

CERIAS Tech Report 2007-91

Security Education, Training, and Awareness from a Human Performance Technology Point of View

by Melissa Dark

Center for Education and Research

Information Assurance and Security

Purdue University, West Lafayette, IN 47907-2086

Security Education, Training, and Awareness from a Human Performance Technology Point of View

Melissa J. Dark

Introduction

This chapter focuses on the role of training, education, and awareness (TEA) in an organization's overall information security strategy. A major premise of including this chapter in the book is that information security is about more than technology; it includes people and process as well as technology. In fact, the 'people' piece of the security puzzle is perhaps the most critical for several reasons.

Information security incidents continue to rise. More people are using more information technology for more tasks and this trend is expected to continue. Information technology is becoming more sophisticated and complex, yet in order to market products to lay users, vendors are creating applications that are seemingly easy to use. The ease of use often masks security issues and concerns. The lack of understanding of security issues coupled with the pervasive and growing use of computers by the general population makes people a critical factor in the information security equation. In most organizations, novice or lay information technology users range from the receptionist to the CEO. These individuals are prime targets for information security breaches because of their lack of understanding the technology and associated threats and vulnerabilities.

Organizations need security training, education, and awareness because many times the first line of defense is the human line of defense. Human beings are an essential part of the prevention, detection, and response cycle. Knowledgeable human beings can better prevent information security breaches that occur due to negligence or accident as well as to breaches that stem from malicious activity. Knowledgeable human beings can detect malicious activity of other human beings as well as anomalous behavior of systems. Finally, knowledgeable human beings can efficiently and effectively respond to incidents by reporting them correcting, quarantining problems, and diagnosing and treating problems correctly. Employees are a critical factor in the information security equation.

Given the acute need for people who are information security savvy and the breadth of knowledge that is needed, it is no surprise that there are many different types of security training, education, and awareness (TEA) programs. For organizations looking to add information security training, education, and awareness, the issue of where to start can be a daunting task. The cost of designing and developing new TEA programs can be high. However, the cost of acquiring TEA programs is also high. And regardless of whether an organization elects to develop the program in house, outsource development, or purchase an existing program, there is still the cost of implementation that includes paying trainers, travel, and release time for employees to attend training. No organization wants to invest in TEA that does not actually improve its information security posture. So, the critical question becomes, how can an organization increase the likelihood that their TEA program will provide a positive return on investment?

To help address this question, we turn to an overview of human performance technology with a focus on how human performance technology can help assure that the information security TEA program is effective.

An Overview of Human Performance Technology

Human performance technology (HPT) is also referred to as 1) performance engineering and 2) the science of improving human performance. HPT is the field of work that uses an engineering approach to attain desired results from human beings. HPT draws on the science of learning, teaching, instructional design, organizational behavior, industrial engineering, and psychology. HPT is based on the application of scientific principles to practical ends. The practical end that HPT is focused on is human performance and more specifically how human performance within an organization contributes to the accomplishment of the business goals of the organization.

HPT Principles

A major tenet of HPT is that human performance is necessary to accomplish organizational results; when human performance is systematically aligned with organizational goals, human performance can contribute to the achievement of organizational goals in meaningful and significant ways. In this way, HPT adds value to the organization. Another tenet of HPT is that organizations are complex systems with multiple entities and functional interdependencies. That is, organizations are comprised of multiple functional units, such as finance, human resources, maintenance, administration/management, production, customer service, sales, information technology, and so on. In order for the organization to perform effectively, the business units need to perform effectively. And in order for the business units and the organization to perform effectively, the workforce needs to perform effectively. HPT focuses on identifying the gap between desired and current organizational, unit, and human performance; with a focus on how the improvement of human performance can lead to an improvement in unit and organizational performance. Therefore, to affect meaningful change in organizational performance, it is necessary to determine desired unit and workforce performance. A third major tenet of HPT is a focus on results. Given a gap between current and desired human performance, unit performance, and organizational performance, the results of the intervention will be measured to determine change in human performance and the consequent impact on unit and organizational performance. Finally, the last tenet is that not only does HPT take a systems view, HPT is a system itself. The HPT process takes a systematic approach to 1) assessing performance gaps, 2) the reasons for those performance gaps, 3) finding interventions that address the known gap, 4) implementing those interventions, and 5) evaluating the consequent results. Figure 1 provides an overview of the HPT process.

