

GIAC Enterprises

Establishing a Security Metrics Approach

Joint Written Project

Project Plan

Chris I. Cain, Erik Couture
10/14/2011

Table of Contents

Introduction	3
Project Scope	3
Project Management Approach	3
Milestone List	4
Work Breakdown Structure	4
Cost Management Plan	5
Resource Calendar	6
Sponsor Acceptance	6

Introduction

This tiger team was initiated to provide guidance to the CISO with the goal of improving the company's security posture. In particular, the tiger team will focus on identifying and analysing multiple sources of IT, security and other corporate data with the aim of identifying the most effective methods with which GIAC Enterprises can track and improve its security posture using a metrics-based approach.

Following the successful lead of other recent tiger teams, we will model our security metrics approach on the SANS Top 20 Security Controls. This will allow GIAC's security metrics to be directly mapped to our Security Controls Implementation Plan (SCIP) and should, in implementation, be more effectively integrated with those related Security Controls. Akin to the SCIP's recommendations of implementing quick-win measures for maximum return on security investment (ROSI), this Project will aim to draw out a prioritized list of metrics which reflect the company's real-life risk exposure and will best help inform management as to the company's security posture.

The key deliverables will be a whitepaper presenting the team's findings and a supporting presentation, aimed at senior management. These documents will outline a set of recommendations for the implementation of a metrics-based approach to IT security at GIAC Enterprises and will describe the implementation of a dashboard-type overview giving senior management a snapshot glimpse of GIAC's security posture.

Project Scope

This project scope will include analysis of the following, as they pertain to IT security.

- IT security measures/statistics;
- IT service/helpdesk statistics;
- IT and security operating procedures;
- IT/security change management processes;
- Historical analysis of IT security processes and breaches;
- Organizational business processes/workflows; and
- HR/personnel security training/awareness levels.

Project Management Approach

This project will be co-managed by Erik Couture and Chris Cain. As co-chairs of the tiger team, they

will lead the research, information gathering and production of the assigned deliverables. They will communicate closely with each other and key stakeholders at GIAC Enterprises. They will provide a weekly update to the COO and CISO indicating any areas requiring additional guidance or clarification from senior management.

Milestone List

Milestone	Description	Date
Project Initiated	Project charter received from Mr. Northcutt	9 Sept 11
Project Plan Complete	Plan submitted to Mr. Northcutt by tiger team	14 Sept 11
Project Kickoff	Plan accepted and work begins	~16 Sept 11
Main Deliverables Completed	1 month project window closes, report and presentation submitted.	~16 Oct 11
Project Recommendations Decision Point	President and Board decide on way ahead with regard to security metrics.	~30 Oct 11

Work Breakdown Structure (WBS)

The WBS below outlines key project work areas. It, along with the attached Gantt chart (Appendix 1), provide an overview of key project goals, interdependencies and work assignments. The numbering follows that of the Gantt Chart below.

Level 1	Level 2	Level 3
1 Security Metrics Plan	1.1 Project Plan	1.1.2 Deliverable: Develop Gantt Chart/Tasks 1.1.3 Deliverable: Develop Summary 1.1.5 Develop backup plan
	1.2 White Paper	1.2.1 Verify & Validate User Requirements 1.2.3 Create Preliminary Scope Statement 1.2.5 Develop Metrics for 20 Critical Controls 1.2.7 White Paper Development and Outline 1.2.8 White Paper Executive Summary 1.2.9 White Paper References
	1.3 External Partnerships	1.3.1 Interview CISO's 1.3.2 Contact SANS for logs and review 1.3.5 Create Dashboard

	1.4 Presentation	1.4.1 Develop Presentation Outline 1.4.2 Develop Presentation Notes 1.4.4 Rehearse and Revise Presentation
	1.5 Press Release	1.5.1 Develop Press Release 1.5.3 Post Press Release on various networking sites

Cost Management Plan

This project will be funded out of normal operations and maintenance (O&M) funding, and will not commit to expending additional funds until its recommendations are approved and funded by the Board.

Resource Calendar

Resource	Estimate Time Required	Role
Erik Couture	Full time for 30 days	Team Lead
Chris Cain	Full time for 30 days	Team Lead
President	2 hours (1x2hr meeting)	Project Sponsor
CISO	8 hours (4x2hr mtgs weekly)	Advise on security related procedures and statistics
COO	2 hours (2x1hr mtgs weekly)	Advise on corporate operations; help focus tiger team on correct metrics.
CFO	2 hours (1x2hr mtg)	Advise on IT/security investment/budget, ROI metrics etc.
Helpdesk	2 hours (1x2hr mtg)	Advise on helpdesk/ downtime statistics
HR Manager	2 hours (1x2hr mtg)	Advise on employee training levels, results of any related employee polling/statistics
Employee base	20 minutes	A cross section of the employee base will be asked to complete a ~20 minute questionnaire.

Sponsor Acceptance

Approved by Project Sponsor:

Date: _____

 Mr. Stephen Northcutt
 President GIAC Enterprises