

California State University, San Bernardino

**CSUSB ScholarWorks**

---

Theses Digitization Project

John M. Pfau Library

---

2011

## **Metrics framework for computer security incident response: A practical guide for the federal government**

Vincent Nithi Sritapan

Follow this and additional works at: <https://scholarworks.lib.csusb.edu/etd-project>



Part of the [Information Security Commons](#)

---

### **Recommended Citation**

Sritapan, Vincent Nithi, "Metrics framework for computer security incident response: A practical guide for the federal government" (2011). *Theses Digitization Project*. 3602.

<https://scholarworks.lib.csusb.edu/etd-project/3602>

This Project is brought to you for free and open access by the John M. Pfau Library at CSUSB ScholarWorks. It has been accepted for inclusion in Theses Digitization Project by an authorized administrator of CSUSB ScholarWorks. For more information, please contact [scholarworks@csusb.edu](mailto:scholarworks@csusb.edu).

METRICS FRAMEWORK FOR COMPUTER SECURITY INCIDENT  
RESPONSE: A PRACTICAL GUIDE FOR THE  
FEDERAL GOVERNMENT

---

A Project  
Presented to the  
Faculty of  
California State University,  
San Bernardino

---

In Partial Fulfillment  
of the Requirements for the Degree  
Master of Business Administration

---

by  
Vincent Nithi Sritapan

June 2011

METRICS FRAMEWORK FOR COMPUTER SECURITY INCIDENT

RESPONSE: A PRACTICAL GUIDE FOR THE  
FEDERAL GOVERNMENT


---

A Project  
Presented to the  
Faculty of  
California State University,  
San Bernardino

---

by  
Vincent Nithi Sritapan  
June 2011

Approved by:

  
C.E. Tapie Rohm Jr., Ph.D., Committee  
Chair, Information and Decision Sciences

  
Walter Stewart, Ph.D.

  
Jake Zhu, Ph.D., Department Chair,  
Information and Decision Sciences

*9 June 2011*  
Date

© 2011 Vincent Nithi Sritapan

## ABSTRACT

As technology advances and society becomes more dependent on information technology (IT), the exposure to vulnerabilities and threats increase. In the year 2000 the "I love you" virus, was able to cause over \$2 billion in damages worldwide. Many cyber threats have been reported and documented throughout the advancement of IT, resulting in not only monetary damages but invasion of privacy and risks to national security. Realizing the need for enhanced cyber security and information security management criteria, federal regulations have mandated the capability, provision, and notification of cyber security incidents. In this new direction, incident response plays an essential role in cyber security. It is one of the last lines of defense and is vital in the event of a cyber-catastrophe. However measuring the performance and creating accountability for computer security incident response (CSIR) capabilities still remains an issue. Many government organizations still struggle to determine what security metrics to use and how to find value within them.

In this effort a metrics framework has been developed for incident response to serve as an internal analysis, supporting continuous improvement in incident reporting and strengthening the security posture for an

organization's mission. There are five elements that are critical to the metrics framework for CSIR:

- 1) understanding the three types of measures,
- 2) establishing objective driven metrics, 3) produce results based on audience considerations, 4) tie incident response (IR) evaluations to improve IR capabilities that support the organization's mission, and 5) process flow identification for CSIR.

The goal of this metrics framework for (CSIR) aims to provide a holistic approach towards security metrics which is specific to incident reporting and promotes efforts of more practical and clear guidelines on measuring the computer security incident response team (CSIRT). An additional benefit to this project is that it provides middle management with a framework for measuring the results of incident reporting in a CSIR program.

## ACKNOWLEDGMENTS

I wish to thank the following people for helping me in my journey to discover what computer security incident response is and for aiding me in developing this metrics framework for computer security incident response:

- Committee Members for This Project: Dr. C.E. Tapie Rohm Jr., Dr. Walter Stewart, and Dr. Jake Zhu.
- Dr. Javier Torner, James Macdonnel, Laura Carrizales, Information Security Office at California State University San Bernardino
- Department of Treasury, Office of the Chief Information Officer in Cyber Security: CISO Edward Roback, ACISO Don Cohen, Senior Analyst (System One Contractor) Barbara Gorsen
- Gartner Analysts Michael Smith and Jeffrey Wheatman
- Scholarship for Service Program
- Information Assurance & Security Management Program at CSUSB
- California State University San Bernardino, MBA Research Grant and Business Alliance for their financial support

## DEDICATION

I wish to dedicate this MBA project to my family, friends, and CSUSB's MBA Information Assurance & Security Management program. Thank you all for the guidance, support, and encouragement to strive for more. My achievements are only as great as the people I am able to share them with. So thank you all and I will continue to excel and make you all proud.



## TABLE OF CONTENTS

ABSTRACT .....	iii
ACKNOWLEDGMENTS .....	v
LIST OF TABLES .....	ix
LIST OF FIGURES .....	x
CHAPTER ONE: BACKGROUND	
Introduction .....	1
Purpose of the Project .....	2
Problem Background .....	3
Context of the Problem .....	5
Scope of the Project .....	7
Significance of the Project .....	8
Assumptions .....	8
Limitations .....	9
Definition of Terms .....	10
Organization of the Project .....	11
CHAPTER TWO: REVIEW OF THE LITERATURE	
Introduction .....	13
Measurement Types for Computer Security Incident Response .....	14
Three Types of Measurements: Cost, Time, and Quality .....	15
Security Metrics .....	17
Objective Driven Measurements .....	18
Process Flow Identification .....	18
Audience Based Metrics .....	20

Tying Security Metrics to Organization's Mission .....	20
Summary .....	21
CHAPTER THREE: FORMATION OF THE PROJECT	
Introduction .....	22
Coursework .....	22
Internship .....	23
Literature Research .....	24
Summary .....	25
CHAPTER FOUR: METRICS FRAMEWORK FOR COMPUTER SECURITY INCIDENT RESPONSE	
Introduction .....	26
Steps to Use the Metrics Framework .....	27
Three Types of Measures for Computer Security Incident Response .....	28
Objective Driven Measurements .....	34
Audience Based Measurements .....	36
Tying Measurements to the Agency's Mission .....	39
Process Flow Identification .....	40
Measurement Form for Computer Security Incident Response .....	43
Summary .....	48
CHAPTER FIVE: APPLICATION OF THE FRAMEWORK	
Introduction .....	50
Case Scenario .....	50
Sample Data .....	53
Metric Development .....	55

Step by Step Application .....	55
Scope of Analysis .....	62
Results .....	63
Root Cause .....	67
Decision to Be Made By Management .....	68
Summary .....	70
CHAPTER SIX: CONCLUSIONS AND RECOMMENDATIONS	
Introduction .....	71
Conclusions .....	71
Recommendations .....	72
Summary .....	72
APPENDIX A: UNITED STATES COMPUTER EMERGENCY READINESS TEAM REPORTING CRITERIA .....	73
APPENDIX B: FORMULAS FOR COMPUTER SECURITY INCIDENT RESPONSE BY CENTER FOR INTERNET SECURITY .....	75
APPENDIX C: ACRONYMS .....	77
REFERENCES .....	79

## LIST OF TABLES

Table 1. Sample Incident Reports .....	54
Table 2. Duration for Sample Incident Reports .....	65

## LIST OF FIGURES

Figure 1.	Metrics Framework for Incident Response .....	27
Figure 2.	Three Measurement Types for Incident Response .....	28
Figure 3.	Cost Types for Incident Response .....	29
Figure 4.	Time Measurement Points for Incident Response .....	32
Figure 5.	Audience Based Measurements .....	36
Figure 6.	Bureau Level Process Flow .....	41
Figure 7.	Agency Level Process Flow .....	42
Figure 8.	Incident Response Measurement Form Part 1 .....	44
Figure 9.	Incident Response Measurement Form Part 2 .....	47
Figure 10.	The Metrics Framework for Incident Response .....	48
Figure 11.	Columns and Names for Sample Incident Reports .....	52
Figure 12.	Measurement Form for Metric ID 001 .....	57
Figure 13.	Measurement Form for Metric ID 002 .....	59
Figure 14.	Measurement Form for Metric ID 003 .....	61
Figure 15.	Incident Count by Category .....	63
Figure 16.	Incident Count by Category and Bureau .....	64
Figure 17.	Percentage of Incidents Reporting On Time .....	66
Figure 18.	List of Root Causes by Computer Emergency Response Team Coordination Center .....	67
Figure 19.	Measurement Form for Metric ID 004 .....	69

## CHAPTER ONE

### BACKGROUND

#### Introduction

As technology becomes more prevalent and reliance on IT expands, the exposure to vulnerabilities and threats increase. Malware, social engineering, and zero day attacks have evolved to outpace current IT security controls. In the 2009 Cyberspace Policy Review by the White House, the United States (US) acknowledged its need for more reliable, resilient, and trustworthy digital infrastructure for the future (White House, 2009). Realizing the need for enhanced cyber security and information security management criteria, federal regulations have mandated the capability, provision, and notification for cyber security incidents (H.R. 2458-56). The United States-Computer Emergency Readiness Team (US-CERT) requires incidents by category type for computer security incident response to be reported within specific timeframes. The requirement creates an audit trail for the purpose of awareness and collaboration. However, the main concern drawn from this initiative is accountability. How can an organization follow alerts, check validations, and track remediation efforts? What controls are in place to

determine if appropriate reporting methods exist and are being used properly? How can an organization verify that requirements are being met? Additionally, in the event that reporting methods are confirmed, how can organizations measure performance? By examining the federal work space, it is apparent that federal agencies are required to adhere to the Federal Information Security Management Act (FISMA) of 2002 (H.R. 2458–56), Office of Management and Budget (OMB) directives (OMB Circular No. A-130, Appendix III), and the Department of Homeland Security's (DHS) US-CERT timeframe reporting requirements (US-CERT, 2011). In this effort the metrics framework for incident response has been developed to serve as an internal analysis, supporting continuous improvement in incident reporting and strengthening the security posture for an organization's mission.

### Purpose of the Project

The purpose of this metrics framework for CSIR aims to provide a holistic approach towards security metrics which is specific to incident reporting and promotes efforts of more practical and clear guidelines on measuring the CSIRT. In addition, the purpose of this project is to provide middle management with a framework

for measuring the results of incident reporting in a CSIR program.

### Problem Background

From the birth of the Computer Emergency Response Team Coordination Center (CERT/CC) in 1988 (Computer Emergency Readiness Team, 2011A) to the establishment of the US-CERT<sup>1</sup> in 2003 (US-CERT, 2008), the US has acknowledged the need for real cyber security and CSIR reporting. In 1988 the Morris Worm, a self-replicating program, brought over 6000 computers worldwide to its knees (Garfinkel, 2005). In 1999 the Melissa Virus used Microsoft's Word and Excel exploits to propagate itself across the net via email (Mills, 2009). In 2000 the "I love you" bug, very similar to the Melissa Virus, added the ability to destroy data causing over \$2 billion in damages worldwide (PC Tools, 2010). Today, countries such as Estonia and Georgia are examples of when nation states have been incapacitated by the real dangers of cyber-attacks (Davis, 2007; & Markoff, 2008). Cyber threats now persist in the expansion of attack sophistication and in intruder knowledge (Software Engineering Institute, 2010). Since these events, efforts

---

<sup>1</sup> US-CERT is the operating arm of the National Cyber Security Division (NCSD) at DHS



for Public Private Partnership (PPP) and the construction of the US Cyber Command (USCYBERCOM) have demonstrated the new direction that the US government and US military are partaking (Armed Forces Communications & Electronics Associate, 2010). In this new direction, incident reporting plays the role of networking and collaboration. It is one of the last lines of defense and is vital in the event of a cyber-catastrophe.

The challenge to accurately determine if requirements are met is a tremendous difficulty to overcome. The Inspector General (IG) of an Agency and DHS, in pursuit of FISMA audits, has the role and responsibility to check if requirements are satisfied. Audits now move from yes and no questions to asking for greater detail to ensure compliance. As part of the 'National Cybersecurity Strategy' the DHS has been designated the focal point for critical infrastructure protection, where incident reporting is a main component of ensuring our national cyber security (National Security Council, 2011). Unfortunately, the past has demonstrated the lack of cyber security preparedness when it comes to federal agencies. The last review (2009) by the General Accountability Office (GAO) on federal wide information security controls stated that almost all 24 major federal agencies had

weaknesses in their information security controls (General Accountability Office, 2009). The US government as a whole is now trying to move towards greater cyber security controls, but ensuring collaboration and accountability is another issue.

