Global Information Assurance Certification Paper

Case Study:
Empowering Your IT Call Center as Information Security Advocates

Prepared for:

GIAC Security Essentials Certification (GSEC)
GSEC Practical Assignment
Version 1.4b, Option 2

Prepared by:

Carrollynn Biggers Brown, CISSP

Table of Contents

Table of Figures

Conventions Used in this Paper

Tables, diagrams, and picture objects are denoted as Figures. The label appears under each object in *Arial 10 pt italicized* font. The naming convention is as follows:

Figure X.Y.Z: Title here

Where X, Y, and Z are determined by which Heading and Heading 2 the object falls such that:

- X = Header1 section (e.g., 1-7)
- Y = Header2 section (e.g., 1-4)
- Z = sequential number of object for that X.Y label

For example, *Figure 3.2.3: Sample* would denote that this Figure is under Section 3, sub-section 2 and is the third object in that subsection.

NOTE: All figures, unless noted otherwise, are taken from materials I created and owned.

Abstract

This practical covers how my Information Security (IS) organization empowered the Information Technology (IT) Call Center as security advocates. My case study covers the operational aspect of information security and on implementing security processes at it related to the ITCC business environment. Particularly, I address the strategic direction I took in transitioning front line support of information security to the IT Call Center (ITCC). This includes identifying the training and tools I provided to facilitate the successful transition and discussing the long-term strategy for ensuring continuous improvements both in our inter-relationship and the processes and training provided to the ITCC. I saw this as a unique opportunity to have a pro-active relationship with a vital, but often un-respected component of any IT department, the ITCC. Key to its success was the development and implementation of processes vital for the ongoing successful maintenance of that partnership based on information security policies and technical solutions.

I was able to build a relationship with the ITCC that served as the foundation upon which the IS organization was able to transition cohesive tactical and strategic programs. Our partnership has become an integral part of the overall information security program with the ITCC having a tremendous impact on our business operations model. I realized the value of leveraging the ITCC as security advocates because as the interface to the IT department, the ITCC touches all aspects of the company. This effort has enabled the shift from a purely re-active engagement model to one that now is more pro-active in nature. As a result of a successful engagement, the IS organization and the ITCC have strived to ensure security is a component of their business operations and implemented a continuous improvement program to ensure they are provided with the skills, tools, and methods they need to continue to act in the capacity as information security advocates.

Background

Before delving into my case study, I want to give a general overview of my company and its IT department. I cover my role as a member of the IS organization and as it relates to the IT Call Center. I also outline the method of problem solving I used to address the issue of how to leverage the ITCC as security advocates.

Overview of Company

My employer is a Fortune 500 company with over 50,000 employees worldwide and offering over 300 products and services. Its net revenue exceeds $20 billion. The IT department makes up approximately 5% of the total the corporate workforce and is aligned to support the infrastructure and productivity needs and the requirements of its core business segments. IT is essentially responsible for providing the information technology products and services, in addition to controlling operating costs, to help the company run effectively and efficiently.

The ITCC is a major group of the IT Customer Services (ITCS) organization and serves as the umbrella for all groups that have direct contact with the employees of the company employees. The ITCC is global, made up of various teams within each region, and collectively, provides 24x7 regional support to the organization itself – its corporate employees and contract employees. It is the first stop for employees with a computing problem and its primary services include helping employees meet their day-to-day computing needs. The ITCC group works closely with product/services engineers and product managers with IT to deliver solutions to the worldwide employee base. They use scripts, typically procedures that detail systematic instructions, to handle all employee problems and questions about all office software and hardware, network, and productivity. Their key mediums for handling calls are via the telephone, email, and web interface.

The IS organization is primarily based in the continental United States with matrix organizations in Asia and Europe regions. It sits three levels down from the CEO of the IT organization - another problem, another case study. IS is recognized as a corporate organization and is chartered with driving security across the company and is not limited to providing security programs, solutions, or consultation to IT. The IS organization is composed of several groups and the group to which I belong will be called Enterprise Computing Security (ECS).

My Role as IS Liaison

I was hired as an information security specialist in the IS organization. I worked on a team who was responsible for providing security support (consultation and solutions) to several groups within the IT department. Over the years, the objects of my support have varied and expanded outside IT to include Human Resources, Finance, and Legal departments. Because the one constant was my involvement in IT programs and projects, I have consistently retained that department as a core customer and a few years later, I became the IS liaison for the ITCS organization.

In my role as the IS liaison to the ITCC, I have participated on various programs and projects driven by that organization. As it pertains to this case study and in working with the ITCC, I have been their point of escalation for non-emergency IS-related queries or issues. In addition, I have led joint projects with the ITCS organization to include risk assessments and product and new technology evaluations. It was during this period that I began to realize the tremendous opportunity to leverage that customer base and to build on a partnering relationship that would serve to empower ITCC security advocates.

Problem Solving Approach

I used the seven-step method for problem solving and quality tools. They are process flows, brainstorming, cause and effect diagrams, decision-making, and success indicators. These tools support the problem-solving process by assisting in documenting the as-is process, determining and measuring performance gaps, identifying potential causes leading to implementing solutions, and monitoring and

assessing the improvements. Table 2.1.1 shows how I have mapped the 7-step method for problem solving into the core sections of this practical. This case study covers my work on a project that was implemented in phases where each phase was a sub-project. The sub-projects overlapped each other, as noted in the comments column. This layout is also mirrored in the Table of Contents.

7 STEP METHOD FOR PROBLEM SOLVING	COMMENTS
"BEFORE" SNAPSHOT	
Step 1. Defining the Problem Step 2. Analyzing the Current Situation Step 3. Identifying and Determining Root Cause	Conducted risk assessment of current situation
"DURING" SNAPSHOT	
Step 4. Developing Solution(s) Step 5. Implementing Solution(s)	Project broken down into two sub-projects
"AFTER" SNAPSHOT	
Step 6. Standardizing Solution(s)	Identified for both sub-projects
Step 7. Determining Next Steps	Identified for the overall project, particularly sub-project 2 (or Phase II)

Figure 2.3.1: 7-step method for problem solving

I used standard methodology for managing this project. Each of the project management phases roughly matched with the 7-step method for problem solving. Where appropriate, I have included screen shots of the project plan.

"Before" Snapshot

IS revamped its engagement model and communicated to employees that the ITCC was providing front line information security support. IS was expecting employees to now contact ITCC for all information security support and ITCC to provide timely, accurate responses. However, employees had become accustomed to contacting IS directly. ITCC had a small set of information security scripts and was not comfortable handling addressing such queries or issues.

Defining the Problem

Due to limited resources and the need to focus more on strategic solutions, the IS organization decided to offset some of its day-to-day operational tasks to the ITCC. On behalf of the IS organization, I negotiated with ITCC to have them provide front line support in dispositioning any employee queries received by telephone that pertained to information security. The general agreement was that ITCC would resolve what they could and escalate the unresolved ones to ECS.

The initial agreement included the following:

- ECS would provide scripts or procedures that ITCC uses when dispositioning an employee's call for assistance, help or direction to facilitate the ITCC's successful resolution of employee IS questions
- ITCC would log each call, as they do all their other calls, into the call tracking system
- ITCC would route the employee IS calls that they could not resolve into an IS-specific queue for ECS to follow up on and resolve
- ECS would use the call tracking tool to document closure on any IS queries that the ITCC escalated

To this end, ECS worked with the ITCC to modify the company phone system menu with the new option for information security support and added a variable option in the call tracking tool for identifying IS calls and one for designating the call queue for IS escalations. Members on the team brainstormed on a list of quick procedures/scripts that we could write and implement for the ITCC that would provide them with the means to get started on providing answers to IS questions. A small set of IS scripts that mirrored the content of the newly published IS policy set[1] was implemented. In parallel, we created messages and communicated them to the corporate population on the engagement model where the focus was to shift employees to call their ITCC instead of a member in the IS organization.

We soon discovered that where the process worked, it worked a little too well and where it did not, it really did not. Employees were beginning to call their local ITCC instead of an IS personnel directly, resulting in a small decrease in the number of direct customer queries. However, we were still handling too many front-line type consultations as ECS was now being inundated with an influx of escalations from ITCC. Frustration began to permeate between ITCC and IS organization as the ITCC found it ill-equipped to successfully handle the additional call volume. Employees, as well, were becoming dissatisfied with the ITCC responses and still having to contact ECS after wasted time with ITCC. We certainly had a two-fold problem – the IS organization was still handling too many front-line calls and the ITCC group did not have the training or tools needed to facilitate their new role in providing front-line information security support to the corporate employees.

Analyzing the Current Situation

Obtaining ITCC management approval to take on this additional work was the relatively easy part. The challenge was to do this in a manner that essentially removed us from the front line, empowered the ITCC with the training and tools they need to pick up this task without detrimentally impacting the customer, and enabled the IS organization to provide continuous operational security improvement. My next step was to do an analysis of the current situation.

[1] IS policy set consists of policies, standards and procedures. The terms are used interchangeably.

Business Operations Process

Based on discussions with representatives from ITCC and members of ECS, I identified a fluid workflow for providing support to employees on IS queries. An employee, in an attempt to get an answer to information security questions or find resolutions to information security issues, will do at least one of the following:

- Searches for the solution on the corporate intranet – infosec web sites
- Contacts his/her local ITCC group via phone call, email or web
- Contacts the ECS team

Being able to find the answer or solution on the intranet web sites is by far the most preferable option. The employee is satisfied; ITCC is freed up to take other calls, and IS organization can continue focusing on less tactical endeavors. This is ideal because the employees will look on the web sites first and successfully find answers or possible solutions.

The workflow for the latter two options is depicted in Figure 3.2.1. It is evident that even this level of consultation can become cumbersome.

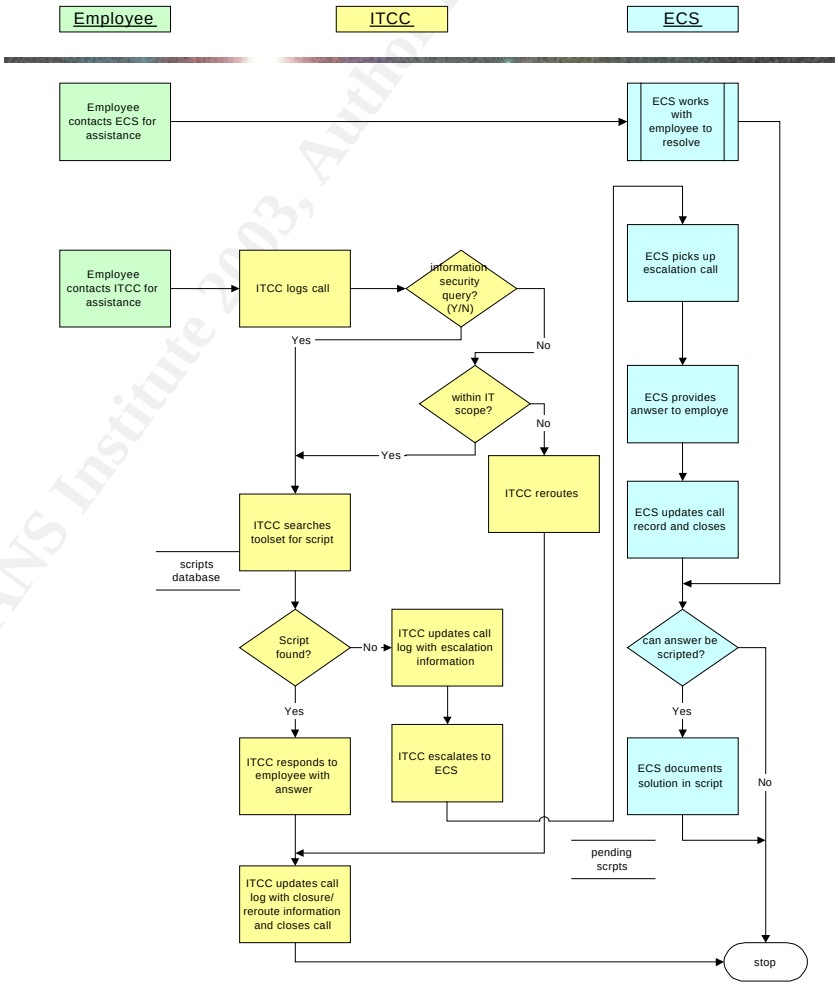


Figure 3.2.1: Employee query/resolution process flow

The ITCC has its own processes for handling employee questions. Each ITCC dispositions the call based on several factors as it pertains to the IT support model and if a script is available.

