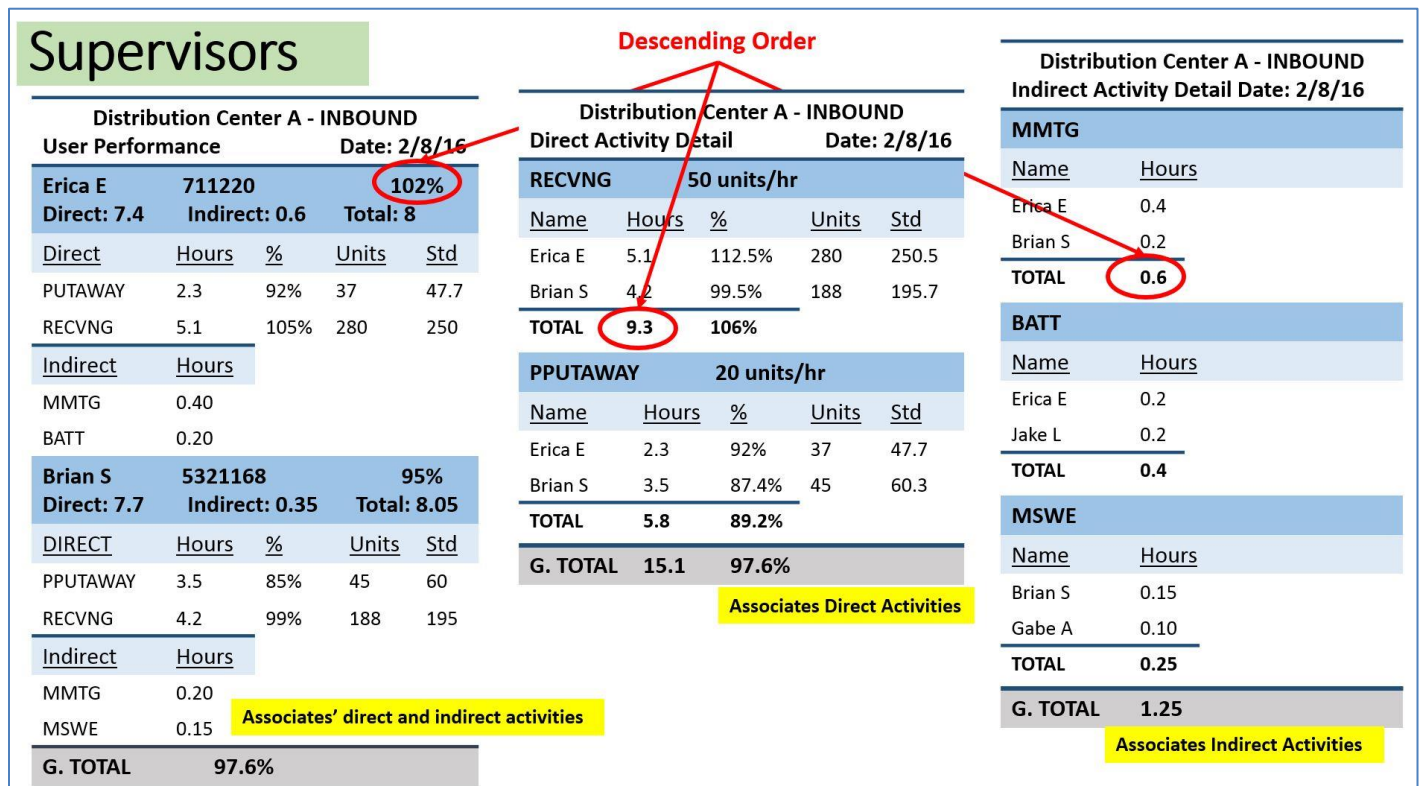


Figure 14 Slide 1 - Supervisors Reports Mockup

Operations Manager

Distribution Center A - Operations
Direct Activity by Dept Date: 2/8/16

Activity	Hours	%	Units	Std
PUTAWAY	5.5	105%	37	47.7
RECEIVING	7.1	92%	280	250
TOTAL	12.6	102%		

Activity	Hours	%	Units	Std
PTBLINES	8.1	99%	45	60
PTMPICK	3.6	85%	188	195
TOTAL	11.7	93.2%		

Activity	Hours	%	Units	Std
NCRPK	9.2	91%	45	60
PSHUTTLE	4.3	88%	188	195
TOTAL	13.5	89%		

G. TOTAL	37.8	94.7%		
-----------------	-------------	--------------	--	--

Direct Activities per Department

Distribution Center A - Operations
Indirect Activity by Dept Date: 2/8/16

Activity	Hours
BATT	5.5
MMTG	7.1
TOTAL	12.6

Activity	Hours
BATT	8.1
PALL	3.6
TOTAL	11.7

Activity	Hours
MMTG	9.2
MAINT	4.3
TOTAL	13.5

G. TOTAL	37.8
-----------------	-------------

Indirect Activities per Department

Distribution Center A
Operations Summary 01/31/16 – 2/06/16

Productivity				
	IB	OP	OB	TOTAL
1 st Shift	87%	91%	99%	92.3%
2 nd Shift	91%	92%	102%	95%
3 rd Shift	95%	103%	103%	100.3%
TOTAL	91%	95.3%	101.3%	95.8%