Performance Analysis

Performance analysis is conducted for the purpose of defining the performance need or opportunity. Performance analysis consists of two elements: 1) organizational analysis and 2) workforce performance analysis. The purpose of organizational analysis is to revisit the organizational vision, mission, values, goals and objectives with specific attention to factors that are detracting from the accomplishment of organizational goals.

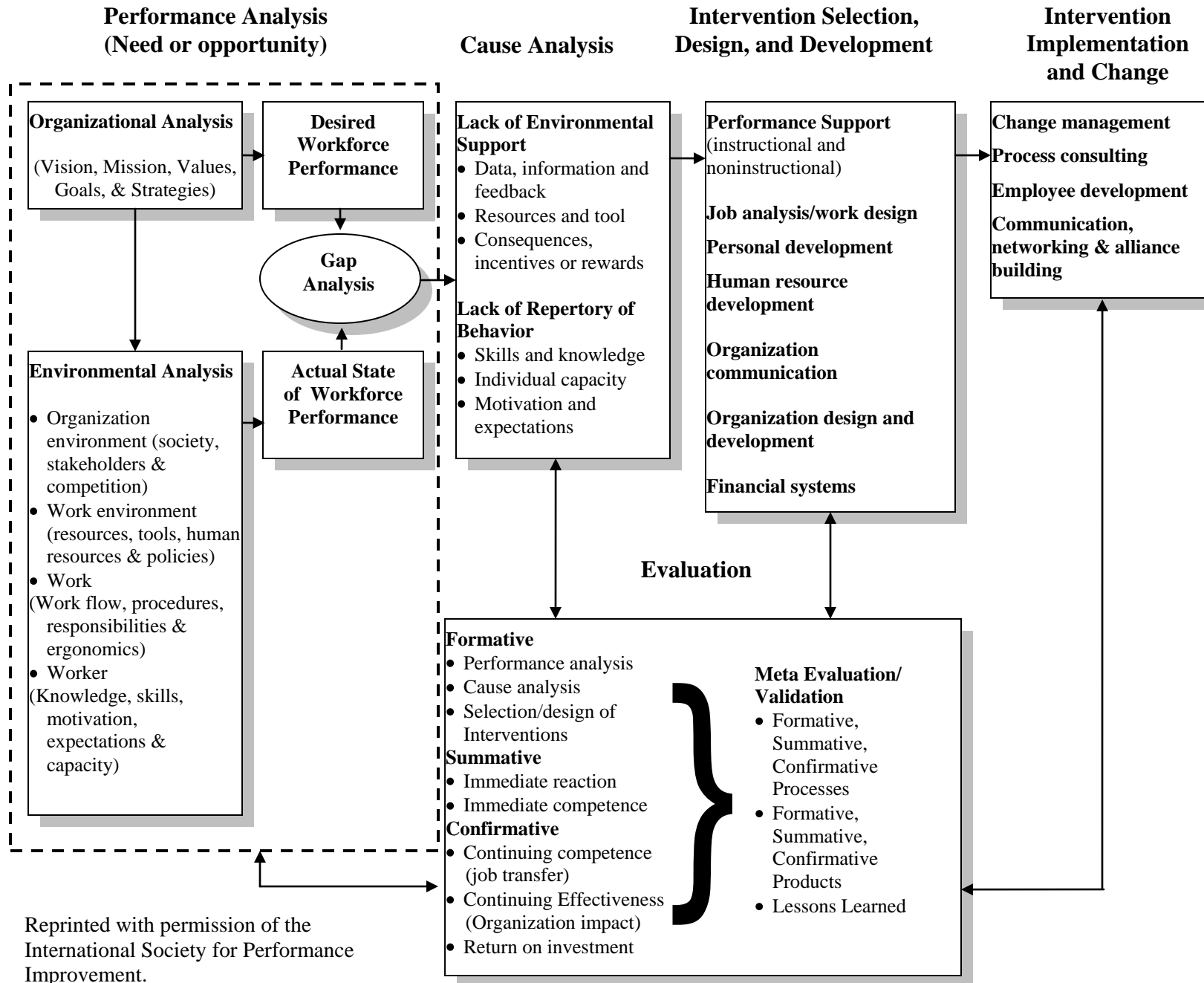


Figure 1: HPT Model

Organizational analysis consists of analyzing the 1) organizational environment to determine key stakeholders, competitors, etc., 2) work environment including tools, resources, policies, etc., 3) work analysis to determine job task requirements, work flow, required efficiencies, etc., and 4) workforce analysis to determine aptitude, knowledge skills, desire, and commitment.