Step 1: ITCC determines nature of call and documents in call tracking tool.

Step 2: ITCC dispositions call accordingly, where one of the three occur:

- Resolve. The ITCC agent uses existing scripts to provide employee with an answer. The call is then closed.

- Reroute. If the ITCC determines that a non-IT organization owns the answer, the employee is rerouted to the appropriate contact. The call is closed.

- Escalate. The ITCC will escalate within the IT organization if they do not have the script or the script instructs them to escalate. The initial escalation stays within ITCC and goes to a team lead or manager. ECS will be the next point of escalation if the team leader or manager cannot resolve. The call is not closed.

In the event ITCC escalates the call to ECS, we picked up the service request and began consultation with the employee. Our process was as follows:

Step 3: Answer the call either by following up with the employee or by providing the resolution to the ITCC agent. The call is then closed and more often than not, the ITCC agent makes the update in the call tracking system.

Step 4: Determine if the question and answer could be scripted for ITCC use. If so, document and provide to me. I, in turn, would work with my counterpart in the ITCC group to ensure it was complete and accurate before making the script accessible to the ITCC group.

Many times, employees will skip the self-help option and their local ITCC to directly contact someone in the IS organization, usually a member of the ECS team. When this happens, we are usually able to quickly resolve. There are times too when a consult request may require a more detailed engagement, for example project participation, diplomacy in response, or even involving our HR and/or Legal departments.

Note that on some occasions, ITCC may instruct the employee to contact ECS directly. The conversation from many of the employees who contacted us directly often started like this: *"I called ITCC and they told me to contact you about …."* And often, the employees were unaware if the ITCC had documented their initial call in the call tracking system. The point is that even with an agreed-upon process flow, both ITCC and ECS recognized that in practice, implementations might vary.

IT as a Role Model of Information Security

So you may have wondered why would ITCC take on additional work that on first appearance seemed to be outside its current operating model. The IT CEO had taken the stand that IT would role model information security throughout the company. According to Greg Shipley in "How Secure is Your Network", he re-affirmed that having an executive champion security is a vital ingredient for a winning information security program.[2] As such, all IT organizations began to identify security deliverables in their respective projects and programs. For IS, this put us a step closer to realizing a more pro-active information security business model. My engagement with the ITCC was one of the key components of the overall information security program just as their mutually partnering with IS was also lucrative for their business operations.

Summary of Current Situation Analysis

I was able to clearly identify the stakeholders and the potential impact to them using the previously documented workflow process, Figure 3.2.1. An analysis of the current situation yielded answered "who, what, when, where, why and how". My summary findings are shown in Figure 3.2.2.

WHO HAS A STAKE IN SOLVING THE PROBLEM?	
Employees	Expect quick resolutions to any questions they direct to IT support personnel
ITCC	Has a huge impact on how employees see the success of the IT organization
IS	Striving to focus on more strategic business opportunities
WHAT IS THE IMPACT TO THE STAKEHOLDERS?	
Employees	Not able to get IS questions resolved in a timely manner, possibly resulting in negative customer satisfaction
ITCC	Potential loss of business due to perception of being incompetent to answer information security questions
IS	Potential loss of credibility due to perception that the ITCC is an extension of the IS organization
WHEN DOES THE IMPACT OCCUR?	
Employees	During deployment (shortly after implementation) and possibly at first call to the ITCC
ITCC	During deployment (shortly after implementation) and possibly at first call to the ITCC
IS	During deployment (shortly after implementation) as employees will revert to calling the IS organization directly.
WHERE DOES IT OCCUR?	
Employees	Over the phone with ITCC
ITCC	Over the phone with employee

[2] Shipley, Greg, p. 72.

IS	With escalation from ITCC, in meeting with the customer/group
WHY IS IT IMPORTANT?	
Employees	• Information security may have a huge impact to their project or program delivery • May rely on IS organization providing a solution if there is an information security issue or concern • May move ahead without addressing security in program/project or make security impacted decision based on their limited knowledge
ITCC	Affect the bottom line for the IT organization where performance is a critical factor in determining effectiveness of IT organization.
IS	Perception may serve to perpetuate that information security is a showstopper instead of a business enabler
HOW DID WE GET HERE (HISTORY OF THE PROBLEM)?	
Employees	Employees have attended mandatory information security awareness training within the first 3 months of employment and were informed of where to seek additional assistance if they have questions about information security
ITCC	CEO has designated that IT will become a role model of information security. As such, the ITCC has looked to take on new business in this area.
IS	• Effective awareness, training and education programs resulted in increasing requests for IS organization to provide support to their programs and projects • The new engagement model has been announced and published throughout the company.
HOW MUCH DOES IT COST THE STAKEHOLDERS?	
Employees	Although it is difficult to project how much this problem could cost the company, it is safe to say that the potential for serious damage does exist. Scenarios range from cost associated with having to re-do a security solution or retrofit a product or process with security to incurring loss as a result of having to pull a product from production or the market due to a security issue. Other costs include losses attributed to a damaged corporate reputation (confidence, identity) and subsequent decline in market-share, all of which could potentially represent millions of dollars in revenue.
ITCC	
IS	

Figure 3.2.2: Current Situation Analysis matrix

Identifying Causes

My next step was to identify all the possible causes of this problem. I facilitated separate discussions with call agents in ITCC, ECS members, and a small set of employees. We brainstormed on the issues and identified causes to determine root causes.

Inherent Nature of ITCC

The ITCC is primarily focused on ensuring their customers are satisfied, often equating to *availability* and are indicators-driven. As noted by Chad McClennan in his article "Call Center Musts:", this is typical of a call center.

> "Those responsible for running the day-to-day call center and customer contact operations are extremely busy with day-to-day issues. Personnel, scheduling, technical infrastructure stability, reporting, practices and procedures, service levels, etc - all infringe on their ability to think and act strategically. This is a fact of life – just ask them. It is not that they are incapable – they just lack resources and time (and in some cases, expertise)."[3]

Having the ITCC group take on providing front-line IS support also represents a new business model for them. Historically, they disposition customer queries that are related to PC usage and IT-supported software and hardware questions. The IS organization was introducing the requirement to address all customer queries, not just those within the scope of the IT arena. Because the ITCC was focused on answering technical "how to" questions and specifically, those that pertained to the use of IT-supported products, a lot of IS consults ended up routed back to the IS organization to disposition.

Also, many of the IS consults did not lend themselves well to clear-cut answers. Being a metrics/indicators-driven organization, the ITCC chose the most amicable solution – escalate (did not record this was a call they received initially). They were chartered to close calls and keep customers happy.

IS Organization and Limited Resourcing

The IS organization had made sufficient progress in raising awareness of information security. In addition to having corporate information security policies and annually updating our corporate risk assessment, the ECS team also worked with the high-risk business groups to help them understand the threats and potential impact due to a compromise and how to protect their assets and the information against unauthorized access and modification, or attacks. We strived to operate in a manner that would serve to re-enforce we were there to help them achieve their business goals as opposed to being obstacles. We had effectively drummed up the business. The increase in awareness also increased resourcing requests from employees. Suffice it to say, resources in our environment – and in IT in general – have never been enough.

The IS organization had recently published an updated set of information security procedures. Communications on the new customer entry model was ramping up. Yet, we were still spending an inordinate amount of time handling general employee queries. Most of these queries were via the IS mailbox and the remainder was

[3] McClennan, http://www.crmcommunity.com/news/article.cfm?oid=6EF3717D-D460-480A-B440EA9391F8CA18

spread over "hallway" consults and cold phone calls. Many times, when the ECS engaged each other on these consults, we discovered there were times when the same or similar questions were asked. Also, the ECS was doing a weekly rotation among its team members to support the IS mailbox. As such, we may run the risk of giving different answers for the same situation.

Given the dynamics of information security, it is not practical to identify answers to all the variants of questions an employee can ask about any given policy, standard or procedure. We used our personal experiences and understandings when determining if it would be worthwhile to script the answer to a particular query.

Root Causes

I used the listing of potential causes and grouped them in a fishbone diagram (also known as a cause and effect diagram). As noted in Figure 3.3.1, the most prevalent root causes were lack of tools and processes to facilitate effective support for information security.

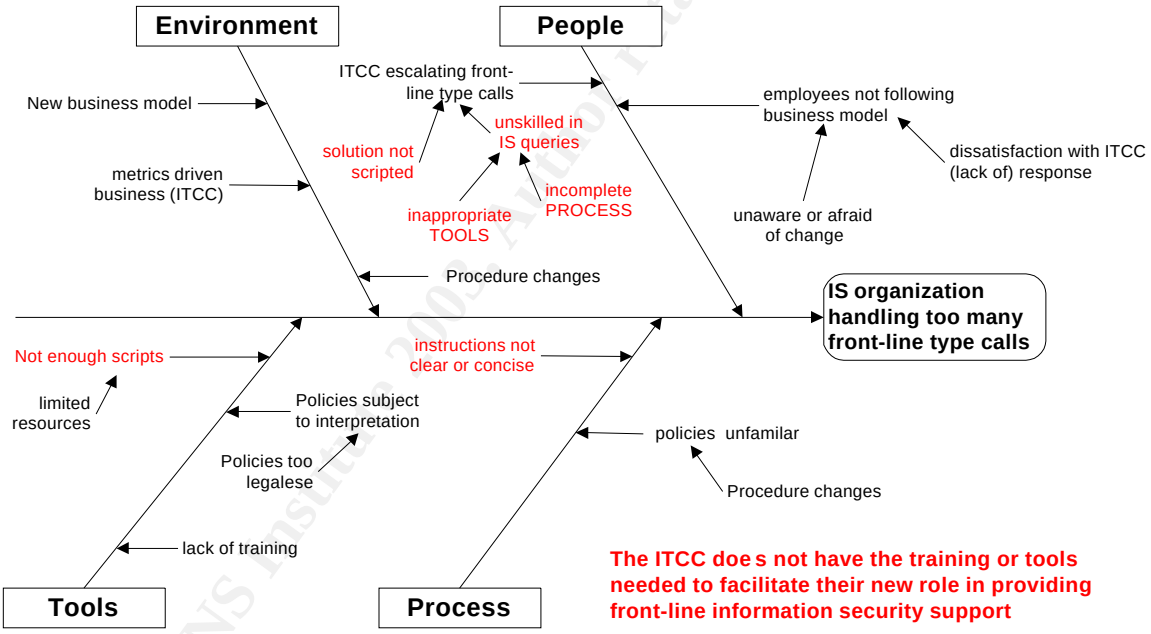


Figure 3.3.1: "Cause and Effect" diagram

Calculating Potential Risk

I realized as the stakeholders provided input on assessing the current situation that a scenario-based model lent itself to help in calculating potential risk. Using scenarios, I identified problems that could occur and grouped them. Next, I calculated composite risk by defining the threats, vulnerabilities, and consequences. This risk analysis depicted where it would be most beneficial to implement controls that would serve to meet the business objectives while minimizing the risk.

In the current environment, ITCC would give one of the following responses to an employee IS query:

1. ITCC gives the correct answer for resolution.
2. ITCC gives incorrect answer for resolution.
3. ITCC does not know answer and escalates to ECS.

Obviously, the greatest risk is to be found in response #2. Expanding on response #2, I then documented the most obvious vulnerabilities and potential risk using scenarios. Each of these scenarios illustrates errors that may lead to security breaches.[4]

A helpdesk is often a common target for social engineering. In this scenario, ITCC is the intermediate target for acquiring information or access to information leading to the eventual unauthorized access to systems for purposes of compromising its confidentiality, availability, or integrity.