### Context of the Problem

Although security metrics have gained large focus from government and industry, many organizations still struggle to determine what metrics to use and how to find value from them (Center for Internet Security Community, 2009; Gorsan, Personal Communication, 2010; & Torner, Personal Communication, 2011). The fundamental concern with security metrics comes from knowing how to capture the cause and effect. With greater requirements for security controls being mandated for accountability (Joint Task Force Transformation Initiative, 2009), many groups are creating their own security metrics without understanding the full scope or how it connects to the organization's objectives. For example, in the evaluation of incident reporting, incident types are categorized by the US-CERT. Timeframe requirements for reporting are given with the purpose of providing a methodology for awareness and coordination amongst key providers of our

technological infrastructure. In the federal work space the OMB Circular No. A-130 Appendix III directs federal agencies to "ensure that there is a capability to provide help to users when a security incident occurs in the system and to share information concerning common vulnerabilities and threats" (OMB Circular No. A-130, Appendix III, Para. A,3,a,2,d). In addition, places like NIST (NIST, 2011), CIS (Center for Internet Security Community, 2010), and CERT/CC (Computer Emergency Readiness Team, 2011B) all provide guidance and various metrics on measuring incident response handling. The amount of security metrics coming from government and other communities make it very difficult to interpret and properly comprehend how to properly measure CSIR capabilities. The lack of a governing body or collaboration between security metrics within the federal space also makes it almost impossible to come to a conclusion. Furthermore, determining which security metric is appropriate and which to use over another can be frustrating. Without a consensus and with requirements and directives mandating greater security controls and greater accountability, organizations are up in arms when creating their own metrics for their own auditing purposes. Along with the chaos of trying to constantly anticipate audits

and reviews for specific requirements, there is a need for a structured metrics framework to help organizations achieve their objectives.

In order to measure the effectiveness and efficiency of incident management we must have at least a basis of understanding of the metrics that measure the effectiveness and efficiency of our organization's major processes. Incident management is a means to an end for an organization. However, it is not the end state of the organization. It is an end state objective. Therefore, when dealing with efficiency and effectiveness of incident management, the security metric must relate back to the overall organizational objective. This metrics framework attempts to address the confusion behind security metrics to provide a holistic view that aids organizations to better utilize security metrics, improve processes for incident reporting, and strengthen the organization's overall security posture.

#### Scope of the Project

The scope of this project is to develop a metrics framework for use in measuring CSIRT performance. This project specifically targets program manager's measuring CSIR program performance. The requirements for timeframe

reporting by US-CERT are applied throughout this metrics framework for CSIR and are used in Chapter Five Application of the Metrics Framework.

### Significance of the Project

The significance of this project is to assist in real world problems such as, passing FISMA audits, achieving plan of actions and milestones (POA&Ms), and informing management of the value from having CSIR capabilities. Using the developed metrics framework and accompanying metric form, performance measurement for CSIR can be better structured to inform upper management on current CSIR capabilities, areas of CSIR that are doing well, and areas of CSIR that need improvement. With this developed metrics framework, managers can understand what they are measuring, why they are measuring, and how they can go about measuring. This will enable management to make better, more informed decisions in regards to continuous improvement for CSIR and tie security metrics to support the agency's mission.

### Assumptions

The following assumptions were made regarding this project:

1. The agency is bound by the Federal Information Security Management Act of 2002 (H.R. 2458-56), Office of Management and Budget directives (OMB Circular No. A-130, Appendix III), and US-CERT Government reporting requirements (US-CERT, 2011)
2. The agency has computer security incident response capabilities
3. The agency is capturing CSIR data and has a collection of incident reports
4. The agency is using this metrics framework for CSIR to measure CSIR performance and capabilities

#### Limitations

During the development of this project, a number of limitations were noted. These limitations are as shown:

1. Some formulas apply specifically to Federal Government reporting requirements
2. The metrics framework is specific to measuring performance for computer security incident response capabilities
3. Accurately measuring cost will depend on the amount of information known for assigned costs

and the amount of time and effort an organization wishes to consume in order to achieve greater accuracy.

#### Definition of Terms

The following terms are defined as they apply to this project.

Computer Security Incident Response Team: "an organization or team that provides services and support to a defined constituency for preventing, handling, and responding to computer security incidents" (Alberts, Dorofee, Killcrece, Ruefle, & Zajicek, 2004, p. 1).

Framework: "an essential supporting or underlying structure" (Soanes & Stevenson, 2008, para. 13)

Incident: "any event that takes place through, on, or constituting information technology resources that requires a staff member or administrator to investigate and/or take action to reestablish, maintain, or protect the resources, services, or data of the community or individual members of the community" (Rezmierski, Deering, Fazio, & Ziobro, 1998, p. 14).

Measurement: "single-point-in-time views of specific, discrete, factors" (Payne, 2006, p. 1).

Metric: "generated from analysis; derived by comparing to a predetermined baseline two or more measurements taken over time" (Payne, 2006, p. 1).

Triage: "The process of receiving, initial sorting, and prioritizing of information to facilitate its appropriate handling" (West-Brown, Stikvoort, Kossakowski, Killcrece, Ruefle, & Zajicek, 2003, p. 191).

Personally Identifiable Information (PII): "any information about an individual that is maintained by an agency, including information that can be used to distinguish or trace an individual's identity, such as name, Social Security number, date and place of birth, mother's maiden name, biometric records, and any other personally information that is linked or linkable to an individual" (General Accountability Office, 2008, p. 5).

### Organization of the Project

This project is divided into six chapters. Chapter One provides the introduction, purpose, problem background, context of the problem, scope of the project, significance of the project, project limitations, and definition of terms. Chapter Two comprises of a literature



review on relevant works pertaining to the metrics framework for CSIR. Chapter Three documents the steps involved in developing the project including funding, coursework, work experience, and literature research. Chapter Four presents the metrics framework for CSIR and the measurement form for middle management to measure CSIR performance. Chapter Five provides an illustration for use of the metrics framework and measurement form. Chapter Six presents the conclusion and recommendations drawn from the development of this project. The appendices and references follow Chapter Six. The Appendices for the project consists of: Appendix A US-Cert Reporting Criteria; Appendix B Formulas For Computer Security Incident Response; Appendix C Acronyms.

## CHAPTER TWO

### REVIEW OF THE LITERATURE

#### Introduction

Since the early 1990s, from the Defense Advanced Research Project Agency's (DARPA's) push for CERT/CC to the establishment of US-CERT by DHS, the federal government has initiated multiple efforts for cyber security and CSIR (Ellis, Fisher, Longstaff, Pesante, & Pethia, 1997; White House, 2009; & Wilshusen, 2011). The efforts for accountability have been established under FISMA (H.R. 2458-56), OMB directives (OMB Circular No. A-130, Appendix III), and IG audits (Department of Homeland Security, 2010). However, the effectiveness for measuring performance and compliance still remains a controversy (General Accountability Office, 2010; Hopkins, 2009). Audits have continually evolved from yes and no questions to how many and why (Gorsen, Personal Communication, 2010). Efforts to effectively account for programs such as CSIR have become an area of concern.

This review of the literature on security metrics for CSIR focuses on the following questions:

- 1) How can computer security incident Response be measured?

- 2) What types of security measurements exist for computer security incident response?

#### Measurement Types for Computer Security Incident Response

There is a wide variety of reputable publications illustrating measurement types and metrics for CSIR. In the NIST Special Publication 800-55 Revision 1, Chew, Swanson, Stine, Bartol, Brown, and Robinson (2008) define measurement types for information security as implementation, effectiveness/efficiency, and impact. The authors establish that these are measurement types but they are actually purposes, the drive for measuring information security. In another NIST publication, NIST Special Publication 800-61 Revision 1, Scarfone, Grance, and Masone (2008) suggest possible metrics for CSIR as the number of incidents handled, time per incident, objective assessment of each incident, and subjective assessment of each incident. These metrics are very practical but suggest only a small portion of possible metrics and measurement types for measuring CSIR. In another technical report from Carnegie Mellon's Software Engineering Institute (SEI), Dorofee, Killcrece, Ruefle, Zajicek (2007), measures incident management based on common functions and processes within CSIR work flow. Their

approach to measure CSIR capabilities, also stated as incident management capabilities, is based on evaluating business functions. This form of measuring CSIR looks primarily at overall performance, while attempting to apply its own scoring rubric to business functions within CSIR. An additional measurement type or scale is defined by Allen & Davis (2010) as nominal, ordinal, interval, and ratio. These are specific measurement types based on possible mathematic operations and measurable service types for CSIR. Lastly, another insight into the types of measurements for CSIR is suggested by Gartner Analyst and metrics expert Jeffrey Wheatman (2010) as cost, time, and quality for any metric. Wheatman's statement of cost, time, and quality for metrics is based on common sense and practical knowledge. Compared to the various types of measurement or metrics suggested from other authors, Wheatman's approach to measurement types of security metrics in CSIR is holistic because it provides the flexibility to measure for any purpose or objective.

#### Three Types of Measurements: Cost, Time, and Quality

Measurements of cost, time, and quality are evident in business as the 'iron triangle', but the terms are used in a different context for this metrics framework for

CSIR. Atkinson (1999) reviews the measurements of cost, time, and quality as it pertains to project management. The tradeoffs that exist within a project are similar to a cost benefit analysis that is useful to project management. However, for this metrics framework for CSIR, Wheatman's (2010) basic concept of cost, time, and quality is used for the three measurement types. Allen and Davis (2010), in a technical report agree with the definition of cost as a value of money. The evaluation of cost is taken in a literal sense as encompassing only financial value, meaning dollars and cents. Scarfone, Grance, and Masone (2008) refer to time as the time an incident occurs to the time it is resolved. The importance of time as a measurement is referenced to timeframe or duration of an incident. As for quality, West-Brown, Stikvoort, Kossakowski, Killcrece, Ruefle, Zajicek (2003) identify quality as quality parameters that are common between services or functions. Quality is defined as good or bad based on how well the expectation level and set parameters are met. The three types of measurements for CSIR exist throughout aspects of publications regarding CSIR.

## Security Metrics

There are numerous publications for security metrics, but there is not one governing source that combines the efforts of creating security metrics. Chew, Swanson, Stine, Bartol, Brown, and Robinson (2008) provide a guide for creating measurement for information security programs. They provide a comprehensive guide that is very useful for measuring information security. Additionally, the Center for Internet Security Community (2010) has derived 28 metric definitions that apply broadly to 7 information security programs such as, incident management, vulnerability management, patch management, application security, configuration management, and financial metrics. They emphasize providing common metrics and definitions that support measurement of important business functions. In addition, Jansen (2009) indicates the direction of security metrics research going towards formal models and security measurement and metrics, historical data collection and analysis, artificial intelligence assessment techniques, practical concrete measurement methods, and intrinsically measurable components. Security metrics is on the path stated by Jansen and evidence of more practical and formal models are demonstrated by the effort of this project.

## Objective Driven Measurements

The purpose of a measurement is to serve a particular objective. Chew, Swanson, Stine, Bartol, Brown, and Robinson (2008) state that organizations should define the scope of their information security measurement program based off strategic goals and objectives among other things. In an interview with Barbara Gorsen (2010), Gorsen states that objectives need to be clearly defined before pursuing measurements within CSIR. Allen and Davis (2010) identify the importance of establishing objectives as a basis for measurements. Measurements, therefore, are derived from objectives to validate the reason for assessment. Lastly, in the Security Measurement and Analysis Project by Carnegie Mellon's SEI, Alberts, Allen, and Stoddard (2011) discuss mission-objective-driver protocols that drive analysis. This metrics framework clearly identifies objectives as an essential criterion to the development of measurements and to drive the basis for evaluation.

## Process Flow Identification

Identifying incident response capabilities process flow provides a map of how an incident is handled from start to finish. In a technical report from Carnegie

Mellon's SEI, Alberts, Dorofee, Killcrece, Ruefle, and Zajicek (2004) define incident management processes for CSIRTs using a process model. The process model for incident management outlines and documents process activities to aid in benchmarking. The common processes for evaluation are stated as: "Prepare/Sustain/Improve (Prepare), Protect Infrastructure (Protect), Detect Events (Detect), Triage Events (Triage), and Respond" (Alberts, Dorofee, Killcrece, Ruefle, & Zajicek, 2004, p. 8). Additionally, recommendations for creating a CSIRT by Scarfone, Grance, and Masone (2009) address the need for developing incident response procedures that cover all the phases of the incident response process. There is a direct correlation between understanding and documenting processes and benefiting from it when measuring CSIR capabilities. Chew, Swanson, Stine, Bartol, Brown, and Robinson (2008) state that developing performance measures in advance during the creation of a security program allows for the benefit and ease of security metrics. Understanding the processes for improvement is again stated by Dorofee, Killcrece, Ruefle, and Zajicek (2007) as essential for metrics evaluating incident management capabilities. Identifying and being aware of processes



enables for more accurate measurements and offers process improvement opportunities.

#### Audience Based Metrics

The notion of audience based measurements derives from professional experience, personal communication, and from the idea that different perspectives exist. Gartner analyst Michael Smith (2010) discussed the importance of understanding the audience and their expectations, and their needs associated with their position as a stakeholder within CSIR. Additionally, Niven (2008) addresses the four perspectives that exist for a balanced scorecard. This includes the customer perspective, internal process perspective, financial perspective, and employee learning and growth perspective. The concept of different views as a basis for metric requirements was essential in the development of audience based metrics.

#### Tying Security Metrics to Organization's Mission

Chew, Swanson, Stine, Bartol, Brown, and Robinson (2008) state that federal agencies need to link information security with enterprise strategic planning. West-Brown, Stikvoort, Kossakowski, Killcrece, Ruefle, and Zajicek (2003) also state that CSIRTs mission must complement the organization's mission. The point of

information security efforts is to support the agency's overall goals and objectives. Additionally, in an interview with Gartner Analyst Michael Smith (2010), Smith noted that the point of CSIR is to assist in the agency's mission. Therefore, measuring CSIR should follow suit by looking at ways to improve CSIR capabilities to support the agency's mission. Tying security metrics to the organization's mission is vital to the success of security metrics for CSIR.