HPT is focused on present and desired levels of human performance in the context of organizational performance. The purpose of workforce performance analysis then is to determine the gap between desired workforce performance and current workforce performance. Workforce performance analysis is more comprehensive than identifying the need for training, education, and awareness. Training, education, and awareness programs assume that a lack of knowledge is the primary cause of substandard human performance. HPT assumes that: 1) performance is a function of ability and motivation; 2) ability is a function of aptitude and education, and 3) motivation is a function of desire and commitment (see figure 2) and therefore assumes that there are many factors that contribute to poor performance.

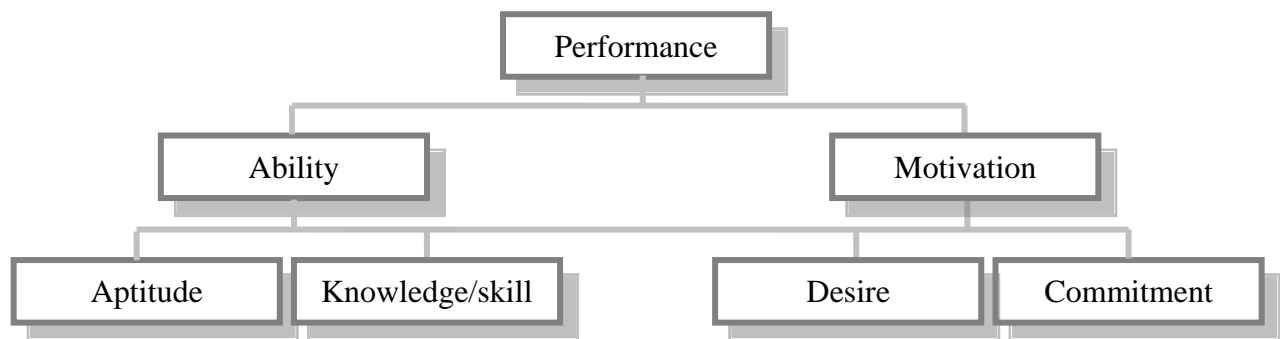


Figure 2: Performance Model

HPT also considers human performance in the context of the organization, its goals and culture. So HPT actually extends past the model of performance shown in figure 1 by considering the dynamic influence of the organizational culture on human performance and conversely the influence of human performance on the organization (see figure 3).

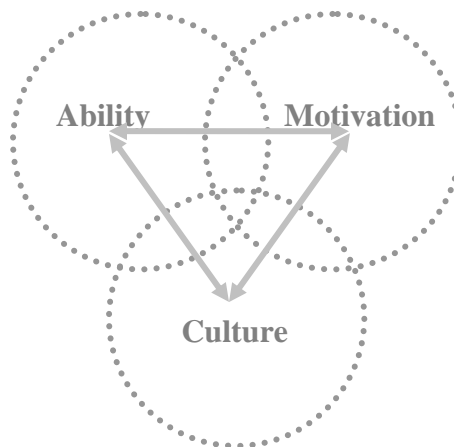


Figure 3: Ability, Motivation, Culture Model

The process of conducting performance analysis can begin with the organizational analysis or with the workforce performance analysis. Often the two are done simultaneously or in rapid iterations. This is because they are mutually interdependent; workforce performance issues cannot be analyzed without analyzing the larger organizational environment and analysis of the organizational environment is meaningless without a focus on some aspect(s) of workforce performance.

Cause Analysis

The next component of HPT is cause analysis. While the gap analysis documents the gap between current and desired behavior, often the results of gap analysis are merely the identification of the gap. Cause analysis then is the diagnosis of why the gap exists. Cause analysis in HPT usually considers the influence of the following factors on performance: 1) consequences, incentives, and rewards for good performance, 2) data, information, and feedback used to set and reinforce expectations, 3) environmental support, resources, and/or tools needed to perform the job task, 4) individual capacity, 5) worker motives and expectations, and 6) worker knowledge and skills. By conducting cause analysis, the organization is more likely to implement solutions that address all root causes or at a minimum the most important root causes. The output of cause analysis is a detailed specification for selecting or designing/developing various types of interventions that are targeted at closing the gap. If the root cause has been identified as a lack of appropriate tools or resources to perform the job, then the recommended intervention will focus on making tools and other resources available. If the root cause has been identified as a lack of expectations and a lack of consequences or rewards/incentives, then the recommended solution will be methods to communicate expectations along with enforcement policies and incentive systems if appropriate. In practice, there are often several root causes; seldom is the recommended solution just one intervention. In addition to providing guidelines for selecting or designing/developing the intervention, the design blueprint is also used to develop valid measures that will indicate if the program is accomplishing its goals.