Direct Hours				
	IB	OP	OB	TOTAL
1 st Shift	340	372	345	1,057
2 nd Shift	272	289	271	832
3 rd Shift	169	224	176	569
TOTAL	781	885	792	2,458

Overall Productivity per Shift per Department

Figure 15 Slide 2 - Functional Managers Reports Mockup

Inventory Control Manager

Inventory Control – Distribution Center B						
CYCLE COUNTS	WEEK 5					01/31/16 – 02/06/16
	M	T	W	TH	F	TOTAL
1 st Shift	859	901	854	820	890	4,324
2 nd Shift	828	871	883	908	836	4,326
3 rd Shift	902	883	917	909	850	4,461
TOTAL	2,589	2,655	2,654	2,637	2,576	13,111

Cycle Count Locations

Inventory Control – Distribution Center B						
IC Productivity	WEEK 5					01/31/16 – 02/06/16
	M	T	W	TH	F	TOTAL
1 st Shift	97%	95%	104%	101%	87%	97%
2 nd Shift	100%	98%	111%	92%	89%	98%
3 rd Shift	99%	95%	100%	97%	91%	96%
TOTAL	99%	96%	105%	97%	89%	97%

Direct Activity Productivity

Inventory Control – Distribution Center B						
Indirect Hours	WEEK 5					01/31/16 – 02/06/16
	M	T	W	TH	F	TOTAL
1 st Shift	46	48	43	50	41	228
2 nd Shift	49	50	46	49	52	246
3 rd Shift	51	51	41	49	44	236
TOTAL	146	149	130	148	137	710

Indirect Activity Productivity

Figure 16 Slide 3 - Inventory Control Manager Reports Mockup

Plant Manager

Distribution Center D					
DC Summary by Dept. 01/31/16 – 02/06/16					
Productivity					
	This Week	Last Week	MTD	QTD	YTD
IB	91%	99%	96%	95%	95%
OP	97.2%	95%	96%	97%	97%
OB	104%	97%	99%	98%	98%
IC	100%	100%	97%	97%	97%
VAS	97%	95%	95%	93.5%	93.5%
TOTAL	98%	97%	97%	96%	96%

Overall Productivity by Department + Chart

Distribution Center D						
Plant Summary by Shift 01/31/16 – 02/06/16						
Productivity						
	IB	OP	OB	IC	VAS	TOTAL
1 st Shift	87%	91%	99%	100%	95%	92.3%
2 nd Shift	91%	92%	102%	102%	95%	96%
3 rd Shift	95%	103%	103%	-	78%	94.75%
TOTAL	91%	95.3%	101%	101%	89%	95.2%
Direct Hours						
	IB	OP	OB	IC	VAS	TOTAL
1 st Shift	340	372	345	225	360	1,642
2 nd Shift	272	289	271	105	281	1,218
3 rd Shift	169	224	176	-	230	799
TOTAL	781	885	792	330	871	3,659

Overall Productivity by Shift + Chart

Figure 17 Slide 4 - Plant Manager Reports Mockup

North America

North America						
Network Summary by DC 01/31/16 – 02/06/16						
Productivity						
	IB	OP	OB	IC	VAS	TOTAL
DC A	87%	91%	99%	100%	95%	92.3%
DC B	91%	92%	102%	102%	95%	96%
DC C	95%	103%	103%	99%	78%	94.75%
DC D	104%	97%	99%	98%	-	102%
TOTAL	91%	95.3%	101%	101%	89%	95.2%
Direct Hours						
	IB	OP	OB	IC	VAS	TOTAL
DC A	781	885	792	330	871	3,659
DC B	850	922	645	425	945	3,787
DC C	461	530	780	191	-	1,962
DC D	566	675	715	298	154	2,408
TOTAL	2,658	3,012	2,932	1,244	1,970	11,816

Productivity per Department per DC

North America					
Network Summary Cumulative 01/31/16 – 02/06/16					
Productivity					
	This Week	Last Week	MTD	QTD	YTD
DC A	91%	99%	96%	95%	95%
DC B	97.2%	95%	96%	97%	97%
DC C	104%	97%	99%	98%	98%
DC D	100%	100%	97%	97%	97%
TOTAL	98%	97%	97%	96%	96%

North America				
Network Indirect Hours by DC 01/31/16 – 02/06/16				
Indirect Hours				
	Indirect Hours	Total Hours	%	% last week
DC A	240	3,899	6.2	5.1
DC B	342	4,129	8.3	7.9
DC C	269	2,231	12	12
DC D	368	2,776	13.2	9.8
TOTAL	1,219	13,035	9.4	

Figure 18 Slide 5 - North America Executives Reports Mockup