> Scenario #1: An ITCC agent receives a call from someone who provides just enough information to make the agent think the caller is an employee. The agent, after revealing tidbits of information the caller can use to further his/her attack, may realize that the caller is indeed an imposter, and disconnect from the caller. Even if the agent reports the call, he did not gather enough data that could be used to launch or conduct an investigation.

Probably more common is a situation akin to the following scenario where the risk is due to an unintentional error or lack of knowledge/understanding of information security policies.

> Scenario #2: An ITCC agent is assisting an employee on a technical issue and discovers that the employee is or has violated an Information Security policy. The agent may or may not make a note of his/her discovery in the call tracking system and will likely continue to assist the employee, even if rendering that service does violate policy. Moreover, the ITCC agent may not feel it necessary to inform the IS organization of the breach.

This last scenario depicts a complex situation that could potentially damage the company's reputation and financial standing.

> Scenario #3: The employee, probably not aware the answer he/she received is erroneous, perpetuates it as the "official" answer. The ECS is not aware of this query since it did not result in an escalation to them. Now let's assume the answer was needed as it relates to a strategic program the employee is driving for his organization and the delivered

[4] SANS Institute Resources "Mistakes People Make that Led to Security Breaches"

product or service is intended to be used both internally and externally. As a result, the company has developed and implemented a product that allows for the transmission of their customers' credentials including passwords, social security number, and other personal information insecurely. Worst still, the selling point of this product has been its security features.

Without elaborating in detail, Figure 3.3.2 depicts a summary of the composite risk.[5] The threat analysis is limited in scope to having the ITCC act in the role as a security gatekeeper.

PRIMARY THREAT	VULNERABILITY	CONSEQUENCE	COMPOSITE RISK
Internal "attack" – include unintentional and those committed by disgruntled employees and social engineering	• Human error (ITCC) • Improper use of technology (employees in general) • Misuse by authorized users • Inability to react quickly or appropriately	• Perpetuation and repetition of incorrect answers or errors • Potential exposure of proprietary information • Attacker to modify data or impact access by authorized persons	Med-High
External "attack", including social engineering	• Inability to react quickly or appropriately	Potential exposure of proprietary information; attacker to modify data or impact access by authorized persons	High

Figure 3.3.2: Composite risk matrix

Even as ECS was being inundated with the influx of escalations from ITCC, it served to reinforce that we needed to do more than just designate them as the front line for IS. We realized we needed to empower them to act and become security advocates and continue to build on our partnership.

"During" Snapshot

I presented to my ECS team on possible solutions, viability and evaluation of each, and recommended solution set. The team participated in a short pilot to assess the volume and types of calls the ITCC would be able to answer. I then conducted the pilot analysis and defined deliverables for the project. I also documented our

[5] Composite risk is defined by the following formula: $R = T_T + V_T + C_T$, where $_T$ = summation of the product of the (T)hreat, (V)ulnerabilty, and (C)onsequences to information confidentiality, integrity and availability.

roadmap as it pertains to collaborating with the ITCC organization and providing tools and resources to facilitate the resulting support model.

Developing Solutions

The evaluation of the current situation re-affirmed what ECS surmised when the problem first arose – that the IS organization needed to be more proactive in our engagement with ITCC. It was vital that we provide ITCC with the training and tools they needed to in order to provide effective front-line support to the corporate employees for information security. We also wanted to ensure they could recognize security-related problems and would know how to respond to them. If we were successful on this front, reducing the volume of first-level type calls we were receiving, we would then be in a better position to complete the support transition by having the ITCC group also provide front-line support for the IS mailbox.

Defining Viable Solutions

The ECS spent had several meetings to discuss possible solutions to the problem. Our goal was to identify a strategy that would serve to address the issues already identified. We evaluated each proposal and Figure 4.1.1 shows our findings based on ease of implementation or complexity, cost, likelihood of success, and residual risk.

PROPOSED SOLUTION	COMPLEXITY	COST	LIKELY SUCCESS	RISK
Do nothing – maintain status quo	Low	Low at first; High in the long-run	Low:	High: Will generate more issues
Provide a more comprehensive set of scripts	Low-Med	Med	Med-High	Low-Med
Transition front-line support of the IS mailbox to ITCC	Low	Med	High, with appropriate training	Low-Med
Define a dedicated team in the ITCC just to handle IS queries	Med	High	High, in long run	Med:
Disengage for partnership	Low	Low	Low	Med

Figure 4.1.1: Risk scenarios

We used consultative decision-making. My goal was to mitigate or reduce risk by putting controls in place.

Solution Set

I chose to implement a two-prong solution – provide more scripts and complete front-line support transition. I split the project into two sub-projects or phases. Phase I was essentially the "scripting" solution and Phase II, the transition of front-line support for the IS mailbox.

Implementing Solutions

I kicked off the first sub-project, referred to as Phase I, with a pilot to study and analyze the types of calls to the IS mailbox and to help determine where it would be most valuable to define ITCC procedures or scripts. As Phase I was nearing sustaining mode, I kicked off Phase II. In Phase II, I started with a revalidation of the success of Phase I and moved to transition front line support for the IS mailbox to the ITCC.

Overlapping Sub-projects

I previously noted that this project is two sub-projects. For the most part, many of the activities and deliverables associated with Phase I are predecessors to the start of Phase II. Near the wrap up of Phase I, Phase II is kicked off, as shown in Figure 4.2.1. The image is not drawn to scale and not intended to convey anything other than that the sub-projects overlap and are active at differing stages of the project plan. This is best illustrated when I cover the sustaining mode and next steps of Phases I and II.

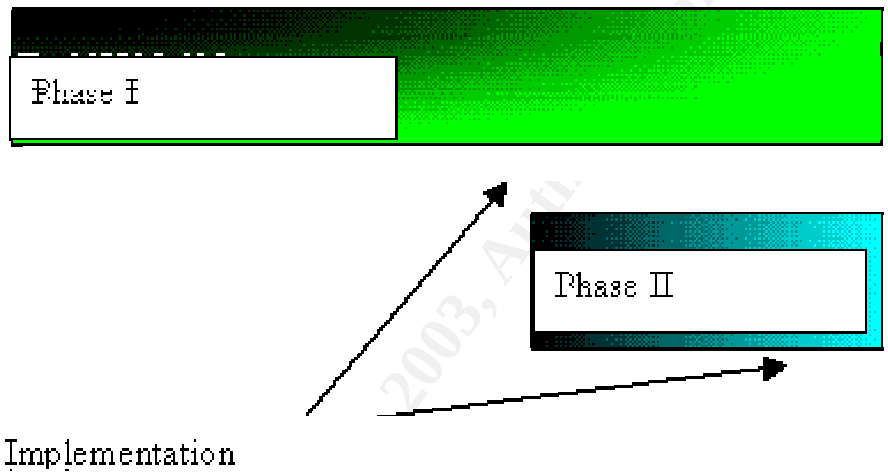


Figure 4.2.1: Phase I and Phase I sub-projects Interdependency

Phased Implementation Approach

My approach in this paper is to do the documentation in chronological order. The exception would be occur in certain instances where the project plans run in parallel with each other. In this paper, I address each sub-project separately and where there is commonality, I indicate it by referring to the project as a whole.

A core component of implementing the solutions was documenting the scripts that the ITCC would need to be successful in providing complete front-line information security support. We already had buy-in from the Customer Services organization and ITCC resources by default of their already providing IT support. As a result, I was able to focus more for Phase I on the actual planning and execution of solutions. In Phase II, because it had greater impact, I equally had to focus on getting buy-in from stakeholders.

Phase I: IS Scripting Initiative

Developing and delivering a more comprehensive set of scripts was the immediate solution. In recognizing one of our long term goals was to have the ITCC provide all front-line support for the IS organization, we wanted to better understand the types of consultation requests we were receiving and know which would be appropriate for the ITCC to handle. The IS mailbox was the best place to start.

Scripting Pilot

The ECS conducted a pilot for three months where we recorded details about the calls that came to the IS mailbox. The goal was to identify those calls that were indicative of calls the ITCC could handle as front-line consults. I led the pilot, my manager discontinued the team rotation support, and I became the sole responder to employee email queries sent to the IS mailbox. There were several reasons for the change in our mailbox support model. The key reasons are listed as follows:

- Ensure consistency in classifying calls, tracking and responses
- Remove overhead associated with the rotation

I led a small global project team consisting of three members from ECS and four members from the ITCC group. We were chartered to provide the global ITCC with IS-related scripts to support their being the front line for the IS organization. The key objectives of the first phase of the project were as follows:

- Get IS-related scripts in place for ITCC to use
- Define maintenance process for updating IS-related scripts and creating new ones
- Communicate to ITCC on scripts available and continue to re-enforce to employees that the ITCC is the first level support for information security questions

Recall, the initial set of scripts was based on the phone calls the IS organization personnel were receiving. Even through the ECS team had stated that we would continue to provide scripts for any front line support-type calls we received and dispositioned, this step was not happening on a consistent enough basis. We still were providing the primary support for queries that came to the IS mailbox, but were not tracking any data on the calls. We were intimately familiar with information security and so had not documented the process for dispositioning calls to the IS mailbox.

As the team lead, I began the legwork that would eventually serve to provide indicators by which I was able to sell to ITCC global management to complete the provision of providing front-line support for the IS organization (as noted in Phase II). I used the project team primarily as a sounding board by asking for their input on content for scripts. The role of the ITCC members was specifically to ensure the scripts were usable by them. Within a reasonable short period, I was able to group

the calls into several categories. As I answered employee queries sent to the IS mailbox, I began to document the process flow and track the calls.

I used a simple spreadsheet to track data about the email messages that were coming into the IS mailbox. A screen shot of the overall metrics, depicted in Figure 4.3.1 is indicative of the average volume of email to the IS mailbox.

Year - Qtr	Employee Termination Reports	Evaluation Requests	How Do Is	Violations & Incidents	Waiver Requests	Web Site Fixes	Other	Other - Specify	Total # of Emails*
2000 - Q3									
July ww28	1	0	0	0	0	0	0		
ww29	1	0	0	1	0	0	0		
ww30	1	0	0	0	0	0	0		
ww31	1	0	0	0	0	0	0		
Jul totals	4	0	0	1	0	0	0		5
Aug ww32	1	0	2	2	2	0	3	spam mail; FYI-notebook security; disk alert on mailbox	
33	1	0	0	0	0	0	0		
34	1	0	2	2	2	0	2	spam mail; obtain Top Secret cover sheets	
35	1	0	3	1	0	0	1	cannot open term report	
Aug totals	4	0	7	5	4	0	6		26
Sep ww36	1	0	5	1	0	0	1	How to mass email?	
37	1	0	2	2	1	0	0		
38	1	0	9	1	4	2	2	email hoax?; info on acq.	
39	1	0	10	3	0	0	0		
40	1	0	2	0	0	0	0		
Sep totals	5	0	28	7	5	2	3		50
Q3 Totals	13	0	35	13	9	2	9		81
	16%	0%	43%	16%	11%	2%	11%		

Figure 4.3.1: IS mailbox calls tracking by category

Summary:
- The IS mailbox received over 100 emails per quarter (not counting threaded messages)
- Calls initially grouped into 7 categories, (eventually expanded to 11 categories)
- Ability to now map to existing IS policies

In Figure 4.3.2, I show the breakdown of the IS mailbox call volume by categories. Key findings can be summed as follows:

- "How Do I" represented nearly half the total volume of IS mailbox calls.
- Receive queries that are not information- security specific
- The level of "Suspected Infractions" gave rise to concerns about the validity of the report and the types of infractions

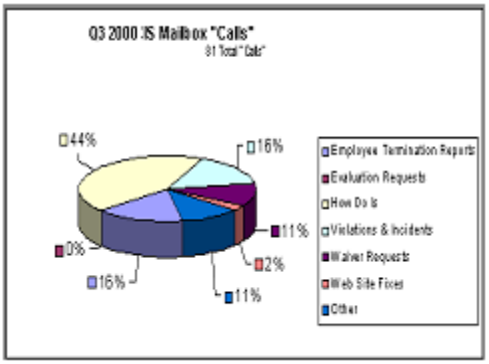


Figure 4.3.2: IS mailbox calls tracking by IS policies

My analysis revealed that there was no clear process for handling reported infractions and I needed to look more closely at the "Other" to determine if we could flush out more categories. After further examination, my analysis also revealed that the "How Do I" typify questions that can be handled by ITCC.