#### Summary

The literature important to the project was presented in Chapter Two. The analysis of the above literature was essential in establishing a foundation of past and current literature relevant to CSIR. In addition, the literatures most relevant to the components of the metrics framework for CSIR were reviewed. From these literatures the metrics framework moves forward in an effort to support collaboration and practical security metrics for CSIR.

## CHAPTER THREE

### FORMATION OF THE PROJECT

#### Introduction

In order to bring value to this metrics framework for CSIR, it was important to incorporate higher level education, work experience, and literature research regarding current initiatives and best practices for CSIR. The formation of this project involved gaining the knowledge and experience necessary to fully comprehend what is needed for security metrics in CSIR. In order to make this possible I pursued an intensive course at Carnegie Mellon, a 10 week internship under the program of incident management, and conducted an in-depth research and analysis for existing documentation relevant to CSIR best practices.

The knowledge gained from this project was attained through the following activities:

#### Coursework

Coursework: Software Engineering Institute by Carnegie Mellon - Fundamentals of Incident Response Handling (5 days intensive course - Arlington, Virginia)

Description: "The course is designed to provide insight into the work that an incident handler may

perform. It provided an overview of the incident handling arena, including CSIRT services, intruder threats, and the nature of incident response activities" (Software Engineering Institute, 2011, para. 2).

### Internship

Information Security Office, CSUSB: Practical experience with vulnerability assessments using Nessus and the intrusion detection system using Snort. Internship offered hands on experience dealing with incidents from internal controls within a university setting (2 years part-time - San Bernardino, California).

Incident Management, Cyber Security Division, Department of Treasury: Discussion with System One (Contractor) Senior Analyst, Barbara Gorsen, and Gartner Analyst, Michael Smith, on metrics framework for CSIR. Additionally, I conducted an internal analysis on incident reporting.<sup>2</sup> I also assisted with preparations for FISMA and inspector general (IG) audits under the sections related to incident management (10 weeks Full-time - Washington, District of Columbia).

---

<sup>2</sup> Sensitive But Unclassified: details unavailable for disclosure.

The education and internship experiences were necessary to give me a solid foundation into CSIR and how analysis on CSIR capabilities really worked. From that point I analyzed the existing literature to extract the best practices and create a clear, more practical framework for measuring CSIR.

#### Literature Research

The literature research conducted for this project involved analysis of originating documentation for CSIR to current best practices used in the field. Thanks to the coursework and internships, I received direction from professionals in the field, enabling me to start my literature research on target.

The original documentation for CSIR starts with Carnegie Mellon's Computer Emergency Response Team/Coordination Center's (CERT CC) Handbook for Computer Security Incident Response Teams. The best practices and governing literature on CSIR exists in NIST Special Publication 800-55 and 800-61, Carnegie Mellon's Software Engineering Institute publications and the Center for Internet Security's Security Metrics V.1.1.0. The literature research tries to encompass past and present documentation relevant to the field of CSIR.

## Summary

For the benefit of this project's metrics framework for CSIR, the full scope of education, work experience, and literature research was undertaken. The formation of the project was to understand the essential literatures and real work experiences that are needed to measure CSIR capabilities. In order to make a practical yet effective metrics framework for CSIR, acquiring the knowledge, skills, and experience were the foundation for the formation of this project.

CHAPTER FOUR

METRICS FRAMEWORK FOR COMPUTER  
SECURITY INCIDENT RESPONSE

Introduction

Metrics framework for CSIR, for the context of this project, is a basis for measuring the performance of a CSIR program. The framework comes from the construct of the different measurement types and the essential elements needed to determine, select, and execute a particular measurement within CSIR. The five elements that are critical to the metrics framework for CSIR include:

- 1) understanding the three types of measures,
- 2) establishing objective driven metrics, 3) produce measurements and results based on audience considerations,
- 4) tie incident response (IR) evaluations to improve IR capabilities that support the organization's mission, and
- 5) process flow identification for CSIR.

The purpose of the metrics framework is to provide a practical guide that enables CSIR stakeholders to measure IR performance and improve IR capabilities. The following sections will go into detail on the major aspects of the metrics framework for CSIR and provide a holistic yet practical approach for

evaluating IR. (See Figure 1. Metrics Framework for Computer Security Incident Response, Below)

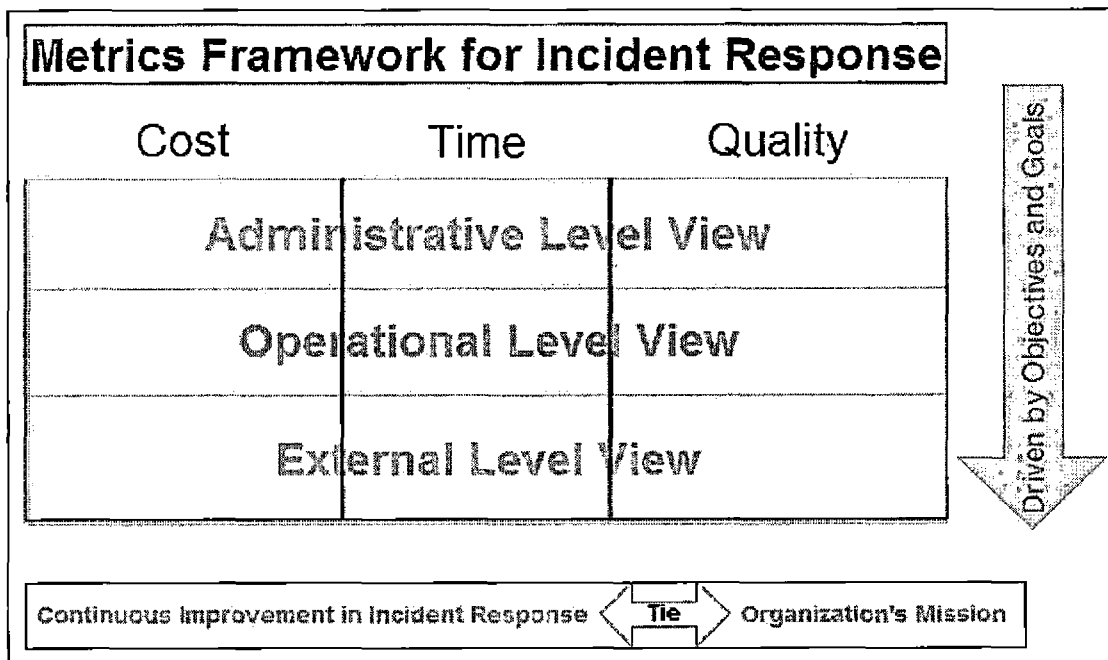


Figure 1. Metrics Framework for Incident Response

#### Steps to Use the Metrics Framework

Before using the metrics framework one needs to have an understanding of one's agency's CSIR capabilities, its maturity level, and what types of measurements exist for evaluating CSIR. The first step is to determine what is the objective and purpose for measuring CSIR capabilities. The second step is to select what measurement to use based off the determination of the objective and purpose. The third step requires the identification of all data sources



and responsible parties. Then the measurement is conducted with the appropriate approval from management. The fourth step is to tailor the results specific to the needs of the audience base, giving consideration to viewing requirements. The fifth step is to assess the results and determine if action is needed. The sixth step is to take action, if needed, and review all previous steps that have been taken.

#### Three Types of Measures for Computer Security Incident Response

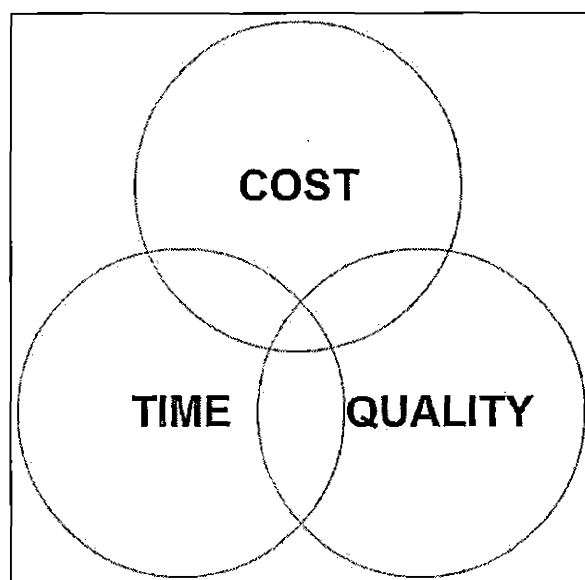


Figure 2. Three Measurement Types for Incident Response

Three types of measures that exist for evaluating IR include cost, time, and quality (See Figure 2. Three Measurement Types for Incident Response, Above) (Wheatman,

Personal Communication, August 2010). These three measures provide a holistic approach towards evaluating efficiency, effectiveness, and implementation in an IR program. When evaluating incident reports, these three measures can overlap by comprising a mixture of two or three measures. For example, when using the metrics framework to evaluate compliance for timeframe reporting the result may require management to consider implementing changes that impact the cost of the IR program. The cost benefit analysis for decreasing reporting time to meet timeframe requirements is a measurement of quality. This involves all three measurement types to address compliance. Depending on the purpose for measuring IR, these three measurement types will be the foundation to evaluate and measure a CSIR program.

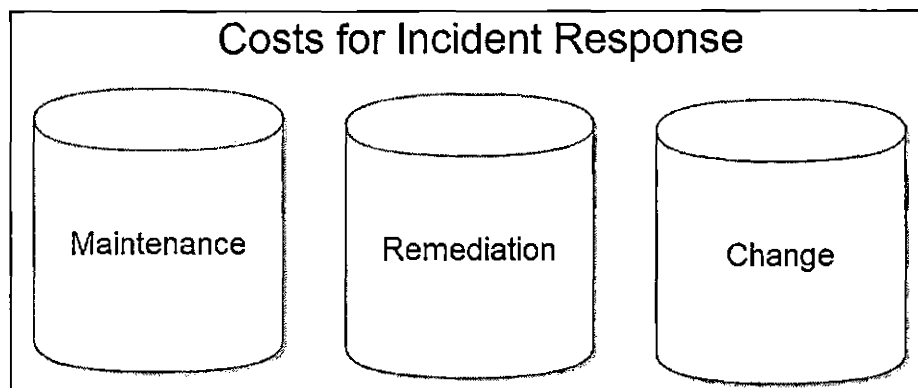


Figure 3. Cost Types for Incident Response

Cost in CSIR is determined based on three areas:

1) the cost to maintain IR capabilities, 2) the cost to remediate an incident, and 3) the cost to implement change in an IR program (Rezmierski, Deering, Fazio, & Ziobro, 1998; Torner, Personal Communication, February 2011) (See Figure 3. Cost Types for Incident Response, Above). Please note that cost for this metrics framework deals only with financial cost. There are existing formulas (See Appendix B) that aid in evaluating IR and offer standardized expressions to make IR evaluations more consistent. When evaluating costs for IR, the more entities that are identified and assigned costs, the more accurate the cost measurement will be. For tangible items, cost is easier to assign. But for intangibles such as reputation and trust it becomes much harder to assign a dollar amount. The criteria for evaluating cost for IR requires identification of the three cost areas and the ability to continually assign related costs as new costs are identified.

The cost to maintain CSIR capabilities and services include direct and indirect costs that can be attributed to CSIR operational costs. From an accounting perspective the cost of direct labor, direct material, and applied overhead costs should be considered (Brewer, Garrison, &

Noreen, 2009). Activity based costing method for calculation is suggested. However, the trade-off to more accurately assigned activity costs is the time and money needed to discover the cost of each activity. The best way to determine cost to maintain CSIR is to evaluate ones need to measure and how much one is willing to pay in order to obtain accurate cost estimates.

The cost to remediate varies depending upon the incident and the methods chosen to remediate. But for this metrics framework it is important to find common incidents that have relatively similar financial costs. Although costs will vary, it is crucial that all methods of remediation attribute a financial cost when applicable. As noted before, intangibles like trust and reputation do not always have an associated financial cost. Therefore, it is important to look at costs for either costs savings or improvement in remediation efforts.

Implementation costs are financial costs attributed from the impact of making change to CSIR capabilities. The cost to implement change is reliant on both the cost to maintain services and the cost to remediate. A cost benefit analysis approach is recommended for determining implementation costs (Xie & Mead, 2004). The importance of implementation costs are determining whether or not making

change is worth the financial costs, given the desired outcome and the likelihood it would occur.

The importance of measuring time for CSIR is the duration between activities and the total time it takes to resolve an incident. This deals with points of time and the lengths of time in between points. In particular there can be two or more points that exist within a CSIR event. The three points of time for an incident include: 1) Start Time, 2) the Time-in-Between, and 3) the Finish Time (See Figure 4. Time Measurement Points for Incident Response, Below).