Intervention Selection, Design, and Development

The next component of HPT is intervention selection, design, and development. As shown in figure 1, the types of interventions are many, e.g., performance support, job analysis/work design, organizational communication, training, and so on. The types of intervention that are appropriate are determined by the cause analysis. The design blueprint that is developed as a result of cause analysis is a list of all potential interventions. However, it is often the case that it is not possible or desirable to select or design/develop interventions for every cause that was identified. The main reason that it is not possible is resource constraints (limited time and money). Most organizations are looking to spend time and money on solutions that will produce high benefit or impact with limited investment. In order to determine those solutions that will have higher impact, yet cost less, a cause prioritization should be conducted.

Cause prioritization can be based on several factors. A few of the commonly used factors are; 1) capability, 2) opportunity, 3) administrative access and control, and 4) cost. Capability refers to the collective knowledge and skills of individuals, departments, and the organization needed to execute the solution. A solution might be appropriate for the problem identified during cause analysis, but if the organization lacks the knowledge or skill needed to develop the solution or if the organization lacks the resources to outsource the solution to a vendor with the appropriate knowledge/skill, then that solution is not as viable as another. Opportunity refers to

the level of organizational support and commitment. Organizational support and commitment are necessary from the highest levels within the organization. It is important to focus on solutions that have support at the highest levels within the organization. Administrative access and control refers to the levels of organizational structure the project requires; generally speaking there is a direct relationship between the number of functional areas and involved and the time required to execute the project. A solution that requires less coordination across business units to execute is usually more desirable. Cost refers to the money required to acquire or design/develop the solution, as well as the implementation and evaluation of the solution. Cost should be considered not only in terms of the least expensive solution, but the potential for the solution to produce high impact results given the cost investment.

The design blueprint should be referred to several times throughout this phase to ensure that to ensure the integrity of the solution. The output of intervention selection or design/development includes products, processes, systems, or technologies that address the performance gap(s) and root causes. Examples products, processes, systems, and technologies include training, performance support tools, newsletters and other communication tools, a new incentive program, a re-engineered process, the deployment of a new technology, and so on. The type of intervention that is needed will also be considered when designing and developing evaluation to determine if the workforce performance gap is being closed.

Intervention Implementation and Change

The next component of HPT is intervention implementation and change. This phase of HPT includes deploying the solution and managing the change that is required within the organization to sustain the desired performance. Research has shown the performance interventions have a significant immediate impact on human performance, but without ongoing change management efforts, there is a diminishing return. For the most part, human beings like to know why change is necessary and are more likely to change if they know why it is necessary. When explaining why change is necessary, research shows that individuals are more likely to change when they understand 1) how change will help them individually, as well as 2) how the collective change will help the organization. Research also shows that if immediate change is recognized, reinforced, and rewarded, the change is more likely to continue over time. Therefore, the change management plan should include feedback strategies that communicate what level of change is occurring, reinforces the desired performance, and specifically rewards those who have changed as well as reiterating expectations and consequences for those who do not. The change strategy then should detail how the effort will be communicated, to whom, and exactly what will be communicated about the effort before, during, and after the intervention has occurred. Other items to consider in the change management plan include: a project management plan with a rollout schedule and contingency plans outlining what to do in case of resistance.

Evaluation

The next component of HPT is evaluation. The output from the performance analysis feeds into cause analysis; and the output from both performance analysis and cause analysis feed into the design, development, and implementation of the evaluation. In other words, meaningful evaluation cannot be conducted if it is not based on performance and cause analysis.