The plan going forward was to:

- Track call volume/analysis on a monthly basis, cleaning up the internal monitoring process
- Look at how to scale down mailbox calls to only those that need to come to the IS mailbox
- Refine process for handling emails that require re-routing within the IS organization (The ECS group was no longer aligned by corporate business units, making it more difficult to determine to whom an escalation should go)

Key Deliverables

Figure 4.3.3 is a screen shot of the project plan for the IS Scripting Initiative. Major milestones are denoted by the green italicized text. As part of the IS Scripting Initiative (Phase I), the project team defined the following key deliverables:

- Creation and review process for scripts solutions
- Procedural scripts solutions based on categories of calls
- Communication plan delivered to ITCC and employees

ID	Task Name
1	PHASE I - PLANNING
2	Project description
5	Review Project Plan with manager
6	*Project Plan defined & ratified by IS management*
7	END PHASE I
8	PHASE II - ANALYSIS
9	Levelset with team on efforts so far
12	Define business problem and opportunities
17	Define & prioritize requirements for scripts
18	*Potential scripts listing (dynamic list)*
19	Project feasibility determination
20	Define script creation/review & approval process
21	Define maintenance process
22	Communicate script creation/review process to ECS staff
23	*Script creation/review process defined & approved*
24	END PHASE II

ID	Task Name
25	PHASE III - DESIGN
26	Define IS/ITCC script engagement team
27	Set up placeholder on share for submitted scripts
28	Set up scripting process and guidelines documentation
29	Write scripts related to information security
34	Submit scripts to repository
35	Develop communication piece for ITCC personnel
36	Develop communication piece for general customer base
37	*Communication plan developed*
38	END PHASE III
39	PHASE IV - IMPLEMENTATION
40	Review and approve IS-related scripts
41	Put scripts into production
42	Add IS as a menu option on ITCC web page - How Do Is
43	Add IS as drop down menu option on solutionbase web page
44	Define & implement call metric (measures the customer experienc
45	Implement a partner VOC rating with ITCC
46	Publish communication to ITCC personnel
49	Publish communication to general customer base
53	*Communication Plan delivered to partners, customers*
54	END PHASE IV

Figure 4.3.3: IS Scripting Initiative project plan

--Script Creation/Review Process

We wanted to ensure we had a documented process by which the ECS team could use to quickly identify questions and answers that qualify to be scripted. A quick evaluation of our working environment yielded a three-prong process flow based on member role – IS Rep, IS Reviewer, and ITCC Rep.

- IS Rep: Any IS person who interacted with an employee
- IS Reviewer: The project lead (me) responsible for driving the documentation of new scripts or updates to existing ones
- ITCC Rep: Member from ITCC familiar with scripting process

Collectively, we created, approved, and implemented information security scripts for ITCC to use.

As depicted in Figure 4.3.4, the IS (business) Rep would provide an answer or work with the employee to reach a resolution and be responsible for determining if this

consult was script-worthy. In the event it was, the IS rep then had to document what that script would look like and provide to the IS Reviewer. The IS Reviewer would then work with the ITCC Reviewer to validate and begin the implementation process. Due to resourcing constraints within the IS organization, many times the best effort of the IS Rep was to note what the question/issue was and his/her response. I would then use this data to create a script.

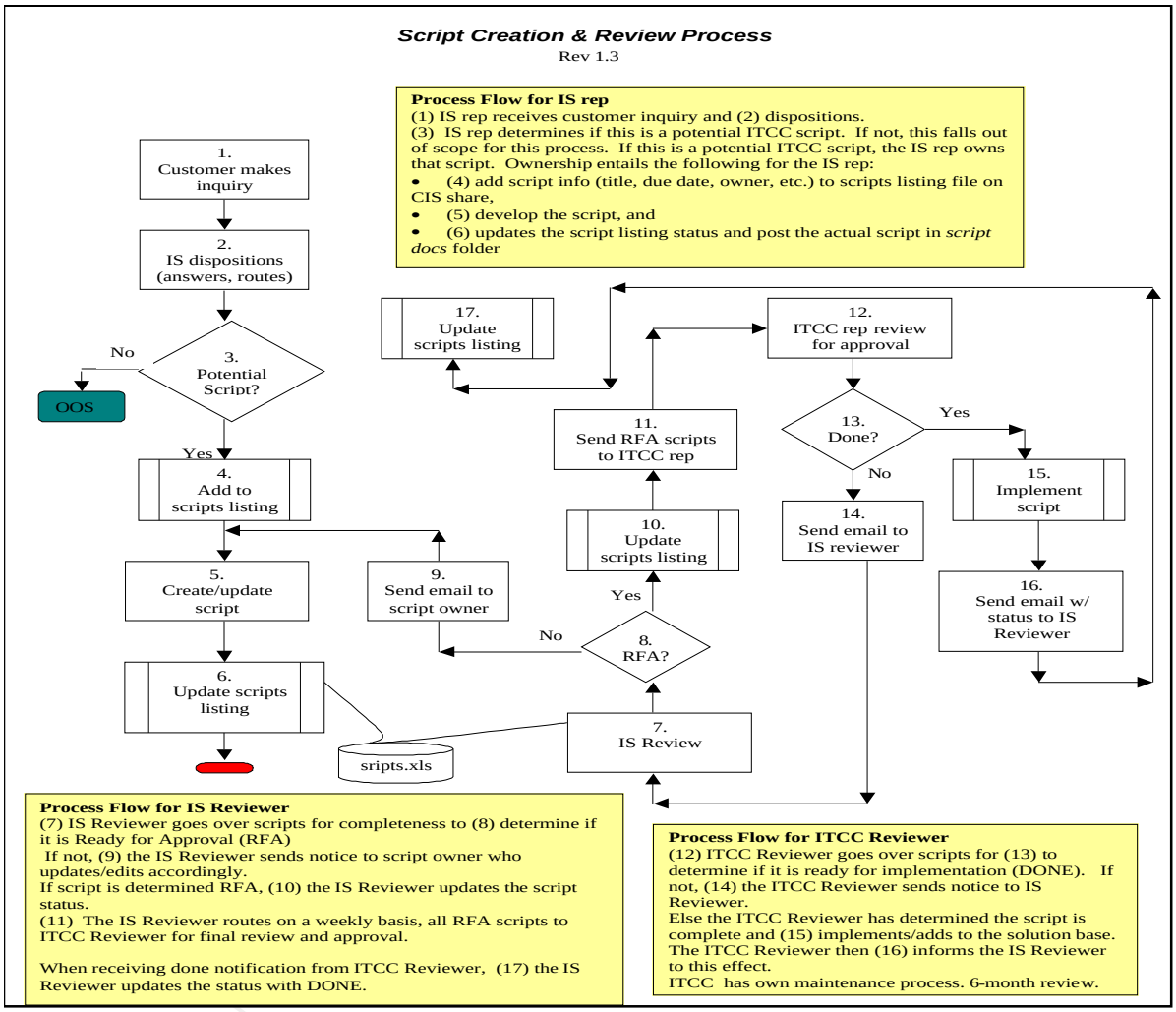


Figure 4.3.4: IS script creation and review process

--Defining Procedural Scripts Solutions

Many of the procedural scripts were defined based on the IS mailbox call type analysis. I defined at least one procedural script for each category of calls. At the beginning, seven broad categories or classes of calls were defined and they addressed many of the more basic information security questions that pertained to existing Information Security policies. We also solicited input from the ITCC teams on what information security questions they were being asked or issues they were running into as a result of their providing technical support. IS personnel also provided a listing of common information security questions and answers. At the

end of Phase I, I had defined approximately 30 procedural scripts for ITCC to help them in addressing information security calls.

As I developed scripts, it also became clear that we had to get enhancements into the ITCC call tracking toolset to accommodate the categories we had defined. Below is a summary of some of the more relevant tasks I completed as part of this project.

- *IS as menu option on the ITCC web pages and phone menus*. I worked with various business operations components of the ITCC to ensure the ITCC web pages and phone menus were updated to reflect information security as a menu option.

- *Root causes definitions.* I created the root causes and worked with the database administration group to reflect the changes appropriately in the ITCC call-tracking database. We delivered a uniform method for information security classes in the call tracking database.

- *Supporting scripts.* I created supplemental support scripts that allowed any ITCC to identify gaps and work with ECS on identifying a solution. We also put in place a process and associated scripts by which ITCC could escalate non-emergency IS issues to the IS organization. This "follow the sun" process provided 24x5 coverage and the script outlined the process for rotation handover.

- *Information Security calls metrics*. I worked with ITCC to define and implement call metrics and routing/escalation path for each script.

- *Information Security escalation queue.* This queue was to be used for re-routing or escalating any calls or issues that the ITCC could not resolve at frontline. I worked with the database owner to ensure the backend routed the escalated calls to the correct person based on region.

Various meetings and working sessions were held as a precursor to completing these tasks, the details of which are not documented here.

--Communication Plan and Delivery

Early on in the project, the team identified the requirement to communicate to two distinct audiences. IS internal communication did not require a specific structured approach and was therefore handled in the same manner as other IS internal communications. I was already closely engaged with the business operations of the ITCC group that made it relatively simply to get messages out through the ITCC management. We also had a dedicated Marketing person who worked with the IS organization on developing and delivering messages to the greater company population.

The ITCC was a key stakeholder of this project. In the early stages of this project, I conducted several brown bags meeting with the teams. In addition to regular monthly meeting with my ITCC Liaison, I was actively plugged in with the communications vehicle for the ITCC group. I leveraged this team to assist me in developing and delivering messages within the various ITCC groups. We used their intranet and provided hard copies to each of the call agents. I also presented in the ITCC staffs.

Employees, in general were also deemed key stakeholders because the success of this project would largely hinge on employees being aware of the support model changes and modifying their behavior accordingly. Here, we delivered broad messages via the IS monthly newsletter, through quarterly business meetings, and our intranet websites on the updated engagement model and ITCC's role in providing front-line support for general information security questions. The delivery of this final message to employees signaled the wrap up of Phase I.

Wrap up - Scripting Initiative

The conclusion of Phase I, Scripting Initiative was marked by the final report out to ITCC and IS management, moving to maintenance stage, and the official disbandment of the project team. The maintenance involved identifying areas for process and productivity improvements as well as maintaining the Information security set of scripts.

The IS mailbox call tracking and analysis, likewise, has been an ongoing process. Part of this included identifying areas for process and productivity improvements. For example, information security-related ITCC scripts and web site updates served to redirect customers to these places for answers. IS has looked continually to improve on how effective and efficient we are able to provide answers to employees questions as well as adjusting our processes and methods to reflect the current organization business model. Less obvious were the recommended improvements resulting from the call analysis and trending. Some examples included the identification of Best Known Methods (BKMs) and Frequently Asked Questions (FAQs) from the calls, having data to support our targeting areas where additional training or communication may be needed, and flagging gaps or where updates may be needed in IS policies. We also used the IS monthly newsletter as a vehicle to communicate specific messages and policy updates as a result.

The IS scripting initiative has been an ongoing process, even as we moved into Phase II of this project. During the interim, I have periodically added to and updated scripts. In addition, we continued with our quarterly analysis of the IS mailbox call and call types and began trending analysis after the passage of a few quarters.

At the kickoff of Phase II, approximately 45 scripts existed in the ITCC solution base and several others were in the works. As Phase I was moving to sustaining mode, I had begun the planning for Phase II.

Phase II: IS Mailbox Support Transition

Phase II of this project was to transition IS mailbox calls to ITCC for front line support. The key objectives, building on Phase I accomplishments, were to standardize on the support model across the company, play a role in increasing employee satisfaction, provide more training specifically targeted training to the ITCC, and build on existing security support within the ITCC. This phase of the project was limited in scope to the IS mailbox and did not include the ITCC providing employee support for any other aspects of IS support to employees.