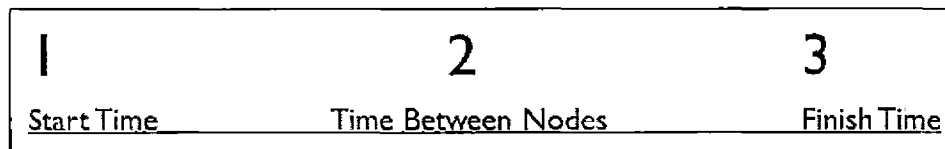


Figure 4. Time Measurement Points for Incident Response

Start Time usually is the time the incident is reported. It is the first recorded and realized moment that an incident has occurred. This statement for start time is probably the most important aspect of measuring time for CSIR because of the discrepancies that exist within a FISMA or IG audits. As shown in Chapter One, the timeframe reporting requirements US-CERT states broad to strict reporting times depending on the different incident

categories. Therefore, it only makes sense that the time to report only starts when an incident is reported and is realized, meaning the first time it is reported at the level being considered.

Time-in-Between deals with the many nodes an incident goes through as it is resolved by one or many entities. The finish time can either be the time the incident is reported as resolved or the time the incident report is closed out. The structure for measuring time depends on how an agency keeps its timestamps and what aspect of time it is trying to evaluate. Time in the sense of IR is all about how long. Determining how long offers the ability to gauge performance. It allows agencies to determine if changes are needed and how changes can affect time.

Quality is self-determined that can be subjective or objective or both depending on the measurement conditions (Scarfone, Grance, & Masone, 2008, p. 3-25). An organization is able to interpret the results of an IR measurement and gauge whether the results are good or bad. Statistics such as counts for incidents initiated, unresolved, or resolved are interpreted based on the priority and values of the organization. A high number of reported incidents may be seen as a good thing because it shows that people are reporting incidents as they occur.

However it could also mean the agency's security controls are not doing their job. Or, adversely, a low incident count could reflect that security controls are working and there are a less number of incidents occurring. However, this could just as well be the agency not reporting because of fear of showing that too many incidents are occurring. Depending on the agency's priorities and goals, any particular moment can drastically effect the interpretation of IR results and the value that exists in that information. Quality is thus self-determined and put into the interpretation of the agency based on where they find value in the information.

### Objective Driven Measurements

It is important to establish the objective for maintaining a metric before introducing IR evaluations to an audience. This allows the audience to relate how measuring performance of an IR program supports the organization's mission. As identified in NIST Special Publication 800-55, security metrics must be driven by goals and objectives (Chew, Swanson, Stine, Bartol, Brown, & Robinson, 2008). The audience must understand the objectives for an IR metric in advance to understand why

measurement of a CSIR is being conducted (Alberts, Allen, & Stoddard, 2011).

This component of the metrics framework is essential in the determination, selection, and presentation for measuring CSIR capabilities. Determining objective(s) is the first step before selecting security measurements for a CSIR program. A crucial part of determining objectives for security measurements is to evaluate organizational needs and the mission of the organization.

By deriving security measurements from objectives and goals, the results from the metric can be meaningful. Objective driven metrics enable the entity that is conducting the measurement to bring value to the organization using the results from the metric evaluation. Clearly stating the objective and goal of the measurement before selecting what to measure offers guidance into what should be measured and explains to the audience why it is being measured in the first place. Therefore, objective driven measurements are essential to the success of conducting security metrics for a CSIR program and gives consideration to organizational measurement concerns.



## Audience Based Measurements

Cost	Time	Quality	
			<b>Administrative View</b>
			<b>Operational View</b>
			<b>External View</b>

Figure 5. Audience Based Measurements

As shown in Figure 5. Audience Based Measurements above, there are three identified audience groups for the intended user of the metrics framework: 1) administrative, 2) operational, and 3) external. Since the intended user is middle management, the audience meant for the security measurement of a CSIR involves upper management, CSIRT staff, and auditors. Each audience groups have their own specific needs. Although their needs may overlap, their purpose for viewing the results of a security metric for CSIR and expectations of the presented information is quite different.

The administrative level view is based on middle to executive level management. Stakeholders at the

administrative level view may include the Chief Information Officer, Chief Financial Officer, Chief Technology Officer, Chief Information Security Officers (CISOs), Associate CISOs, and Directors of bureau CSIRTs. These positions within an agency have relatively large amounts of responsibility for the agency and high level decision making powers, therefore, this group may only be interested in high level information and may want everything synthesized for the purpose of making high level decisions.

The operational level view includes those who are on the front lines dealing with the incident. It includes the technical staff that may want the detailed information to find problems within the CSIR processes. Stakeholders at the operational level view includes CSIRT Managers, CSIRT Analysts, CSIRT Operators, and all other CSIRT personnel that have direct contact with the CSIR processes at the bureau level. It is important to understand the role of stakeholders at the operational level because it offers insight into the expectation of security metrics and metric results. Stakeholders at the operational level may be interested in the cost and or time to respond to an incident within the bureau CSIRT.

The external level view is for auditors, those outside the CSIR program that need an assessment into measuring CSIR performance. Stakeholders at the external level view include FISMA auditors by DHS, IG auditors, and all other entities looking at the performance measure of CSIR capabilities from outside the agency. This may include the IG of an agency which would technically be inside the agency, but because of their role they are considered at the external level view. The importance of grouping this type of audience into the external level view is because their needs are specific to check for compliance against some specific standard, regulation, or mandate.

Understanding that the audience does matter and giving them consideration for the selection of security metrics for CSIR is important to the success of conducting any security metric. This is a critical aspect of the metrics framework because it offers the ability to identify measurements based on audience needs. Therefore, all of these views are important for selecting security metrics for CSIR and tailoring relevant IR metric results to the intended audience.

## Tying Measurements to the Agency's Mission

Tying security measurements and its results to the agency's mission is a crucial segment for the metrics framework. This makes sure that measuring CSIR is not just for the sake of measurements. The reason CSIR exists is to benefit the agency's mission. This could mean passing an audit so the organization is able to continue its normal operations or responding to a reported incident that saves the agency time and money. Therefore, the importance of measuring CSIR is to prove that it supports and enables the agency to accomplish its mission. By describing in words how the measurement ties into the agency's mission, we can demonstrate the value within the CSIR program.

In order to tie the security measurement to the agency's mission, the purpose and objective needs to drive the actual security metric from the beginning. If done properly, the objective and purpose that drives the security measurement for CSIR will be restated and will serve as the bridge to demonstrate how the CSIR program supports the agency's mission. An example of this could result in stating that the measurement is part of a series of measurements that is helping the organization prepare for an audit. Any objective can be stated as long as it supports the agency's mission. But it is still important

to make the tie on how the CSIR metric results support the mission so that the agency as a whole can understand the value behind CSIR capabilities.

#### Process Flow Identification

Process flow identification involves identifying the processes within CSIR capabilities. For a bureau, the process flow starts from the incident being reported/detected, to triaging, to remediating, to sustaining, and at some point reporting to the agency headquarters CSIRT. For an agency it is similar, except the agency reports to US-CERT. Depending on the makeup of the organization the process for notification and remediation will vary. Please see Figure 6. Bureau Level Process Flow and Figure 7. Agency Level Process Flow below for an illustration of Bureau Level and Agency Headquarters Level process flows for incident reporting.

As shown in Figure 6. Bureau Level Process Flow and Figure 7. Agency Level Process Flow below, the figures illustrate the processes and functions within a CSIR capability. They show the methods of communication such as phone, email, and web portal. The importance to note is that at the federal government level, depending on the CSIRTs position within an agency their process and makeup

will vary. Notably the accuracy and greater capabilities in a CSIR program will depend on the maturity level of the CSIRTs.

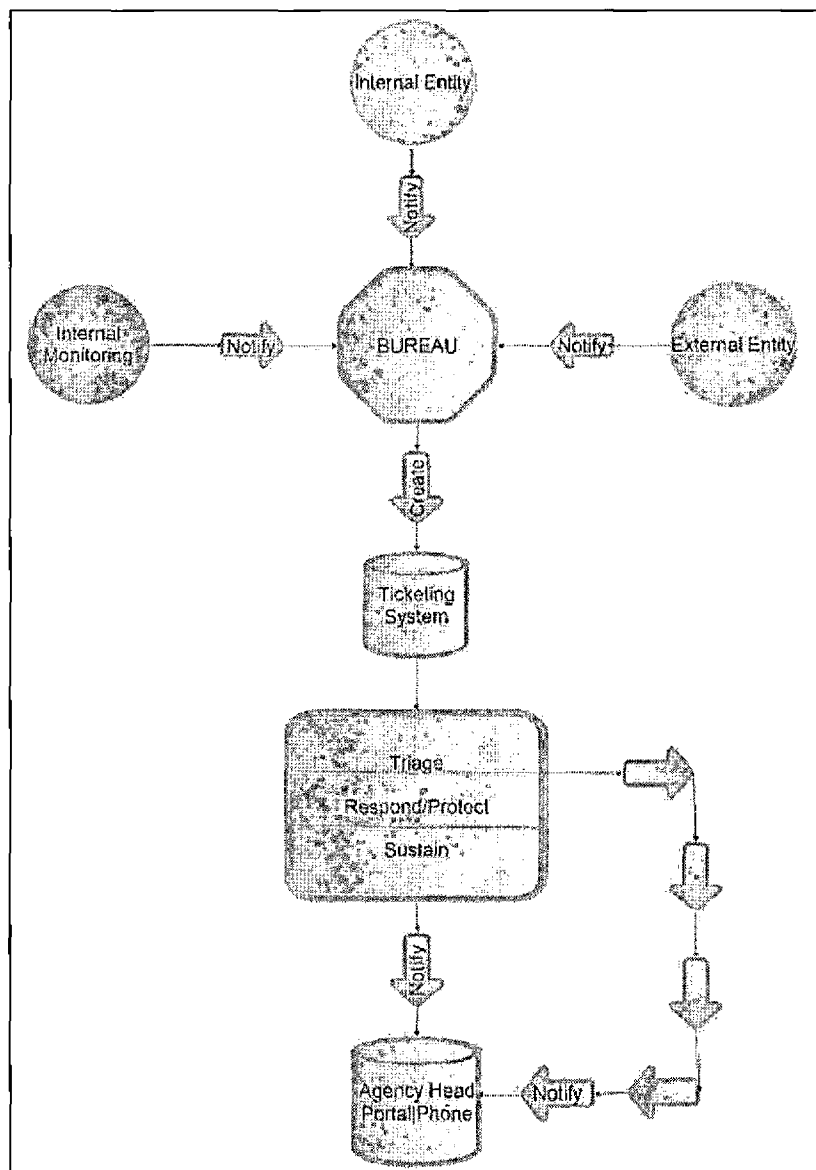


Figure 6. Bureau Level Process Flow

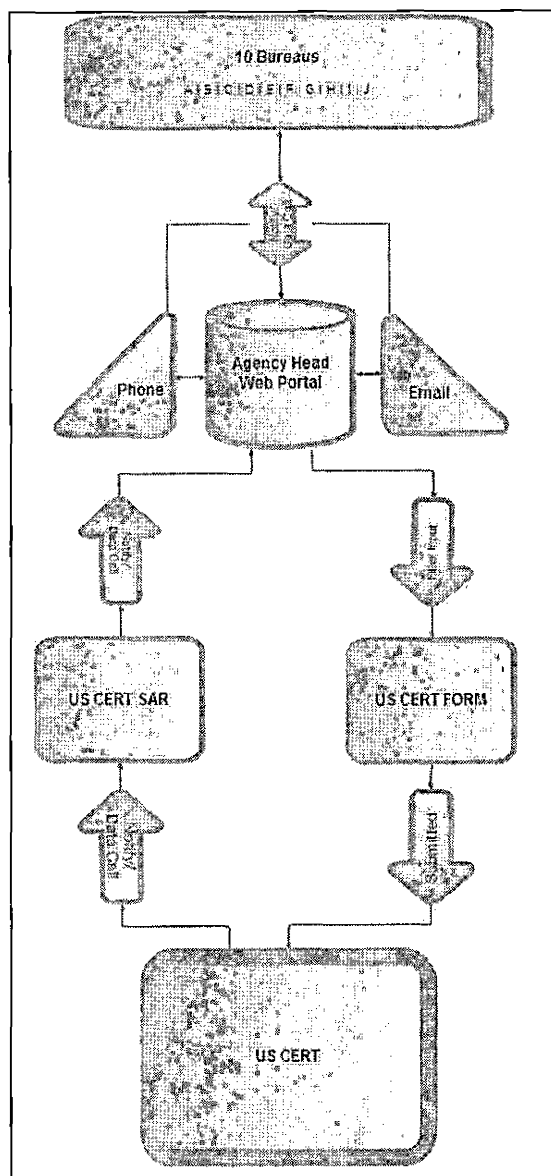


Figure 7. Agency Level Process Flow

In order to identify the process flow for CSIR capabilities it is important to identify information assets and stakeholders within a CSIRT. Aside from looking at an inventory list it is best to look at policies and guides produced by CSIRTs. Usually the policies will

outline current capabilities and processes with a bureau's CSIRT. However, not all organizations follow their existing policies and guides. It is therefore best to verify known process flows. A great way to determine process flows is through discussion with CSIRTs and directors of CSIRTs. This can serve to be invaluable in identifying process flows for CSIR capabilities.

Over time the amount of known processes and entities involved with CSIR capabilities will accumulate. With more accurate information process flow, identification can help determine the cost and time allotted to each entity within CSIR capabilities. Therefore, process flow identification is crucial to security metrics and offers an illustrated approach towards understanding an organization's CSIR capabilities.

#### Measurement Form for Computer Security Incident Response

The Incident Response Measurement Form I've created draws from NIST Special Publication 800-55 Measure 10 and CIS Security Metrics v1.1.0 (See Figure 8. Incident Response Measurement Form Part 1, Below). The names and definitions for each section differ from existing documentation so please be sure to read the descriptions below.



<b>Incident Response Measurement Form</b>		Date: 2011 April, 05 - Tuesday
		Author: Name
<b>Metric ID</b>	<i>Incident Response Metric Name</i>	
<b>Purpose &amp; Objective</b>	<i>Description</i>	
<b>Measure Type</b>	<i>Check all that apply:</i> <input type="checkbox"/> Cost <input type="checkbox"/> Time <input type="checkbox"/> Quality	
<b>Formula</b>		
<b>Description</b>	<i>Measurement/Formula Description</i>	
<b>Data Source(s)</b>		
<b>Responsible Parties</b>		
<b>Audience</b> <i>Check all that apply:</i>	<input type="checkbox"/> Administrative <input type="checkbox"/> Operational <input type="checkbox"/> External <input type="checkbox"/> Other: _____	
<b>Frequency</b>	<input type="checkbox"/> Annual <input type="checkbox"/> Monthly <input type="checkbox"/> Weekly <input type="checkbox"/> Daily <input type="checkbox"/> Other: _____	
<b>Tie to Agency Mission</b>		
<b>Comments:</b>           		
All Copyrights Reserved © 2011 Vincent Sritapan		

Figure 8. Incident Response Measurement Form Part 1

"Metric ID" is a number and/or letter that is assigned by the person conducting the measurement. Following the Metric ID is the metric name, also given by the person conducting the measure.

"Purpose & Objective" is the section where the purpose and objective of the measurement is stated. This is stated before the actual measurement formula and is essential to creating a meaningful measurement.

"Measurement Type" is a section with three check boxes that allows the user of the form to choose which of the three types of measures are being conducted. Please note that the measurement can involve one to as many as three measurement types in the measurement form.

"Formula" is the section where the formula for the measurement can be outlined and detailed. This is a critical part of the measurement because it enables for others to understand how the measurement is being conducted. Using formulas enables others to repeat the measurement and use it for their own measurement purposes.

"Description" is the section that clarifies the meaning of the formula. If there are any exceptions, notations, etc. the author of the form can explain the formula in detail.

"Data Source(s)" is the section where assets containing or controlling sources of data for the measurement are identified. Depending on the agency this can involve one or many sources of data.

"Responsible Parties" is the section that identifies who is responsible for conducting and overseeing the measurement. This could involve technicians, analysts, and/or upper management.

"Audience" is a section that identifies the intended audience. This may comprise of one or multiple viewing audiences depending on the situation.

"Frequency" is the mode of measurement. It is a selection for periods of time for when the measurement is to be conducted or what points of time they wish to review.

"Tie to Agency Mission" is a section that tries to put into words how the measurement ties into the agency's mission.

"Comments" is a free section for the author/user to use this form and place any notes or comments necessary for the measurement. The Comment section is a space that is utilized at the user's discretion.

[illegible]

Figure 9. Incident Response Measurement Form Part 2

Another aspect for the measurement form is the revision control history form that is attached to each metric (See Figure 9. Incident Response Measurement Form Part 2, Above). The above form is intended for CSIRTs and

CSIR stakeholders to reuse the metric ID and formula. Aside from creating a practical and clear guide for security metrics regarding CSIR, this project also looks to promote collaborations supporting the archiving of security metrics.

### Summary

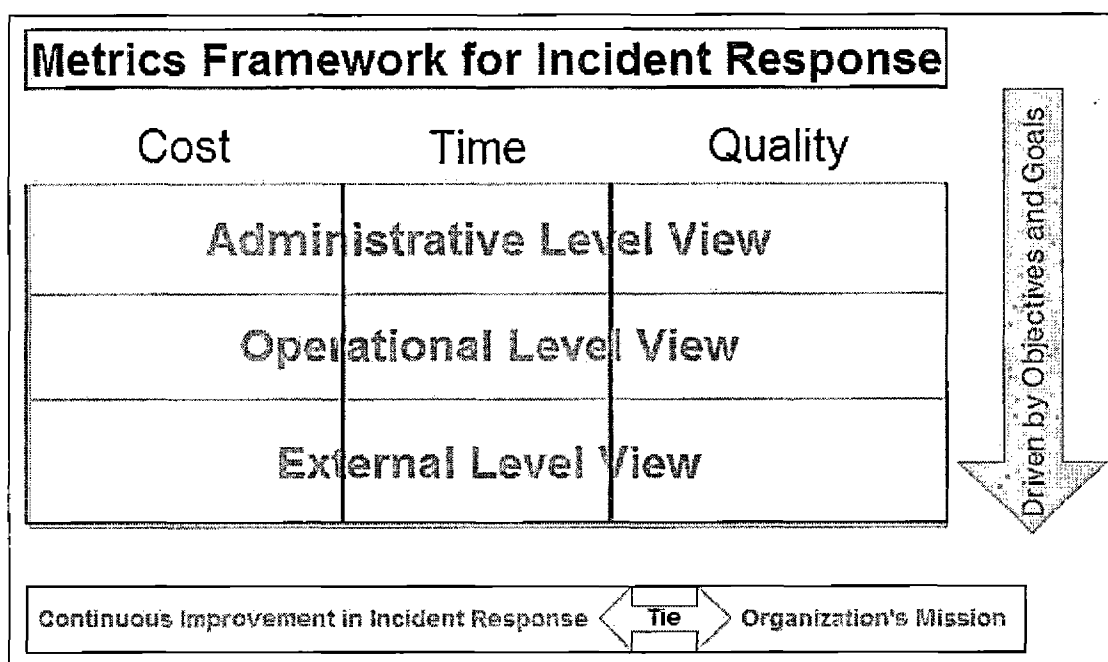


Figure 10. The Metrics Framework for Incident Response

As shown in Figure 10. The Metrics Framework for Incident Response, the metrics framework for CSIR includes three types of measurements for CSIR, cost, time, and quality. It identifies the need for objective driven measurements, the need to consider audience groups for

measurement evaluations and presenting results, the need to tying measurements to the agency's mission, and the importance of process flow identification. The metrics framework for CSIR is also accompanied by a measurement form for CSIR. The measurement form is specifically geared towards utilizing the framework and creating CSIR security metrics. Overall, the metrics framework for CSIR is a product of the education, work experience, and literature research conducted in search for a common platform for measuring CSIR capabilities.

## CHAPTER FIVE

### APPLICATION OF THE FRAMEWORK

#### Introduction

Chapter Five provides a fictitious scenario that uses the metrics framework for CSIR including the measurement form. The case scenario tries to illustrate usage of the different types of measurements that exists for this framework.

#### Case Scenario

In this scenario, an agency containing 10 bureaus is making preparations at the headquarter level for a FISMA audit under the program of incident management. One of the anticipated questions is the compliance for timeframe reporting. The samples of incidents for the 10 bureaus, Bureaus A through J, are shown in Table 1. Sample Incident Reports. For simplification only category 1, unauthorized access, 2, denial of service, and 3, malicious code, incidents were used in this case (See Appendix A United States Computer Emergency Readiness Team Reporting Criteria for incident categories). Note that federal agency must adhere to US-CERT timeframe reporting requirements (US-CERT, 2011).

The case scenario is an audit preparation that involves security measurements for timeframe reporting and it illustrate the use of the metrics framework for CSIR. Please refer to Appendix A for federal agency incident criteria and timeframe reporting requirements.

Before providing the sample data, it is important to understand that each CSIRT will have their own incident reports for measuring depending on their agency's CSIR capabilities. Some agencies may have more or less data points to measure depending on the maturity of their CSIR program. Also, as noted in the assumptions in Chapter One, the agency must have CSIR capabilities and must collect data points for measuring CSIR capabilities. The data points can usually be found at the CSIR Center or with the CSIRT. CSIRTs should have the necessary data specific to measuring timeframe reporting.

Before looking at the sample data Figure 10. Columns and Names for Sample Incident Reports describe each column respective to their column title. The format of the data for each column is shown in Figure 10. Columns and Names for Sample Incident Reports and described in the following paragraph.



Ticket No.	Bureau	Category	Subject	Occurred	Reported	Created	Submit US-CERT	Type	PII	Status
####	Letter	0-6	Text	YYYY.MM.D D.HH.MM.SS	YYYY.MM.DD HH.MM.SS	YYYY.MM.DD.H H.MM.SS	YYYY.MM.DD.HH. MM.SS	Cyber/ Equipment/ Physical	Yes/ No	Open/ Closed

Figure 11. Columns and Names for Sample Incident Reports

As shown in Figure 11. Columns and Names for Sample Incident Reports, "Ticket No." refers to the assigned number when an incident is reported to the agency headquarters level. "Bureau" letter is the bureau letter, similar to a bureau name that would represent the bureau. "Category" is the incident type as defined by US-CERT and NIST Special Publication 800-61. Notably, an incident can have more than one assigned category. "Subject" text is the subject name for the incident, which can also include a limited text description. "Occurred" is the estimated time of an incident occurrence. This can sometimes be exact if the data capture is electronic, but it is normally a perceived time that an individual determines. "Reported" is the time an incident is first reported at the bureau level. "Created" displays the time the incident is reported/submitted from the bureau CSIRT to the agency headquarter CSIRT. "Submit US-CERT" displays the time the incident is submitted from the agency headquarters CSIRT to US-CERT. Please note that the time is constructed with

the year, month, day, hour, minute, and second. "Type" is the type of incident in regards to a physical paper incident, equipment incident, or cyber incident. "PII" is the column that identifies if the incident involves personally identifiable information (PII). "Status" is in regards to whether an incident ticket no. is still open or if it has been closed.

#### Sample Data

According to the scenario, the sample incident reports came from the CSIRT at the agency headquarters level. The information from the sample incident reports is being used to measure performance on CSIR timeframe reporting. This is in preparation for the upcoming FISMA audit. The data set for this scenario can be found in Table 1. Sample Incident Reports below.

Table 1. Sample Incident Reports

Ticket No./		Category/	Subject	Occurred	Reported	Created	Submit US-CERT	Type	PII	Status
Bureau										
1	A	1	N/A	2011.01.01.14.00.00	2011.01.01.14.45.11	2011.01.01.15.05.15	2011.01.01.15.15.16	Cyber	Yes	Closed
2	B	2	N/A	2011.01.01.16.30.00	2011.01.02.08.45.45	2011.01.02.10.15.23	2011.01.02.10.25.24	Cyber	No	Closed
3	C	1	N/A	2011.01.01.18.00.00	2011.01.02.10.28.13	2011.01.02.11.08.14	2011.01.02.11.18.15	Phys	Yes	Closed
4	D	1	N/A	2011.01.02.08.15.00	2011.01.03.11.40.26	2011.01.03.11.55.27	2011.01.03.12.05.28	Cyber	Yes	Closed
5	E	3	N/A	2011.01.02.14.00.00	2011.01.03.14.45.27	2011.01.03.19.45.28	2011.01.03.19.54.29	Equip	No	Open
6	F	1	N/A	2011.01.03.12.00.00	2011.01.04.04.40.28	2011.01.04.05.33.29	2011.01.04.05.42.30	Phys	Yes	Closed
7	G	3	N/A	2011.01.05.04.45.00	2011.01.06.08.10.29	2011.01.06.16.10.30	2011.01.06.16.19.31	Cyber	No	Closed
8	H	1	N/A	2011.01.06.11.00.00	2011.01.08.14.22.30	2011.01.08.14.52.11	2011.01.08.15.01.12	Cyber	Yes	Closed
9	I	1	N/A	2011.01.06.14.30.00	2011.01.09.20.16.31	2011.01.10.20.16.32	2011.01.10.21.24.33	Equip	No	Open
10	J	1	N/A	2011.01.11.14.00.00	2011.01.12.14.12.12	2011.01.12.14.12.12	2011.01.12.14.20.13	Phys	Yes	Closed
11	A	2	N/A	2011.01.11.16.45.00	2011.01.18.07.40.31	2011.01.18.08.30.22	2011.01.18.08.38.23	Cyber	No	Closed
12	B	3	N/A	2011.02.01.11.15.00	2011.02.12.05.45.55	2011.02.14.11.45.56	2011.02.14.11.53.57	Phys	No	Closed
13	B	1	N/A	2011.02.07.08.15.00	2011.02.13.07.38.25	2011.02.13.08.28.00	2011.02.13.08.36.01	Equip	Yes	Open
14	C	3	N/A	2011.02.17.19.30.00	2011.02.19.17.20.36	2011.02.20.11.20.37	2011.02.20.11.30.38	Cyber	No	Closed
15	D	2	N/A	2011.02.11.07.00.00	2011.02.23.19.22.22	2011.02.23.20.12.23	2011.02.23.20.21.24	Phys	No	Closed
16	D	1	N/A	2011.02.21.12.00.00	2011.02.24.14.40.38	2011.02.24.20.20.19	2011.02.24.20.29.20	Cyber	Yes	Closed
17	E	1	N/A	2011.01.07.19.30.00	2011.02.24.18.49.26	2011.02.24.18.59.11	2011.02.24.19.08.12	Cyber	Yes	Closed
18	F	2	N/A	2011.01.16.18.15.00	2011.02.27.23.40.40	2011.02.28.08.05.41	2011.02.28.08.14.42	Phys	No	Closed
19	F	2	N/A	2011.03.01.05.45.00	2011.03.02.21.28.19	2011.03.03.11.28.20	2011.03.03.11.38.21	Phys	No	Closed
20	G	1	N/A	2011.01.21.04.45.00	2011.03.07.15.41.42	2011.03.07.16.11.43	2011.03.07.16.19.44	Cyber	Yes	Closed
21	H	2	N/A	2011.02.11.14.00.00	2011.03.10.19.10.33	2011.03.11.09.11.22	2011.03.11.09.20.23	Cyber	No	Closed
22	H	2	N/A	2011.01.09.22.15.00	2011.03.12.16.09.44	2011.03.12.17.09.45	2011.03.12.17.19.46	Cyber	No	Closed
23	I	1	N/A	2011.03.01.21.30.00	2011.03.15.19.33.52	2011.03.16.08.55.53	2011.03.16.10.03.54	Equip	Yes	Open
24	J	3	N/A	2011.02.11.09.45.00	2011.03.18.23.30.41	2011.03.18.23.30.41	2011.03.18.23.39.42	Cyber	No	Closed
25	J	1	N/A	2011.03.01.22.15.00	2011.03.19.09.43.37	2011.03.19.09.43.37	2011.03.19.09.52.38	Phys	Yes	Closed