At that time, the ITCC was providing a more limited level of support and we both shared the mutual understanding that we would move in the direction of having the ITCC handle all the front line support for the IS organization. And we were still providing the front line support for the IS mailbox. So again, we looked to do more detailed call analysis to determine how best to have the ITCC provide adequate and accurate front line support for the IS mailbox.

Figure 4.4.1 depicts the core tasks, deliverables, and milestones (again denoted in bold italic green) that are associated with the planning and analysis phases of this project.

ID	Task Name
1	PHASE I - PLANNING
2	Project management plan
9	*Project Management Plan developed*
10	Project and action plan
16	*Project defined & ratified by ECS manager*
17	END PHASE I
18	PHASE II - ANALYSIS
19	Analysis of IS mailbox "call" data and metrics
24	Understanding the ITCC's call handling processes
29	Re-evaluation of the IS mailbox "call" handling processes
32	*Preliminary impact assessment completed*
33	Preliminary ITCC call agent requirements and support
37	Development of proposal presentation
43	*Proposal completed*
44	Concept buy-in from ITCC management
49	*ITCC management buy-in received*
50	END PHASE II

Figure 4.4.1: IS Mailbox Support Transition – planning and analysis

Impact Assessment

One thing I want to stress here is that I spent significant amount of time on the impact analysis and proposal to management. I gave special attention to putting processes in place for the data collection and to ensuring that the data was accurate and timely. This was particularly important because ITCC was extremely data-driven and decision-making was predicated on numbers and analytical analyses.

--Support Tools & Processes

An important component in being able to determine what changes are needed to ensure continued productivity and customer satisfaction was the IS Mailbox tools and processes. The IS organization had created tools and templates to record data about the calls that allowed us to make analysis and identify next steps. We have also identified processes to streamline the dispositioning process.

Tracking and analysis of the email messages or "calls"[6] to the IS mailbox has resulted in development and addition to the IS Mailbox toolkit. The mailbox toolkit includes tools for tracking the calls and a detailed systematic process for dispositioning them. To that end, I defined categories of calls and detailed processes relative to dispositioning them.

In the initial analysis of calls, I had already determined a need to record the data in a format that will allow us to do routine, periodic analysis and call volume trending. I wanted to be able to measure those calls that are not indicative of an information security query and well as be able to map calls to the IS policy set, from which the ECS team will be then able to determine where and why we want to focus attention, for example on training, communication and awareness. I also wanted to be aware of the types of calls that required more than one touch after hitting the IS mailbox. An analysis of this data would allow ECS to provide better customer service, improve and streamline our processes, and provide better IS programs.

Previously, I used call data from Q3 2000 and needed to make revalidate findings using the current call volume and data. As part of Phase II, I conducted a preliminary assessment as follows:

- Identify process for ECS to follow when dispositioning calls to the IS mailbox,
- Map the type of calls that came into the IS mailbox into categories, and
- Draw analysis and do trending over the next two quarters

--Tracking IS mailbox calls

One of my first tasks to complete was to document the end-to-end process for dispositioning the IS mailbox calls. A part of that also required that I update the tool we were using to track the mailbox calls. What we had initially was very rudimentary and generally went unused. I opted to keep it simple and create an Excel workbook to track the mailbox calls. There was a workbook for each quarter and each workbook contained the following worksheets:

- *Overview*: Outlines components of this workbook and purpose of and how to use each worksheet. If needed, edit the email subject line and the topic here to make more descriptive. The two should match enough to allow one to easily map back to the call in the mailbox or archives. DO NOT TRACK THREADS! Any responses or follow-ups to the original message (which can span over a week) are treated as one call to the mailbox and are not tracked in the spreadsheet.

- *Daily calls Template*. Make a copy of this template and rename the copy wwXY (XY is the ww #). The template is pre-formatted; each weekday contains 20 rows. Do not modify!

[6] These terms are used interchangeably when referring to email messages to the IS mailbox.

- *Daily calls wwXY.* There is a worksheet for each workweek in the quarter; use to track each week's calls. XY denotes the workweek number.

- *CALLS mapping.* Provides snapshot view of daily call metrics. Use this sheet for your IS mailbox weekly report.

- *CALL-to-STANDARD mapping*. Provides snapshot view of category to standard call mapping on weekly basis.

The tracking was done on the *daily calls wwXY* worksheet and metrics were calculated automatically on the *CALLS mapping* worksheet using the data from the *daily calls wwXY* worksheet. A copy of the instructions that show the details of what each ECS team member would track for an IS mailbox call is shown in Figure 4.4.2.

Email topic:	Record the subject line from the email message in the topic column • If needed, edit the email subject line and the topic here to make more descriptive. The two should match enough to allow one to easily map back to the call in the mailbox or archives. • DO NOT TRACK THREADS! Any responses or follow-ups to the original message (which can span over a week) are treated as one call to the mailbox and not tracked in the spreadsheet.
Category definition:	Enter valid category only and use the 3-letter acronym (see below). Every call maps to one and only one category. DO NOT EDIT OR CREATE NEW CATEGORIES! If you think the data warrants the creation of a new category, please contact the IS mailbox owner. Broad categories are defined initially based on a 45-day sampling of the content of an IS email account. There are 11 pre-defined categories by which a call can be labeled.
Date Tracking & associated SLA:	*Date.* Record the date the call hit the mailbox, the initial response date and the date of closure. Do not record threaded messages. • Calls that came in over the weekend, after close of business on Fridays, PT are recorded in the subsequent workweek. *Response Time. The* SLA track to the Time to Initial Response (TIR) and the Time to Close (TTC), each denoted by Y(es) or N(o). • TIR (Time to Initial Response) is the date a reply was sent to the customer. The SLA for TIR is 2 business days. • TTC (Time to Close) is the date the call was closed with the customer. SLA for TTC is 3 business days

Region:	Record the region from which the sender (may or may not be the originator of the email) is located. You can use the phonebook to search on the office location. • AMR (Americas regions) • GAR (Greater Asia Region) and • GER (Greater Europe Region).
Standards & Procedures Tracking:	For each call, identify the Standard and Procedure to which it maps. • Calls in the following categories should map to Policy: CHA, EXP, HDI, INF, SER, and WAI. If not, enter GAP • Only record N/A for following categories, which do not map to Policy: ADV, ETR, FYI, NIS, and WSF
Category x Standard mapping:	Use the category code and the Standard number in the format <code>#<standard number>. • For example, to denote a How Do I that maps to Standard 3 record the following: HDI#3. This data is used in the CATEGORY-to-STANDARD mapping worksheet.

Figure 4.4.2: IS Mailbox Call Tracking Requirements

--IS mailbox call process flow

The IS mailbox end-to-end call tracking dispositioning process is the detailed process for addressing various types or categories of IS mailbox calls. End-to-end, the process itself is relatively simple.

Steps 1 and 2: Message comes in and the system sends an auto-reply to the sender.

Steps 3 and 4: Label and disposition the call; track the call data. These two steps are the core of the process and Figure 4.3.2 covers Step 3 in more detail. I covered Step 4, tracking in the workbook, already in the previous section.

Step 5: If applicable, roll up FAQs

Step 6: If applicable, validate contacts (recipients of the Employee Termination Report)

Step 7: Send reminder to next monitor (member of the ECS team)

Step 8: Generate weekly report

Each call fits in exactly one category. As such, each call can be answered based on the category in which it fell. Step 3 covers call categorization and dispositioning:

1. Assign category to the email message using one of the eleven pre-defined categories. As a catch all, there is a temporary category to identify calls that do not fall into any of the other 11 categories.

2. Clarify the email subject where warranted. We want to make sure the email subject line is clear and descriptive of the message.

3. Disposition call based on category. For each category, there is a process to follow for answering the call. The diagram shows the modularity, where each category has a sub-process associated with it.

As shown in Figure 4.4.3, this high-level overview of the end-to-end process flow is intended to depict the processing from reception to closure.

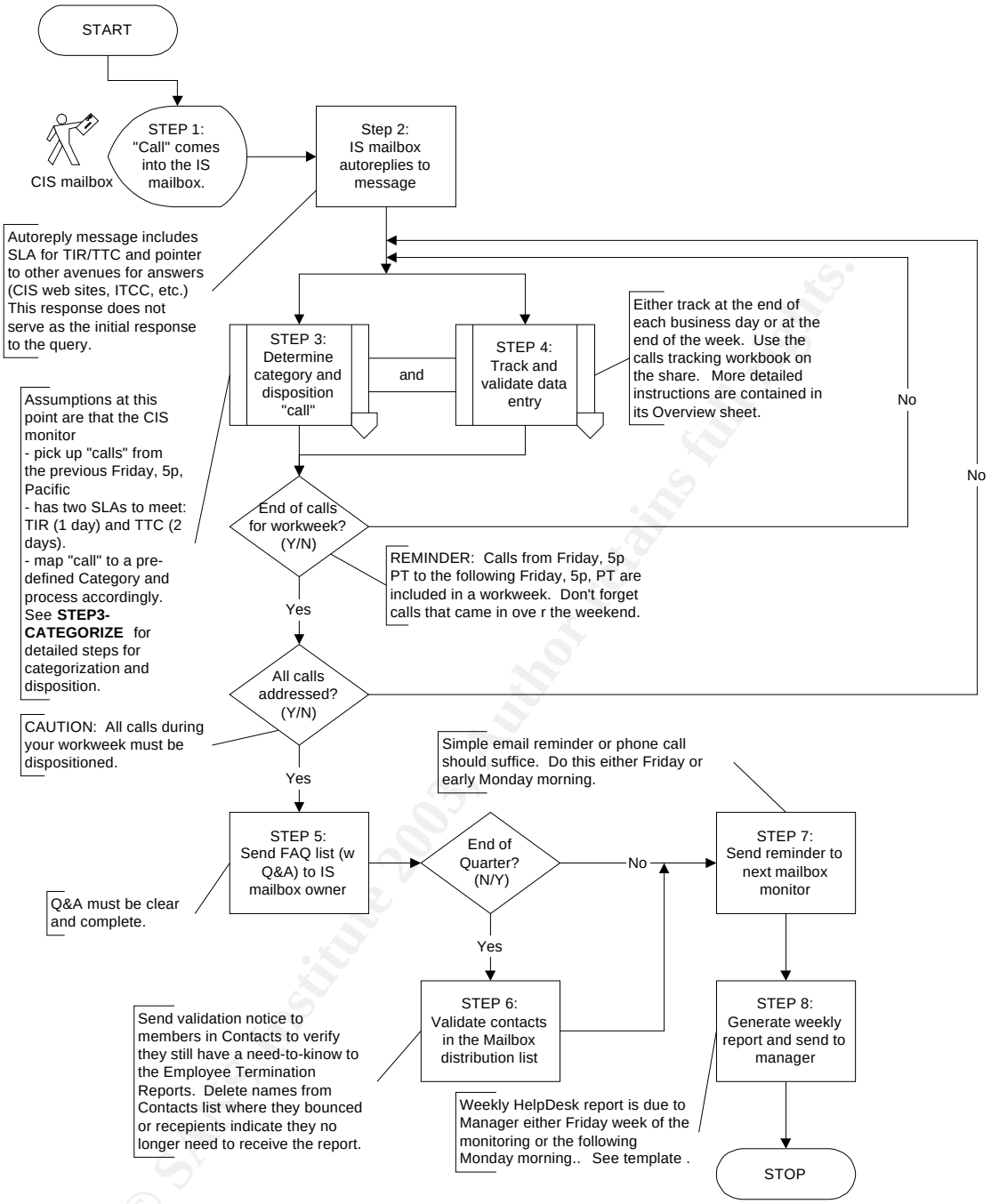


Figure 4.4.3: IS mailbox call dispositioning process flow overview

Again, in part for brevity, I did not include details of the twelve sub-processes in this paper. These sub-processes, in turn, were more flowcharts that got into the details of actually dispositioning a call Suffice it to say, I knew that we were well armed with the appropriate tools and a detailed process to allow anyone to step in and provide coverage of the IS mailbox, as illustrated in Figure 4.4.4.