## Metric Development

For the analysis of this case scenario, Metric ID 001, 002, and 003 were created (See Figure 12. Measurement Form for Metric ID 001, Figure 13. Measurement Form for Metric ID 002, Figure 14. Measurement Form for Metric ID 003, below). Metric ID 001 looks at the number of incidents for the agency based on incident categories 0 through 6. Metric ID 002 looks at the duration for each incident against the time required to report. Metric ID 003 looks at the percentage of incidents reported on time. The analysis identifies the current status of the CSIR capabilities as well as usage of the metrics framework.

## Step by Step Application

Using the metrics framework, the measurement form is applied for each metric developed. First, the objective and purpose is clearly stated. Second, the type of measurement is identified. Third, the formula and description is detailed. Fourth, the data sources and responsible parties are identified. Fifth, the audience group is selected. Sixth, the frequency of the sample or measurement is determined. Seventh, the statement for tying the measurement to the organization's mission is stated. Eighth, the comments are filled in. Then, after

the first metric is developed, more metrics may be developed if needed. Finally, the measurement is conducted and the results are analyzed. Depending on the findings, action may be taken to improve CSIR capabilities. In the case scenario each metric developed will be described, following this step by step application. The decisions to be made will be identified and resolution will be stated.

<b>Incident Response Measurement Form</b>		Date: 2011 April, 05 – Tuesday
		Author: Vincent Sritapan
MetricID001	Number of Incidents for Category0 – 6	
Purpose & Objective	Prepare for FISMA Audit Determine number of Incidents	
Measure Type	Check all that apply: <input type="checkbox"/> Cost <input type="checkbox"/> Time <input checked="" type="checkbox"/> Quality	
Formula	Incident Count by Category = Count (Category # Incidents) Total Incidents for Agency = $\sum$ Count (Category 0 - 6 Incidents)	
Description	Incident count by category is the number incidents separated by category type. Total Incidents for Agency includes all reported incidents for the Agency for a defined period of time.	
Data Source(s)	Agency CSIRC Bureau CSIRTs (A through J)	
Responsible Parties	Agency 1 Headquarters, Division 1 Program Manager: Name ABC Contract Analyst Group: Senior Analyst, Junior Analyst	
Audience Check all that apply:	<input checked="" type="checkbox"/> Administrative <input type="checkbox"/> Operational <input type="checkbox"/> External <input type="checkbox"/> Other: _____	
Frequency	<input type="checkbox"/> Annual <input type="checkbox"/> Monthly <input type="checkbox"/> Weekly <input type="checkbox"/> Daily <input checked="" type="checkbox"/> Other: <u>FISMA YEAR</u>	
Tie to Agency Mission	Helps organization understand the volume of incidents being reported Intended for FISMA Audit by DHS.	
<b>Comments:</b>  Step 1: Determine what incidents are being reported. Metric ID 001, 002, 003, 004 All grouped for FISMA Audit in Incident Management.		
All Copyrights Reserved © 2011 Vincent Sritapan		

Figure 12. Measurement Form for Metric ID 001

Metric ID 001 is shown in the Figure 11. Measurement Form for Metric ID 001 above and is a quality measurement

type that documents at incident counts by category and total incidents for the agency. The purpose and objective for the measurement is to prepare for the upcoming FISMA audit and determine the number of incidents that have occurred for the agency. The data source is the agency CSIR center (CSIRC) as well as the bureau CSIRT. The responsible parties include the agency program manager and the contracting team. The frequency is selected as "other" to include the FISMA year. This scenario is defined as January 1<sup>st</sup>, 2011 through May 1<sup>st</sup>, 2011. This metric is tied to the agency's mission since it helps determine the volume of incidents reported that are relevant for the FISMA audit. The comments section shows that this metric is the first step for preparing for the upcoming FISMA audit and that metric ID 002, 003, and 004 are all related.

<b>Incident Response Measurement Form</b>		Date: 2011 April, 05 - Tuesday
		Author: Vincent Sritapan
Metric ID 002	Duration for Category 0-6 Incidents	
Purpose & Objective	Preparations for FISMA Audits Determine if Agency 1 is compliant for reporting incidents	
Measure Type	Check all that apply: <input type="checkbox"/> Cost <input checked="" type="checkbox"/> Time <input type="checkbox"/> Quality	
Formula	Duration ( <i>Time Created to Time Submitted to US-CERT</i> ) less <i>Time Required</i>	
Description	Time Created is the first official notification time to Agency HQ Time Submitted to US-CERT is the end time for required timeframe reporting Time Required depends on Category 0-6 (Please see US-CERT.gov)	
Data Source(s)	Agency CSIRC Bureau CSIRTs (A through J)	
Responsible Parties	Agency 1 Headquarters, Division 1 Program Manager: Name ABC Contract Analyst Group: Senior Analyst, Junior Analyst	
Audience Check all that apply:	<input checked="" type="checkbox"/> Administrative <input type="checkbox"/> Operational <input checked="" type="checkbox"/> External <input type="checkbox"/> Other: _____	
Frequency	<input type="checkbox"/> Annual <input type="checkbox"/> Monthly <input type="checkbox"/> Weekly <input type="checkbox"/> Daily <input checked="" type="checkbox"/> Other: <u>FISMA YEAR</u>	
Tie to Agency Mission	Helps organization meet timeframe reporting compliance. Intended for FISMA Audit by DHS.	
<b>Comments:</b>  Step 2: Determine Duration of Incident Reports Metric ID 001, 002, 003, 004 All grouped for FISMA Audit in Incident Management.		
All Copyrights Reserved © 2011 Vincent Sritapan		

Figure 13. Measurement Form for Metric ID 002

Metric ID 002 is shown in Figure 13. Measurement Form for Metric ID 002 above is a time measurement type that



determines the duration of an incident and the time required to report. The purpose and objective for the measurement is to prepare for the coming FISMA audit and determine that the agency is compliant in its timeframe reporting. The data source is the agency CSIR center (CSIRC) as well as the bureau CSIRT. The responsible parties include the agency program manager and contracting team. The frequency is selected as "other" to include the FISMA year. This metric is tied to the agency's mission because it helps determine if the agency is meeting the timeframe reporting requirements. The comments section shows that this metric is the second step for preparing for the upcoming FISMA audit and that metric ID 002, 003, and 004 are all related.

<b>Incident Response Measurement Form</b>		Date: 2011 April, 05 - Tuesday
		Author: Vincent Sritapan
Metric ID 003	Percentage of Incidents Reported on Time	
Purpose & Objective	Preparations for FISMA Audits Determine If Agency 1 is compliant for reporting incidents	
Measure Type	Check all that apply: <input type="checkbox"/> Cost <input checked="" type="checkbox"/> Time <input checked="" type="checkbox"/> Quality	
Formula	$\% \text{ of Incidents Reported on Time} = \frac{\text{Number of Incident Reported on Time}}{\text{Total Number of Incidents Reported}}$	
Description	Percentage of incidents reported on time is determined by the category type. (Please see US-CERT.gov)	
Data Source(s)	Agency CSIRC Bureau CSIRTs (A through J)	
Responsible Parties	Agency 1 Headquarters, Division 1 Program Manager: Name ABC Contract Analyst Group: Senior Analyst, Junior Analyst	
Audience Check all that apply:	<input checked="" type="checkbox"/> Administrative <input type="checkbox"/> Operational <input checked="" type="checkbox"/> External <input type="checkbox"/> Other: _____	
Frequency	<input type="checkbox"/> Annual <input type="checkbox"/> Monthly <input type="checkbox"/> Weekly <input type="checkbox"/> Daily <input checked="" type="checkbox"/> Other: <u>FISMA YEAR</u>	
Tie to Agency Mission	Helps organization meet timeframe reporting compliance. intended for FISMA Audit by DHS.	
<b>Comments:</b>  Step 3: Determine Compliance Percentage Note: Management wants 95% and above on time reporting. *All Incidents not reported on time must have documentation. Metric ID 001, 002, 003, 004 All grouped for FISMA Audit in Incident Management.		
All Copyrights Reserved © 2011 Vincent Sritapan		

Figure 14. Measurement Form for Metric ID 003

Metric ID 003 is shown in Figure 14. Measurement Form for Metric ID 003 above and is a time and quality measurement type that determines the percentage of

incidents reported on time. The purpose and objective for the measurement is to prepare for the upcoming FISMA audit and determine if the agency is compliant in its timeframe reporting. The data source is the agency CSIR center (CSIRC) as well as the bureau CSIRT. The responsible parties include the agency program manager and contracting team. The frequency is selected as other to include the FISMA year. This metric is tied to the agency's mission because it helps determine if the agency is meeting their timeframe reporting requirements. The comments section shows that this metric is the third step for preparing for the upcoming FISMA audit and that management requires 95% compliance for incidents reported on time.

#### Scope of Analysis

The analysis shows that there are 25 incidents reported for the agency. For this case scenario the agency headquarters CSIRT was asked to prepare for the FISMA audit based on compliance for timeframe reporting. The only points of time that are of interest to the audit are the "Created" and "Submit US-CERT" times. At the agency headquarters level the time to report begins once the incident is reported. Using the given data set the "Created" is the time reported at the agency headquarters

CSIRT level. With the given information all incidents regarding PII are required to be reported in one hour of notification. The scope of the analysis and its results are taken from the agency headquarters point of view.

## Results

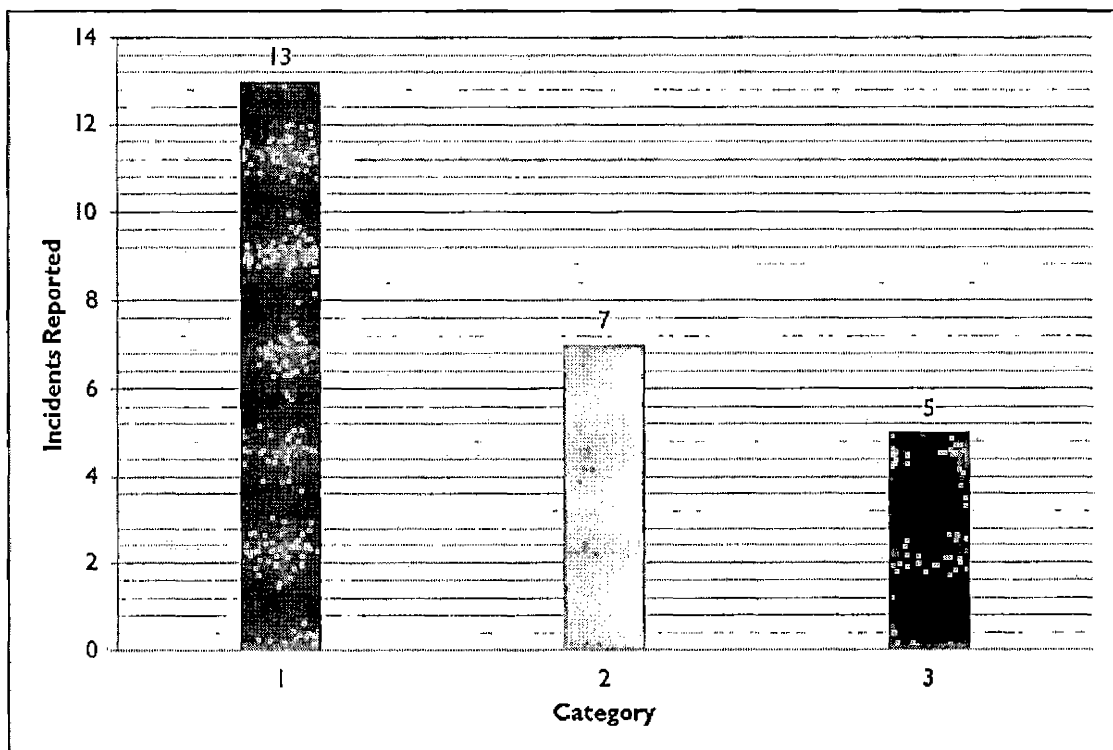


Figure 15. Incident Count by Category

For Metric ID 001 we find that there are a total of 25 incidents reported within the current FISMA year. Of those 25 incidents reported there are 13 category 1 incidents, 7 category 2 incidents, and 5 category 3 incidents (See Figure 15. Incident Count by Category,

Above). Additionally, we can illustrate the results by bureau letter in Figure 16. Incident Count by Category and Bureau below.

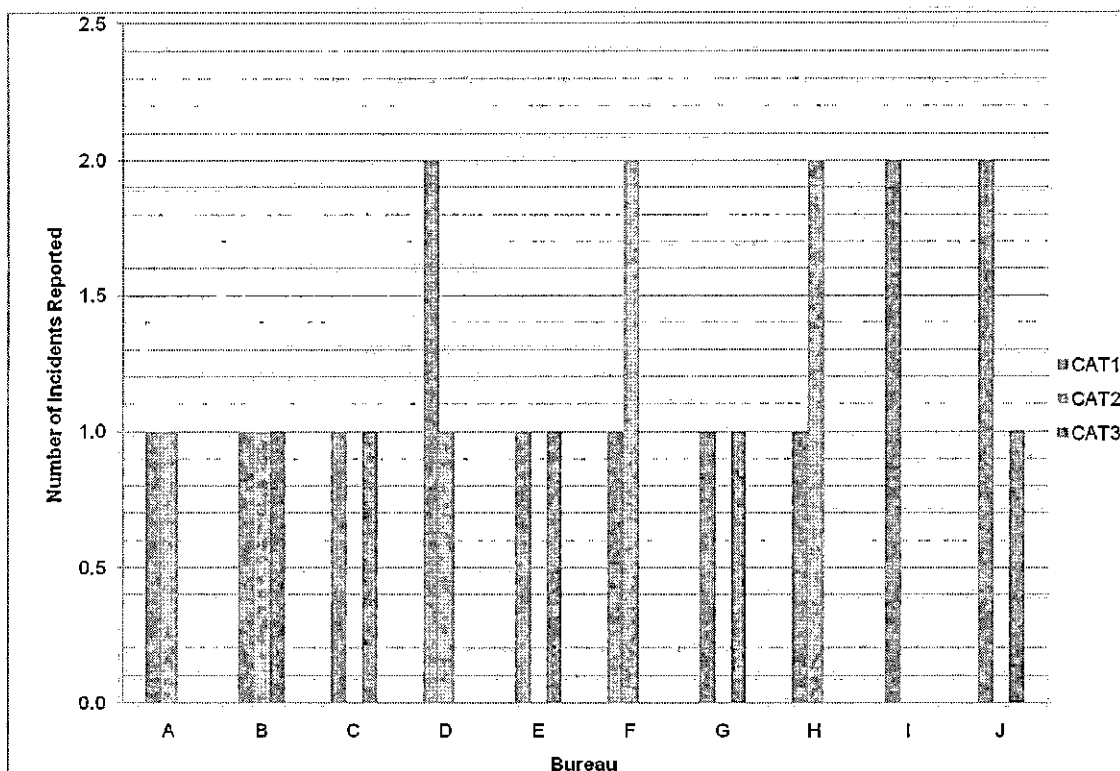


Figure 16. Incident Count by Category and Bureau

For Metric ID 002 we can see that the average time it takes for an incident to be reported from the agency headquarters CSIRT to US-CERT is about 9 minutes with the exception of 2 outliers. The outliers are Ticket No. 10 and 23 involving bureau I and PII for the incidents. Therefore, with the requirement being under one hour, 23 of the 25 incidents have been reported on time.

Table 2. Duration for Sample Incident Reports

Ticket No./ Bureau	Cat.	Created	Submit US-CERT	Duration	Within 1 hour	
1	A	1	2011.01.01.15.05.15	2011.01.01.15.15.16	10 min	Yes
2	B	2	2011.01.02.10.15.23	2011.01.02.10.25.24	10 min	Yes
3	C	1	2011.01.02.11.08.14	2011.01.02.11.18.15	10 min	Yes
4	D	1	2011.01.03.11.55.27	2011.01.03.12.05.28	10 min	Yes
5	E	3	2011.01.03.19.45.28	2011.01.03.19.54.29	9 min	Yes
6	F	1	2011.01.04.05.33.29	2011.01.04.05.42.30	9 min	Yes
7	G	3	2011.01.06.16.10.30	2011.01.06.16.19.31	9 min	Yes
8	H	1	2011.01.08.14.52.11	2011.01.08.15.01.12	9 min	Yes
9	I	1	2011.01.10.20.16.32	2011.01.10.21.24.33	1 hour 8 min	No
10	J	1	2011.01.12.14.12.12	2011.01.12.14.20.13	8 min	Yes
11	A	2	2011.01.18.08.30.22	2011.01.18.08.38.23	8 min	Yes
12	B	3	2011.02.14.11.45.56	2011.02.14.11.53.57	8 min	Yes
13	B	1	2011.02.13.08.28.00	2011.02.13.08.36.01	8 min	Yes
14	C	3	2011.02.20.11.20.37	2011.02.20.11.30.38	10 min	Yes
15	D	2	2011.02.23.20.12.23	2011.02.23.20.21.24	9 min	Yes
16	D	1	2011.02.24.20.20.19	2011.02.24.20.29.20	9 min	Yes
17	E	1	2011.02.24.18.59.11	2011.02.24.19.08.12	9 min	Yes
18	F	2	2011.02.28.08.05.41	2011.02.28.08.14.42	9 min	Yes
19	F	2	2011.03.03.11.28.20	2011.03.03.11.38.21	10 min	Yes
20	G	1	2011.03.07.16.11.43	2011.03.07.16.19.44	8 min	Yes
21	H	2	2011.03.11.09.11.22	2011.03.11.09.20.23	9 min	Yes
22	H	2	2011.03.12.17.09.45	2011.03.12.17.19.46	10 min	Yes
23	I	1	2011.03.16.08.55.53	2011.03.16.10.03.54	1 hour 8 min	No
24	J	3	2011.03.18.23.30.41	2011.03.18.23.39.42	9 min	Yes
25	J	1	2011.03.19.09.43.37	2011.03.19.09.52.38	9 min	Yes

The average time to report to US-CERT from the agency headquarters level is 9 minutes, with the exception of two incidents (See Table 2. Duration for Sample Incident Reports, Above). This means 23 out of the 25 incidents have been reported on time. According the Metric ID 003 the percentage of incidents reported on time is 92% (See

Figure 17. Percentage of Incidents Reporting on Time, Below). As noted in the comments section for Metric ID 003, management requires 95% compliance for on time incident reporting. With this result, careful consideration is needed to determine the root cause of the problem and possible actions may need to be taken to ensure on time reporting.

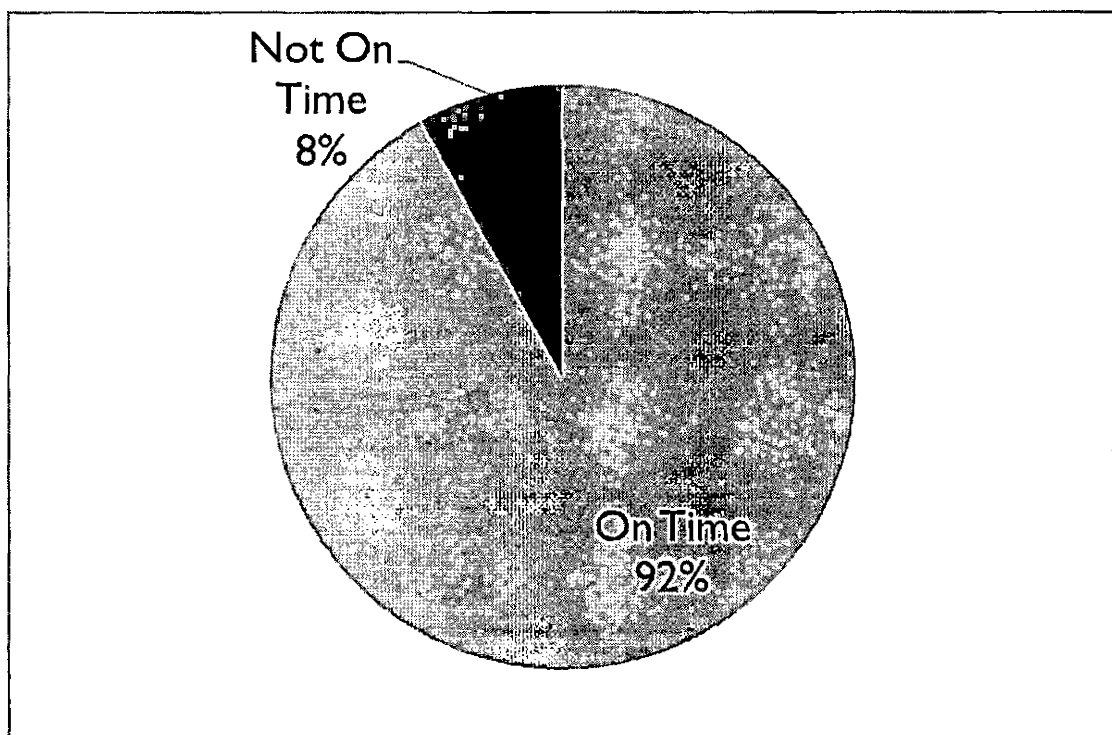


Figure 17. Percentage of Incidents Reporting On Time

## Root Cause

<i>List of Root Causes</i>
Policies not defined
Improper business process design
Improper network architecture
Improper network configuration
Lack of training
Incomplete audits
Insufficient resources
Policies not enforced

(Allen, & Davis, 2010)

Figure 18. List of Root Causes by Computer Emergency Response Team Coordination Center

With further analysis from the case scenario the root cause has been identified. A list of known root causes can be found in Figure 18. List of Root Causes by Computer Emergency Response Team Coordination Center above. By looking at the data set, the bureau where the incident originated from is bureau I. With further investigation the root cause is determined to be the lack of information



provided from the incident reported by bureau I. This causes the submission from the agency to US-CERT to be delayed. The policy at the agency level does not clearly outline the minimum requirement to submit via incident category 0-6. Additionally, the policy does not properly utilize category 6 for incidents that are still under investigation.

#### Decision to Be Made By Management

For this scenario management must decide whether to report incidents to US-CERT even when lacking information or require the bureaus to use category 6 for incidents that are lacking information. The cost measurement is shown in Figure 19. Measurement Form for Metric ID 004 below. Metric ID 004 measures the cost to change policy at the agency level, including the cost to notify and train bureau CSIRTs on using category 6 type incidents.

<b>Incident Response Measurement Form</b>		Date: 2011 April, 05 - Tuesday
		Author: Vincent Sritapan
Metric ID 004	Cost to Change Reporting Procedure	
Purpose & Objective	Improve Incident Reporting Process Measure Cost Benefit for Changing Reporting Procedures	
Measure Type	<i>Check all that apply:</i> <input checked="" type="checkbox"/> Cost <input type="checkbox"/> Time <input type="checkbox"/> Quality	
Formula	$\text{Cost of Policy Change} = \text{Rate}(\text{Labor Hours for Revision \& Notification}) + \text{Materials for Notification}$	
Description	Labor rate may vary for revision and notification Materials for notification include training costs to update Bureau CSIRTs	
Data Source(s)	Agency CSIRC Bureau CSIRTs (A through J)	
Responsible Parties	Agency 1 Headquarters, Division 1 Program Manager: Name ABC Contract Analyst Group: Senior Analyst, Junior Analyst	
Audience <i>Check all that apply:</i>	<input checked="" type="checkbox"/> Administrative <input checked="" type="checkbox"/> Operational <input type="checkbox"/> External <input type="checkbox"/> Other: _____	
Frequency	<input type="checkbox"/> Annual <input type="checkbox"/> Monthly <input type="checkbox"/> Weekly <input type="checkbox"/> Daily <input checked="" type="checkbox"/> Other: <u>FISMA YEAR</u>	
Tie to Agency Mission	Helps organization meet timeframe reporting compliance. Intended for FISMA Audit by DHS.	
<b>Comments:</b>  Determine Cost Change Reporting Procedures Metric ID 001, 002, 003, 004 All grouped for FISMA Audit in Incident Management.		
All Copyrights Reserved © 2011 Vincent Sritapan		

Figure 19. Measurement Form for Metric ID 004

For simplification, the results of Metric ID 004 find that it costs \$10,000 to change the policy and notify/train CSIRT staff. Management finds that clearly

defining use of category 6 solves the issue of on time reporting.