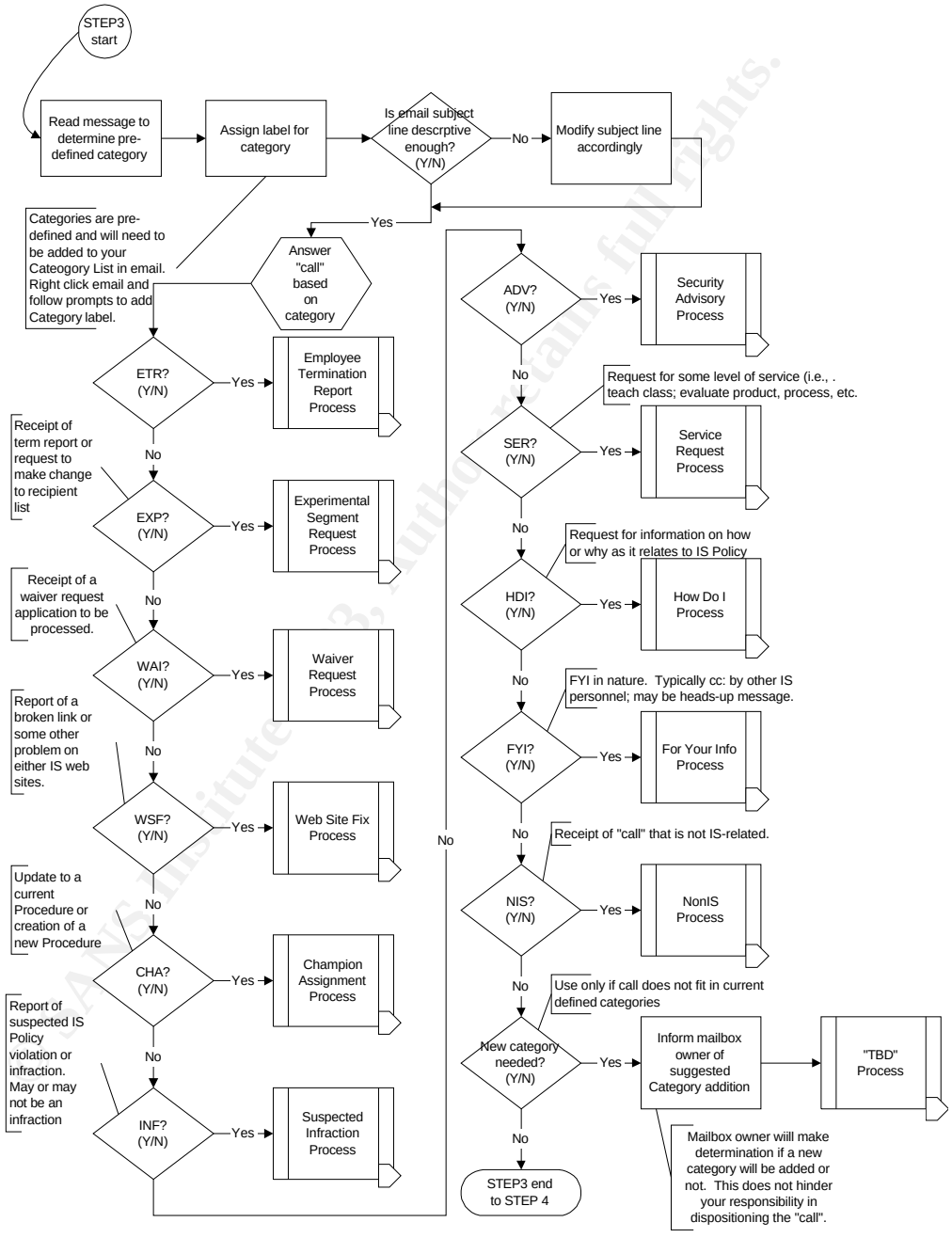


Figure 4.4.4: IS mailbox call dispositioning process flow for categories

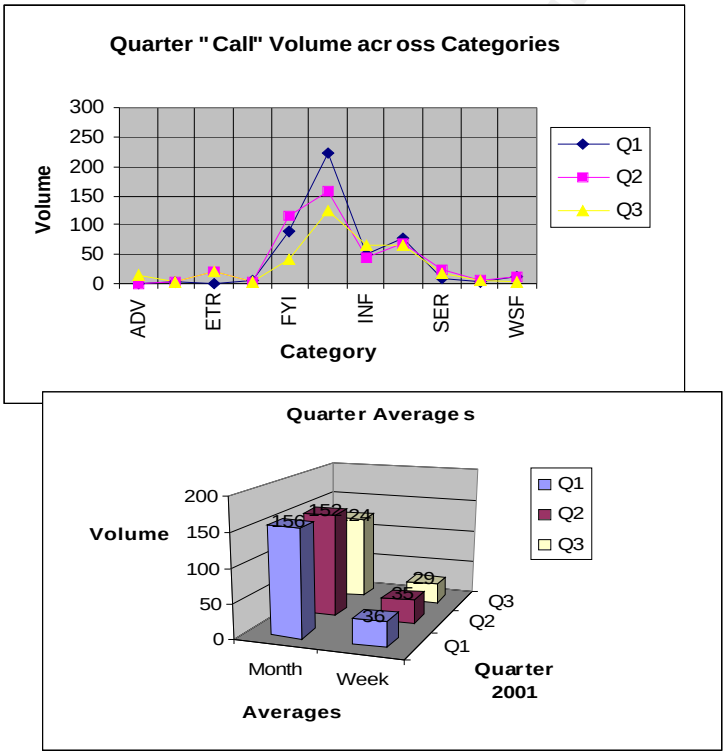
It was pertinent that the process be clearly defined and adhered to. As a result, I gave several presentations to the ECS team on the tools and the process to ensure that the toolset was comprehensive, concise, and complete. The next step was to do a trend analysis to determine if it still makes sense to have the ITCC provide front line support for the IS mailbox.

--Trending Analysis

Right now, the ITCC provides partial front line support for the IS organization. And that was by design. When the IS organization first approached the ITCC to provide first level support, we know that this would be an always refining process. The ECS team was still providing some first level support through its IS mailbox. Recall also that the bulk of the initial set of IS scripts were defined based on calls to the IS mailbox. Since then, additional scripts have been defined and modified based on calls to the IS mailbox, ITCC feedback, and changes to the IS policy set.

The purpose of the trending analysis was to provide metrics on what type of calls were indicative of front line support. My analysis at this point was focused on identifying what volume of the IS mailbox calls the ITCC organization would be able to successfully handle. A key assumption was that we would provide the necessary scripts to facilitate their being able to disposition these calls.

My key findings are illustrated in the screen shots shown in Figure 4.4.5.



The first chart shows the call volume for each quarter across the 11 pre-defined categories and the second, the average monthly and weekly call volume for each quarter.

The data shows the following:

- How Do I has the highest volume of calls across all the quarters and that those categories noted as requiring escalation, have the lowest call volumes.
- The call volume has steadily decreased over the quarters since Q1.

Figure 4.4.5: IS mailbox call volumes and quarterly averages

I completed an analysis of the numbers over three quarters. Trending data is shown in the graphs in Figure 4.4.6. My findings were conclusive, showing the following:

- Calls indicative of ITTC 1st level fall in the categories "How Do I", "FYI", "nonIS", and "Employee Termination Report". Collectively, this represents on average no less than 74%.

- Calls indicative of ITCCC 2nd level fall in the categories "Security Advisory" and "Infraction". Collectively, this represents on average no less than 14%.

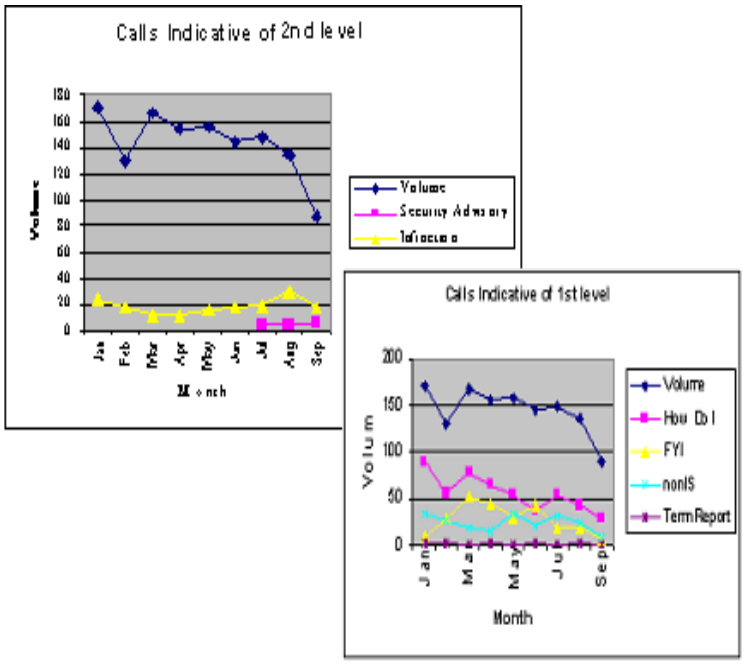


Figure 4.4.6: Call volume indicative of ITCC front-line support

Total volume on average was on the decline. This was an important selling point to ITCC management because they were concerned about what was true normal volume and the time associated with dispositioning IS mailbox calls.

Obtaining ITCC Management Buy-in

Based on findings from the trending analysis, I documented a proposal and strategy document. I knew that the key to getting ITCC management approval of having ITCC take over providing front line support for the IS mailbox was to provide accurate and comprehensive data and metrics that would speak to the potential impact to their business model. I had already been working with the US-based ITCC manager, whose team would be the group to provide that front line support for the IS mailbox. His participation was invaluable in that he was able to tell me what aspects of the proposal and strategy could be potential roadblocks or showstoppers.

A key practice for making security partnerships work is to know your partner's business. In CSO Magazine, Bill Bono, Motorola's CISO, noted in that there are four key ingredients for successful security and strategic schmoozing:

> "Understand the business, understand what makes it successful, identify the factors that can put that success at risk, and then find ways of managing that risk through technical, operational or procedural safeguards."[7]

[7] Hancock, http://www.csoonline.com/read/090402/talk.html

The next step was to obtain buy-in from the global ITCC management board making the presentation to the overall ITCC management board. In my presentation to the ITCC management, I gave an overview of Phase II of this project with its objectives and presented my findings, all of which are documented above. In addition, I also had to illustrate that their taking on this new business did not significantly affect their current business model. Here is where all that process documentation work comes into play. From it, I was able to draw out several factors, opportunities and solidify my recommendations and subsequent benefits.

Key factors that I spoke about include the following:

- The ITCC was expected to be the VOC (Vendor of Choice) driver for the IT organization. This represented a key component of customer satisfaction based on the notion of "one-touch" resolution.

- The ITCC currently provides first-level support for IS organization and if provided with the appropriate scripts, come quickly do that more comprehensively.

- The ITCC team that handled the employee email queries had a business model similar to the one we employed for dispositioning the IS mailbox calls.

- We had a very good working relationship. As the IS Liaison to ITCC, I had been an active participant in nearly all their business projects. Likewise, my peer counterparts in the GAR and GER regions were providing similar support to their respective local regions.

--Similarities of Call Tracking Tools

In many ways, the IS mailbox call tracking is similar to how ITCC tracks their calls. Figure 4.4.7 shows a comparison of the type of data tracked. The core difference is the tool used to track and retain the data.

Service Request:	Received via phone, web interface or email	IS mailbox - (email only)
Tracking tool:	Recorded and tracked in the ITCC call tracking database system.	Recorded and tracked in Microsoft* Excel workbook. This includes only those requests sent to the IS email account.
Data Recording:	• Detailed Employee Data • Request Detail • Assignment • Resolution Data	• Employee Region (require email for name) • Request Detail –found in subject line

		• Assignment – Mailbox monitor • Resolution Data - Includes call receipt date, IS response date and IS closure date
Call Classification:	Category/Application/Root Cause "Infosec" already defined in the call-tracking database.	Have 11 pre-defined categories based on call type. Map to Root Cause

Figure 4.4.7: Call Tracking Model Similarities with ITCC and IS mailbox

--Indicators

I defined the following indicators to measure project-against-schedule (PAS). These were based off the major deliverables.