#### Summary

The case scenario was a basic illustration that used the metrics framework to support improvement in CSIR capabilities. For each measurement form developed, the metric ID always started by stating a purpose or objective, illustrating the driving force for the measurement. The measurement form was used to prepare for upcoming FISMA and IG audits, particular to incident management. The security measurement for CSIR ties into the agency's mission as it enables them to pass audit requirements and continue services that are mission critical. The metrics framework provided was a simplistic framework that identifies the necessary components needed to conduct a security measurement for CSIR.

## CHAPTER SIX

### CONCLUSIONS AND RECOMMENDATIONS

#### Introduction

Chapter Six provides the conclusions and recommendations as a result of this project. It reinforces the purpose of the metrics framework and the need for CSIR metrics within the federal government.

#### Conclusions

The conclusions drawn from the metrics framework for CSIR are as follows:

1. There are three types of measurements for measuring CSIR.
2. Measurements must be driven by objectives and goals.
3. Consideration of the audience needs to identify CSIRT metrics and results are critical for satisfying the audience.
4. Tying measurements to the agency's mission is essential to the success of the security measurement, enabling the user to show the value within a CSIR program.

## Recommendations

The recommendations as a result of the metrics framework for CSIR are as follows:

1. Use the metrics framework and accompanying measurement form to measure CSIR performance.
2. Save security metric formulas and notes for CSIR.
3. Collaborate and share security metric developments with others to save time and money.
4. Routinely measure CSIR capabilities for continuous improvement and to illustrate its value in supporting the agency's mission.

## Summary

Chapter Six reviews the drawn conclusions and the derived recommendations for this developed metrics framework. The overall metrics framework for CSIR is an effort to provide a standard model that supports security metric evaluations for CSIR. I sincerely hope in the future, the public and private sector can come together to create meaningful security metrics for all. As with this metrics framework, the hope is to provide a framework where security measurements provide accountability and support the agency's mission.

APPENDIX A  
UNITED STATES COMPUTER EMERGENCY READINESS TEAM  
REPORTING CRITERIA

### Federal Agency Incident Categories

Category	Name	Description	Reporting Timeframe
CAT 0	Exercise/Network Defense Testing	This category is used during state, federal, national, international exercises and approved activity testing of internal/external network defenses or responses.	Not Applicable; this category is for each agency's internal use during exercises.
CAT 1	*Unauthorized Access	In this category an individual gains logical or physical access without permission to a federal agency network, system, application, data, or other resource	Within one (1) hour of discovery/detection.
CAT 2	*Denial of Service (DoS)	An attack that <i>successfully</i> prevents or impairs the normal authorized functionality of networks, systems or applications by exhausting resources. This activity includes being the victim or participating in the DoS.	Within two (2) hours of discovery/detection if the successful attack is still ongoing and the agency is unable to successfully mitigate activity.
CAT 3	*Malicious Code	<i>Successful</i> installation of malicious software (e.g., virus, worm, Trojan horse, or other code-based malicious entity) that infects an operating system or application. Agencies are NOT required to report malicious logic that has been <i>successfully quarantined</i> by antivirus (AV) software.	Daily Note: Within one (1) hour of discovery/detection if widespread across agency.
CAT 4	*Improper Usage	A person violates acceptable computing use policies.	Weekly
CAT 5	Scans/Probes /Attempted Access	This category includes any activity that seeks to access or identify a federal agency computer, open ports, protocols, service, or any combination for later exploit. This activity does not directly result in a compromise or denial of service.	Monthly Note: If system is classified, report within one (1) hour of discovery.
CAT 6	Investigation	<i>Unconfirmed</i> incidents that are potentially malicious or anomalous activity deemed by the reporting entity to warrant further review.	Not Applicable; this category is for each agency's use to categorize a potential incident that is currently being investigated.

\*Defined by NIST Special Publication 800-61

US-CERT (2011). Federal Agency Incident Categories. *US-CERT, Department of Homeland Security*. Retrieved from <http://us-cert.gov/federal/reportingRequirements.html>

APPENDIX B

FORMULAS FOR COMPUTER SECURITY INCIDENT RESPONSE

BY CENTER FOR INTERNET SECURITY



$$COI = \sum (\text{Direct\_Loss} + \text{Cost\_Business\_Downtime} + \text{Cost\_Containment} + \text{Cost\_Recovery} + \text{Cost\_Restitution})$$

Cost of Incidents

$$MCOI = \frac{\sum (\text{Direct\_Loss} + \text{Cost\_Business\_Downtime} + \text{Cost\_Containment} + \text{Cost\_Recovery} + \text{Cost\_Restitution})}{\text{Count(Incidents)}}$$

Mean Cost of Incidents

$$MIRC = \frac{\sum (\text{Cost\_Recovery})}{\text{Count(Incidents)}}$$

Mean Cost of Incident Recovery

$$MTTID = \frac{\sum (\text{Date\_of\_Discovery} - \text{Date\_of\_Occurrence})}{\text{Count(Incidents)}}$$

Mean Time to Incident Discovery

$$MTBSI = \frac{\sum (\text{Date\_of\_Occurrence}[\text{Incident}_n] - \text{Date\_of\_Occurrence}[\text{Incident}_{n-1}])}{\text{Count(Incidents)}}$$

Mean Time between Security Incidents

$$MTIR = \frac{\sum (\text{Date\_of\_Recovery} - \text{Date\_of\_Occurrence})}{\text{Count(Incidents)}}$$

Mean Time to Incident Response

Center for Internet Security Community (2010). CIS Security Metrics v.1.1.0.  
The Center for Internet Security, 6-39.

## APPENDIX C

### ACRONYMS

ACISO: Associate Chief Information Security Officer  
CERT/CC: Computer Emergency Response Team Coordination Center  
CERT: Computer Emergency Response Team  
CIO: Chief Information Officer  
CISO: Chief Information Security Officer  
CMU: Carnegie Mellon University  
CSIR: Computer Security Incident Response  
CSIRC: Computer Security Incident Response Center  
CSIRT: Computer Security Incident Response Team  
DARPA: Defense Advanced Research Project Agency  
DHS: Department of Homeland Security  
FISMA: Federal Information Security Management Act  
FIRST: Forum on Incident Response and Security Teams  
ID: Identification  
IDS: Intrusion Detection System  
IG: Inspector General  
IR: Incident Response  
NIST: National Institute of Standards and Technology  
OMB: Office of Management and Budget  
PII: Personally Identifiable Information  
SEI: Software Engineering Institute  
US-CERT: United States Computer Emergency Readiness Team

## REFERENCES

- Alberts, C., Allen, J., & Stoddard, R. (2011). *Security measurement and analysis*. Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University.
- Alberts, C., Dorofee, A., Killcrece, G., Ruefle, R., & Zajicek, M. (2004). *Defining incident management process for CSIRTs: A work in progress*. Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University.
- Allen, H. J., & Davis, N. (2010). *Measuring operational resilience using the CERT resilience management model*. Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University.
- Armed Forces Communications & Electronics Association. (2010, July 8). *The 2nd annual AFCEA DC cybersecurity symposium, USCYBERCOM's role in protecting .mil, .gov & .com*. Washington, DC: Chapter, Armed Forces Communications & Electronics Association.
- Atkinson, R. (1999). Project management: Cost, time, and quality, two best guesses and a phenomenon, its time to accept other success criteria. *International Journal of Project management*, 17(6), 337-342.
- Brewer, P., Garrison, R., & Noreen, E. (2009). *Introduction to managerial accounting* (5<sup>th</sup> ed.). McGraw-Hill/Irwin.
- Center for Internet Security Community. (2009). *CIS security metrics v.1.0.0*. East Greenbush, NY: The Center for Internet Security.
- Center for Internet Security Community. (2010). *CIS security metrics v.1.1.0*. East Greenbush, NY: The Center for Internet Security.
- Chew, E., Swanson, M., Stine, K., Bartol, N., Brown, A., & Robinson, W. (2008). *Performance measurement guide for information security*. NIST Special Publication 800-55, Revision 1, 12-15, 22-27.

- Computer Emergency Readiness Team, (2011a). *Publications catalog. Computer emergency readiness team, software engineering institute, Carnegie Mellon univeresity.* Retrieved from [http://www.cert.org/search\\_pubs/search.php](http://www.cert.org/search_pubs/search.php)
- Computer Emergency Readiness Team. (2011b). *Meet CERT. computer emergency readiness team, software engineering institute, Carnegie Mellon university.* Retrieved from [http://www.cert.org/meet\\_cert/](http://www.cert.org/meet_cert/)
- Davis, J. (2007). Hackers take down the most wired country in Europe. *Wired Magazine*, 15, 09.
- Department of Homeland Security, Office of the Inspector General. (2010). *DHS needs to improve the security posture of its cybersecurity program systems.* Washington DC: Department of Homeland Security, United States, OIG-10-111.
- Dorofee, A., Killcrece, G., Ruefle, R., & Zajicek, M. (2007). *Incident management capability metrics version 0.1.* Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University.
- Ellis, J., Fisher, D., Longstaff, T., Pesante, L., & Pethia, R. (1997). *Report to the president's commission on critical infrastructure protection.* Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University. (CMU/SEI-97-SR-003)
- Garfinkel, S. (2005). *History's worst software bugs.* Wired.com. Link: <http://www.wired.com/software/coolapps/news/2005/11/69355?currentPage=all>
- General Accountability Office. (2009). *Information security: Agencies continue to report progress, but need to mitigate persistent weaknesses.* Washington DC: General Accounability Office. (GAO-09-0546)
- General Accountability Officer. (2008). *Information security: Protecting personally identifiable information.* Washington DC: General Accounability Office. (GAO-08-343, 5)

- General Accountability Officer. (2010). *Cybersecurity: Progress made but challenges remain in defining and coordinating the comprehensive national initiative*. Washington DC: General Accountability Office. (GAO-10-338)
- Hopkins, E. (2009). *United State information and communication enhancements act of 2009*. Washington DC: Subcommittee on Federal Financial Management, Government Information, Federal Services, and International Security.
- House of Representatives 245-56. *Federal information security management act of 2002*.
- Jansen, W. (2009). Directions in security metrics research. *NIST Interagency Report*, 7564, 10-15.
- Joint Task Force Transformation Initiative. (2009). *Recommended security controls for federal information systems and organizations*. Washington DC: NIST Special Publication 800-55 Revision 3.
- Markoff, J. (2008). *Before the gunfire, cyberattacks*. The New York Times, Technology.
- Mills, E. (2009). *Melissa virus turns 10*. Security, News, CNET. Link: [http://news.cnet.com/8301-1009\\_3-10206275-83.html](http://news.cnet.com/8301-1009_3-10206275-83.html)
- National Security Council. (2011). *Cybersecurity: What we must do*. White House, United States of America. Link: <http://www.whitehouse.gov/cybersecurity>
- NIST. (2011). *Special publications (800 Series). Computer security division, computer security resource center, national institute of standards and technology*. Link: <http://csrc.nist.gov/publications/PubsSPs.html>
- Niven, R. P. (2008). *Balanced scorecard: Step-by-step: For government and nonprofit agencies*. John Wiley & Sons, Business & Economics.
- Payne, C. S. (2006). *A guide to security metrics*. SANS Institute, 1-3.

- PC Tools. (2010). Top 10 computer viruses. *Security News, PC Tools*. Link: <http://www.pctools.com/security-news/top-10-computer-viruses/>
- Rezmierski, V., Deering, S., Fazio, A., & Ziobro, S. (1998). Incident cost analysis and modeling project 1: A report from the CIC security working group to the CIC chief information officers. *Committee on Institutional Cooperation*, 13-15.
- Scarfone, K., Grance, T., & Masone, K. (2008). Computer security incident handling guide. *NIST Special Publication 800-61 Revision 1*, 2-16, 3-13, 3-14, 3-26.
- Soanes, C., & Stevenson, A. (2008). *The concise oxford english dictionary* (12<sup>th</sup> ed.). "framework n." Oxford University Press.
- Software Engineer Institute. (2011). *Fundamentals of incident handling*. Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University.
- US-CERT. (2008). *US-CERT information sheet v2*. US-CERT, Department of Homeland Security. Retrieved from [http://www.us-cert.gov/reading\\_room/infosheet\\_US-CERT\\_v2.pdf](http://www.us-cert.gov/reading_room/infosheet_US-CERT_v2.pdf)
- US-CERT. (2011). *Federal agency incident categories*. US-CERT, Department of Homeland Security. Retrieved from <http://us-cert.gov/federal/reportingRequirements.html>
- West-Brown, J. M., Stikvoort, D., Kossakowski, K., Ruefle, R., & Zajicek, M. (2003). *Handbook for Compute Security Incident Response Teams (CSIRTs)* (2<sup>nd</sup> ed.). Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University, 10-11, 40-55, 191.
- White House. (2003). *The national strategy to secure cyberspace*. Washington DC: White House, United States of America.
- White House. (2009). *Cyberspace policy review: Assuring a trusted and resilient information and communications infrastructure*. Washington DC: White House, United States of America.

- Wilshusen, C. G. (2011). *Cybersecurity: Continued attention needed to protect our nation's critical infrastructure and federal information systems. testimony before the subcommittee on cybersecurity, infrastructure protection and security technologies.* Washington DC: Committee on Homeland Security, House of Representatives. (GAO-11-463T)
- Xie, N., & Mead, R. N. (2004). *SQUARE project: Cost/benefit analysis framework for information security improvement projects in small companies.* Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University.