- Project: No less than 10% difference between actual and baseline project plan
- Training: 100% of ITCC personnel dedicated to support the IS mailbox are trained; 100% of ECS group receive Escalation Support training
- Scripting: >=1 script for each category/root cause; 90% of IS mailbox scripts implemented and usable

I felt confident that given the proper tools and training, the ITCC could successfully resolve no less than an average seventy-five percent of the IS mailbox calls and quickly move to an eighty-five percent resolution rate. In determining the volume of calls that would be escalated to ECS, I also defined a success indicator of 80% escalation resolution within time-to-close.

--Recommendations and Benefits

I concluded my presentation with a brief list of recommendations and outlined the benefits both to the ITCC and the IS organization. The obvious core proposal was to land the front line support for the IS mailbox in ITCC. To facilitate that support, I would work with that ITCC team to define and provide scripts to mirror the end-to-end IS mailbox call dispositioning process. We would phase in their taking the front line as I worked with ITCC to establish service level agreements for the front line support and the IS escalation support. We would also provide specialized information security training to ITCC. We also agreed to take the lead in driving any necessary communications to ITCC.

Below is a summary of the benefits I expounded as part of my proposal presentation.

- More and consistent information security training
- More efficient process for providing security-required solution to a growing increase in information security-related queries, equating to a more comprehensive set of scripts and optimization of employees time

- Provide copy exactly process, equating to savings in money and time

We want to support ITCC on being better educated about information security policies. This would allow ITTC to do a better job in supporting their customers. In light of the recent virus and worm crisis, it is more imperative and certainly more obvious that we all are custodians of information security. And for IT, that means providing ITCC with the tools needed to facilitate success on that front. We want to build on having the ability to have an even better response to viruses and worms in the wild and even individual incidents. Our front line support needs to be knowledgeable about information security. And this lays the groundwork for that.

--ITCC decision on proposal

At the conclusion of the presentation, the ITCC management board gave the unanimous support of this proposal, provided resources from their group to participate in the project, and gave recommendations on approach. A project team was identified and I began finalizing and implementing the project plan.

The ITCC management board expressed two concerns. The first was with their group taking on this additional responsibility without additional funding.
The last concern was with some of the members belief that the IS processes as implemented within their regional ITCC teams were not consistent across the company. I successfully closed on both of these concerns within a couple of weeks. In the end, ITCC agreed to take on the additional work without additional funding primarily because of the strong relationship we had and the benefits far outweighed their not taking on this new business. For the latter issue, I was already working on a separate project with a new started cross-site/region/functional team within the ITCC who was responsible for ensuring the IS policy set were adhered to in a consistent manner across the ITCC organization. Likewise, the ITCC was moving to a "follow the sun" support model, similar to what we were already providing to them in the way of escalation support. Overall, ITCC management was enthusiastic about the opportunity to learn more about information security and becoming the one-stop shop for initial engagement with the IT organization.

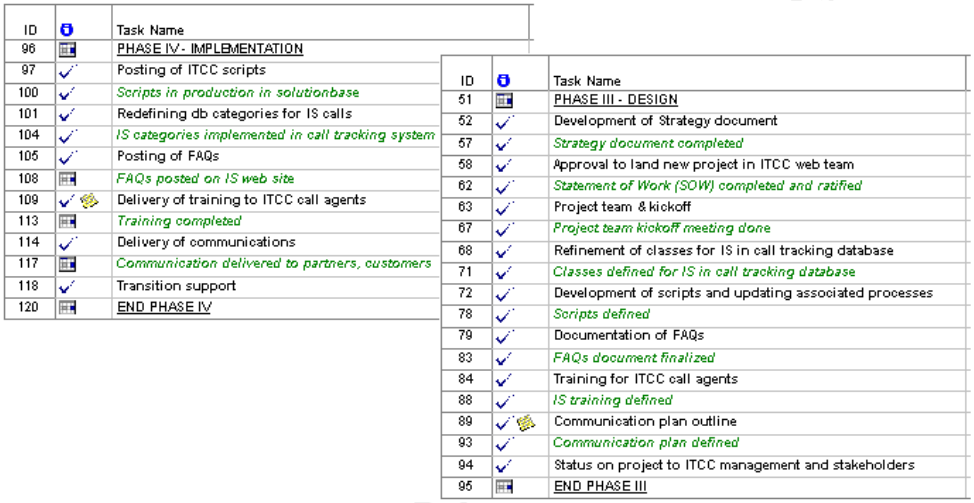
As part of the follow up, I completed the necessary paperwork to include a Statement of Work and Service Level Agreement. Much of its content came from the previously documented data, findings, and strategic direction. I had successfully sold the ITCC management on the IT Call Center being empowered to disposition information security questions and issues.

Key Deliverables

This IS mailbox project was a collaborative project between the IS organization and the ITCC. Members on the ITCC side were representatives from the various global ITCC teams, the ITCC web administrator, and the call tracking database user group. The IS members were a subset of folks from the ECS team and included representation for training and awareness and policy.

Figure 4.4.8 show the high level project plan for implementation and design of the IS Mailbox call Transition project. Again, the major milestones are depicted in bold green italics. Key deliverables of this project included:

- Scripts and processes for IS mailbox support
- Delivery of communication plan
- Specialized training provisions for the ITCC
- Successful transition of front line support to ITCC



ID	Task Name
96	PHASE IV - IMPLEMENTATION
97	Posting of ITCC scripts
100	*Scripts in production in solutionbase*
101	Redefining db categories for IS calls
104	*IS categories implemented in call tracking system*
105	Posting of FAQs
108	*FAQs posted on IS web site*
109	Delivery of training to ITCC call agents
113	*Training completed*
114	Delivery of communications
117	*Communication delivered to partners, customers*
118	Transition support
120	END PHASE IV

ID	Task Name
51	PHASE III - DESIGN
52	Development of Strategy document
57	*Strategy document completed*
58	Approval to land new project in ITCC web team
62	*Statement of Work (SOW) completed and ratified*
63	Project team & kickoff
67	*Project team kickoff meeting done*
68	Refinement of classes for IS in call tracking database
71	*Classes defined for IS in call tracking database*
72	Development of scripts and updating associated processes
78	*Scripts defined*
79	Documentation of FAQs
83	*FAQs document finalized*
84	Training for ITCC call agents
88	*IS training defined*
89	Communication plan outline
93	*Communication plan defined*
94	Status on project to ITCC management and stakeholders
95	END PHASE III

Figure 4.4.8: IS Mailbox Support Transition – implementation and design

--IS Mailbox Support Scripts

Creating the scripts for the IS mailbox support was relatively simply because I had already documented the end-to-end process flow. I also reviewed all the existing IS-owned and other information security related scripts to identify those that needed to be updated to reflect procedures for handling if the call was received via the IS mailbox. In developing these scripts, I worked directly with a member of the ITCC team that would be responsible for the front line support for the IS mailbox. His role was to ensure that what I scripted was doable on the ITCC's end.

It is worthwhile to note that several key things came out of this scripting endeavor.

- *Creation* of *end-to-end document on IS mailbox support.* This document addressed the complete process flow and other requirements as it pertains to the emails in the IS mailbox. This included a core How Do I script because so many of the information security scripts came out of that category. Also, ITCC wanted to have the ability to quickly access all the information security related scripts.

- *Defined standard root causes.* They root causes are equivalent to the categories for the email messages. For each call, a root cause is identified in the call-tracking database. In our processing model, the root causes are used to determine how the call is dispositioned.

- *Implementation of "Follow the Sun" process within IS organization.* The IS organization, namely the ECS and it's counterparts in the non-US regions, committed to providing nearly 24x7 escalation support for non-emergency information security issues. We already had a process in place to handle emergency information security escalations. This was no small effort since it involved all corporate regions. However, the resulting process was simple: the escalation was routed to the region that was in its normal business hours regardless of the origination of the consult in ITCC.

--Streamlined end-to-end Call dispositioning Process Flow

Over the life of the project, I made enhancements to the process. In the previous version of this process flow, there were eight core steps. Here, as shown in Figure 4.4.9, the end-to-end process flow is streamlined. .

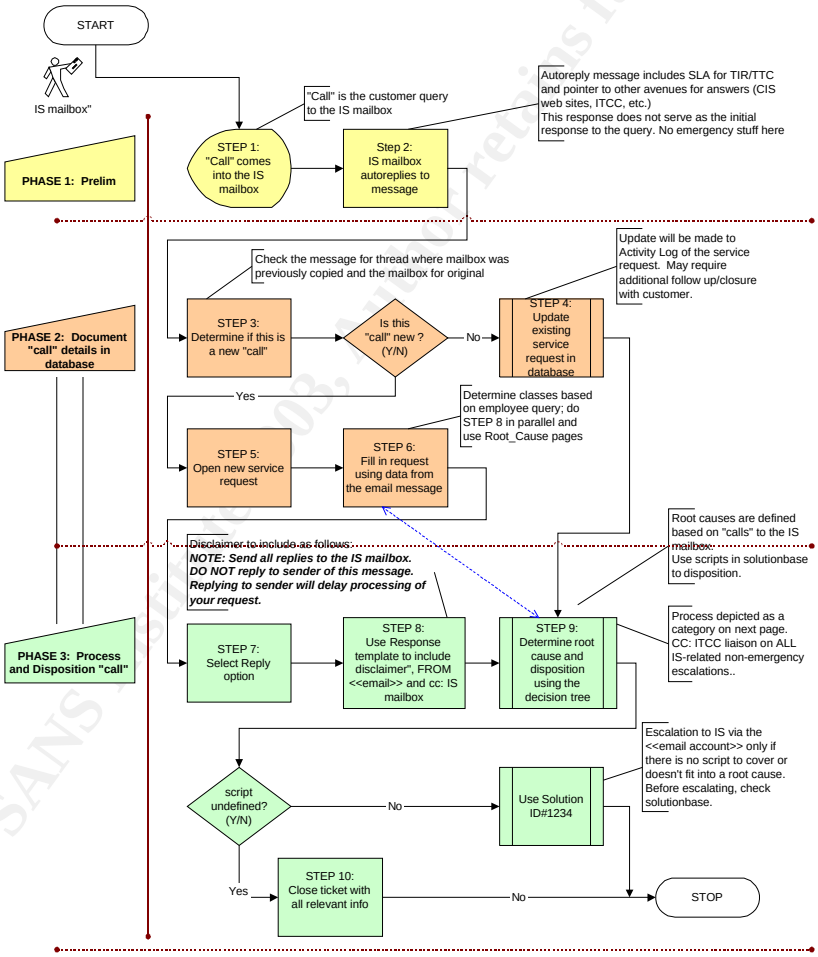


Figure 4.4.9: End-to-end streamlined IS mailbox call dispositioning process

This overview flow depicts the end-to-end process flow for dispositioning customer queries to the IS mailbox. The decision tree is a sub-process that provides the detailed process flow based on pre-defined root causes. The more detailed flow

delves into identification of the IS root causes and the actual scripts to facilitate handling the call.

The flow process is further broken down into phases. The phases are distinguished along the lines of action types. The prelim (Phase 1) requires no action from the ITCC agent. The call documentation phase (Phase 2) pertains to recording the employee query in the call tracking database. Call disposition (Phase 3) delves into the actual processing of the employee query and comprehends guidelines on responding via email.

The root cause process is detailed enough that I am not able to sanitize it without distorting its usefulness. Suffice it to say, for each category or root cause, I have defined at least one script. In many instances, a particular category may have several top-level scripts and a few multiple-layers ones.

Another offshoot of delivering scripts was the establishment of service level agreements (SLAs). Previously in working with my ECS team, I defined response times based on the date the call was received. Recall that SLAs were established for Time-to-Initial-Response (TIR) and Time-to-Close (TTC). The IS organization had been successful in that we have met our response time over 90% of the time and closure time nearly 100% of the time. Our already established SLAs were in accord with those that existing for the ITCC team who managed general consults via email. I did not make any significant modifications here.

--Communication Plan and Delivery

We already had a clear, defined path by which to deliver the messages in a timely fashion to the ITCC organization. In addition, I also created an intranet web site specific for the ITCC group that was providing front line support for the IS mailbox. We used this web site to record BKMs and post any other supporting IS mailbox documentation that did not lend itself well to being documented in an ITCC script.

--Security Training for ITCC

I then spent approximately two to three weeks preparing for and delivering the training to those ITCC personnel who would be providing the front line support for the IS mailbox. Common to my training sessions were the focus on ensuring the processes were complete and the scripts were actually usable. We used live data, that is, did the training using actual emails in the IS mailbox.

In addition to the requirement to complete annual security training, the IS organization was looking at delivering specialized training to the ITCC. We had begun discussions of various topics to include social engineering, handling infractions and being more proactive in handing information security queries.

--Transitioning Front Line Support to ITCC

I was now ready to make the official transition of the front line support for the IS mailbox to the ITCC team. The training was completed and success. Scripts were in place and testing showed they were usable; other processes documentation

likewise had been finalized. To facilitate a smooth transition, we started with frequent meetings between the ITCC and me to assist in immediately addressing any roadblocks or issues. With the passage of time, ITCC became more confident in addressing the IS mailbox emails and we met less frequently. We settled on bi-weekly meetings, when necessary.

Wrap up - Mailbox Support Transition

The conclusion of Phase II, Mailbox Support Transition was marked by the official transition of front line support to ITCC, the start of continuous process improvement meetings with ITCC and moving to maintenance stage. The maintenance involved identifying areas for process and productivity improvements as well as maintaining the Information security set of scripts for the IS mailbox.

I started a Continuous Process Improvement (CPI) Task Force that served as a quasi-maintenance team as part of the Phase II wrap up. Our primary focus was to ensure that we proactively looked for ways to continue to improve the processes, tools, methods, and solutions used for the overall IS mailbox support. This team was much smaller, consisting of 4 members maximum and over time, there has been a lot of rotation on the ITCC side. We started meeting frequently for the first few months and then as time passed, our meeting frequency tapered to once a week if needed.

Continued maintenance yielded further refinement of the IS mailbox call dispositioning process, simplification of existing and creation of new IS mailbox support scripts, and a distinct escalation process. Again, specific BKMs that did not lend themselves well to scripts were developed as part of keeping the business running. At the end of Phase II, approximately 60 scripts existed in the ITCC solution base; today that number is even higher.

"After" Snapshot

Both the IS Scripting Initiative and the IS Mailbox Support Transition projects resulted in significant changes to the ITCC and IS business operation models. Recall, that the overall strategy was to have the ITCC provide complete front line support for the IS organization. I had successfully provided them with scripts based on consultation we were providing to employees or feedback from ITCC on information security queries they were receiving or information security issues they were running into as part of their normal business operations. We completed that circle by then moving the front line support of the IS mailbox to ITCC. At the same time, I had already started to standardize on solutions from Phase I and had begun to do the same for Phase II.

Standardizing Solutions

Many of the solutions as they were implemented, were on their way to being standardized. This is partly due to the dedicated focus upfront on the processes side. That meant that the skills, tools, and methods were already intertwined or

comprehended as I documented the associated processes that would ultimately put ITCC in a position to be and act as information security advocates.

Sustaining for Phase I

The core solutions out of the Scripting Initiative – processes and procedural scripts for handling information security queries and issues – became standards. The ITCC organization already had the necessary skills, tools, and methods in place. I was able to build the additional processes and scripts and plug them into the already existing support infrastructure. Once published, the scripts instantly became the methods for addressing that particular situation. Training had been delivered and the ITCC was made aware of the existing scripts, how to submit changes to the process or scripts and report gaps or issues with the scripts themselves. The content management system that housed the scripts automated the change process. ITCC and others who had authorized access to the set of IS-owned scripts could subscribe to them to receive automatic notifications of changes and submit change requests that would be automated sent to me for review/approval. Likewise, I could make immediate updates and submit new scripts.

One prime example of the standardization had to do with how we wanted the ITCC to handle infractions such as account sharing. We implemented the script and documented in the IS policy set a procedure that served to re-enforce this action. I also worked with ITCC to create a web-based form for automatically reporting the infraction to the IS organization, and documented a follow-up process that also included engagement with the legal and HR departments if warranted.

It is worthwhile to note also that the ITCC used the IS one-stop process as a BKM when they moved in the direction of becoming a true one ITCC shop. In their case, it was more focused on the how the various teams handled and re-routed service requests that were being processed or needed to be processed continuously as opposed to keeping it within the same team or region of origin.

Sustaining for Phase II

The solutions out of the IS Mailbox Support Transition were more of the same but specific to the support of the IS mailbox. In addition to leveraging the skills, tools, and methods already in place, I started a Continuous Process Improvement (CPI) Task Force. In a way, you can view this as the maintenance team after the wrap up of the IS Mailbox Support Transition project. Our primary focus was to ensure that we proactively looked for ways to continue to improve the processes, tools, methods, and solutions used for the overall IS mailbox support. This team was much smaller, consisting of 4 members maximum and over time, there has been a lot of rotation on the ITCC side. We started meeting frequently for the first few months and then as time passed, our meeting frequency tapered to once a week if needed.

Determining Next Steps

For each project, I held post-mortem meetings to evaluate our success against the projects' objectives. In disbanding the project teams, we also identified what the maintenance/support model would look like. I already covered the wrap up for each of the sub-projects. Here I will address the success criteria for the overall project and strategic direction with ITCC.

Success Criteria

Overall, the projects goals were met. The project was completed in accordance with its scheduled timeline with no major slippage. Training was successfully delivered and the dedicated ITCC call agents felt confident they could step in and get up to speed in providing front line support for the IS mailbox. The ECS group, likewise, received training on the Escalation Support model and processes. Because the scripts went through a rigorous review process, they were usable and at most required minor, cosmetic updates after being implemented.

Strategic Direction

My strategy in this project was to have the ITCC provide front line support for the IS organization. In the proposal to ITCC management, I also painted a mural of our strategic partnership. Core to them was the plan for more focus on training. At the time of the proposal presentation, the IS organization was in the process of implementing information security training targeted to IT. The ECS team was also actively working with ITCC teams who were likewise delivering targeting information security training to the call agents about adhering to the IS policy set. We also encouraged ITCC to do train-the-trainer (TTT) that after successful completion would allow them to teach that respective IS course. In addition, we were doing the project planning to deliver social engineering training to the ITCC group.

More than the proposed programs themselves, we conveyed that we were building and maintaining our partnership. In addition to maintaining our level of commitment to participate or provide consultation on their programs, we also shared the opportunity with the ITCC to participate in a security users group we were spearheading through the organization.

Impact

I was able to significantly raise the level of information security awareness in ITCC and empower them to be security advocates using my skills in processes methodology, security expertise, and clear understanding of their business model. ITCC has stretched beyond the convention bounds of just providing reactive support to the company employees to having a healthy level of paranoia when it comes to information security.

State of (Enhanced) Security

As noted by in Douglas Ridgeway's "Making the HelpDesk a Security Asset", an organization's helpdesk can be a proponent of information security.[8] Enabling our ITCC to provide front line support for information security resulted in an enhanced state of security for the company:

- Standardized on complete front line support model for information security. This included the ITCC having the ability to escalate information security issues discovered during their routine day-to-day troubleshooting.

- Spearheaded productivity improvements in both the IS organization and ITCC by providing more accurate and complete set of information security scripts and enhanced information security training

- Leveraging the ITCC expertise in front line IT support allowed IS to provide better information security service because we were now focusing less time on a smaller subset of front-line types of calls and able to run more strategic programs and projects

- The CPI Task Force was in a position to offer pro-active solutions in an environment that is historically known for reacting to information security inquiries and issues.

In addition to these basics, ITCC is in a better position to role model information security. The ITCC has been receiving an increased number of queries about information security since the implementation of this project. The call agents were also seeing and reporting an increased # of issues as it pertained to infractions, such as account sharing, possible social engineering tactics, and inappropriate access, against the current information security policies. The ITCC has become more engaging in the review of proposed changes o the IS policy set and interpretation of policies. They have enhanced the level of security by leading a project to automate the network password reset and distribution process and are active in raising the security awareness by teaching information security classes across the company.

Project Team Recognition

I received recognition from the IS organization on my success with these two projects. I also presented similar awards to the core members of both the project teams during their respective ITCC staff meetings. Recognition included monetary awards, gift certifications, and wall plagues.

[8] Ridgeway, http://rr.sans.org/securitybasics/helpdesk.php..

Conclusion

When you think about information security, the primary schools of thoughts usually fall in the policy space or the technical solution space. Providing policies in and of itself does nothing to provide a means to measure its effectiveness or to ensure compliance across the organization. Deploying security technologies such as Intrusion Detection Systems (IDS) or tools to ensure compliance, such as using a password generation tool to ensure the password created adheres to the requirements identified in the policy, do not complete the information security picture. This is not to say that the implementation of information security policies or technical solutions does not have value. However, the identification of policies and procedures are not sufficient to ensure we exercise due diligence. Similarly, the implementation of technical solutions is not the panacea to all information security problems. It is clear that creating a policies or applying technology to a security problem alone cannot completely solve it. With all the advances in IT and the tendency to automate where possible, the glue that holds it all together comes in the form of the associated processes, particularly as it relates to the human element of information security.

You have heard that the strength of your security (program) is only as strong as its weakest link. You have undoubtedly heard also that technology is not a panacea to all security ills. According to Jason Levitt, the key to good security is sound business practices and does not necessarily lie in more technology.[9] Too often, we will define information security policies, standards, and procedures and then implement technical solutions to facilitate the enforcement of those policies, standards, and procedures. Yet, we may not recognize the value in targeting awareness and training to the ITCC personnel as a vital component in combating the never-ending war of protecting the company's information assets from compromises to its confidentiality, integrity, and availability. Security is an ongoing process that involves not only technology, but people and processes too. The IS organization has come to rely on ITCC to help raise the awareness of information security policies and serve as watchdogs as they interact with employees across the company. I was successful in empowering ITCC as security advocates.

[9] Jason Levitt, pp. 67-8, 72

References

Carr, Jim. "Thwarting Insider Attacks". Network Magazine. September 2002. pp. 42—6.

Duffy, Daintry. "The CSO's Guide to Strategic Schmoozing". CSO Magazine. September 4, 2002. URL: http://www.csoonline.com/read/090402/talk.html (October 11, 2002)

Levitt, Jason. "Security – The Enemy Within". Information Week, Apr 23, 2001. pp. 67-8, 72

McClennan, Chad. "Call Center 'Musts': What VPs Should Know.,.." Market Trends, CRM Community. URL: http://www.crmcommunity.com/news/article.cfm?oid=6EF3717D-D460-480A-B440EA9391F8CA18. (October 11, 2002).

Ridgeway, Douglas. "Making the HelpDesk a Security Asset". SANS Reading Room. October 22, 2001. URL: http://rr.sans.org/securitybasics/helpdesk.php. (October 24, 2002).

Shipley, Greg. "How Secure Is Your Network". Network Computing. November 27, 2000 (2000): 58-72.

Sullivan, Brian. "Getting Hurt by What You Don't Know". Computer World. January 11, 2002. URL: http://www.computerworld.com/securitytopics/security/story/0,10801,67319,00.html (October 11, 2002).

CISSP Common Body of Knowledge Review Seminar, Copyright 1995-2000. "Security Management", p. 12-44 (foil #33-38).

SANS Institute Resources "The 7 Top Management Errors that Lead to Computer Security Vulnerabilities". URL: http://www.sans.org/newlook/resources/errors.htm (November 17, 2002)

NOTE: All figures, unless noted otherwise, are taken from materials I created and owned.