There are three types of evaluation that are used in HPT: formative, summative, and confirmative evaluation. Each type is conducted for a different purpose. Formative evaluation is

conducted for purposes of making improvements in the HPT program and is usually conducted during the design and development phases. Things that are typically evaluated during formative evaluation include the output of the performance analysis and cause analysis and the corresponding selection/design of the intervention. By comparing the emerging intervention with the performance and cause analysis, the human performance technologist is looking for ways to improve the program and ensure that will meet its workforce performance and organizational impact goals. Summative evaluation is conducted for the purposes of determining immediate impact on workforce performance and is conducted immediately after the program. Generally speaking, during summative evaluation you are measuring what you did and the degree to which the solution produced the desired results. In addition, summative evaluation often includes measures of cost. Cost benefit analysis combines benefits gained in light of costs incurred and is frequently a part of summative evaluation. Confirmative evaluation goes beyond summative evaluation to look at the longer term effects of the intervention. The time at which confirmative evaluation is conducted varies, but a reasonable range is 2-12 months after the intervention(s) was implemented.). Confirmative evaluation looks at continued competence on the job, continuing impact or organizational performance, and continuing return on investment.

Given this overview of HPT, we will now take a look at an extended case study where HPT was applied to information security management within an organization.

Information Security HPT Case Study

The first half of the chapter focused on describing the HPT tenets and model. The next half of this chapter will be a detailed case study of an information security HPT program that was developed using the HPT model. This case study was performed for a Midwestern university with approximately 15,000 students and 5,000 faculty and staff. The case study is organized according to each major step of the HPT model. The results of each step and how the data were gathered are reported in detail. The hope is that by studying an extended example, you will be better able to utilize the HPT model to improve information security within your organization.

Performance Analysis

The first step was to conduct the performance analysis. This consisted of conducting both an organizational analysis as well as a workforce performance gap analysis. The goals of the performance analysis were to:

1. define organizational vision, mission, goals.
2. define business need, target environment, and target performers.
3. collect actual and desired organizational performance data.
4. conduct environmental analysis.
5. conduct workforce performance gap analysis.

Define Organizational Mission, Vision, and Goals

The mission of the university is to serve the citizens of the state, the United States, and the world in three areas: 1) research that expands the realm of knowledge, 2) teaching through dissemination and preservation of knowledge, and 3) service through exchange of knowledge. The vision of the university is to be prominent in research, teaching, and service. The goals of the university are to achieve and sustain prominence in research, teaching, and service.

Against the organizational backdrop, the mission of Information Technology department is to provide IT infrastructure in a cost effective manner that allows students, faculty, and staff to make maximum use of the appropriate information technology tools in the learning, teaching, research, outreach, administration, and support activities. The vision of the Information Technology department is to be the best in leveraging and expanding IT infrastructure in a manner that helps the institution achieve and sustain prominence. The goals of the IT department are to:

- Leverage technology to support research, teaching, and service.
- Find cost effective IT solutions.
- Explore emerging technologies that show potential for application in all mission areas.

Define Business Need, Target Environment, and Target Performers

The business need driving the performance analysis was the need for a secure IT infrastructure within the organization. The organization requesting the performance analysis is a university with slightly more than 20,000 users. Among the 20,000 users, approximately 15,000 of the users are students. The students use the computing network in the dormitories called StudentNet. The IT department is encountering excessive workload due to the insecure practices of students using StudentNet. Because of this excessive workload fighting to keep StudentNet secure, the IT department has been unable to meet other performance goals for the business year. For example, the university is interested in a new payroll system as well as a new online library system. Neither of these projects will be possible given current demands in security. The university has decided that they need to reduce the amount of staff time dedicated to securing Student Net from 7 FTE to 4 FTE. One FTE is about 2,020 hours of work per year and roughly \$84,500 in salary and fringe benefits. The reduction from 7 FTE to 4 FTE will provide a salary savings of almost \$255,000 that can be reallocated to the new payroll system and the new online library system.

Collect Actual and Desired Organizational Performance Data

Table 1 below shows the current and desired IT security performance data in several key areas. The difference between the current and desired performance is the gap that needs to be closed. In addition, table 1 indicates how the data were collected.

Performance Issue	Current Performance	Desired Performance	Data Collection Method
Machines compromised in any outbreak of vulnerability	28% of machines compromised	<5% of machines compromised	IT Staff
Email spam	40% of email messages are spam	<20% of email messages are spam	IT Staff
Mailhub viruses	Average of 2,000 machines infected during last 5 virus outbreaks	0 machines infected during next 5 virus outbreaks	IT Staff

Table 1: Performance Analysis Results

It was determined that if the IT department could achieve the desired performance levels listed in table 1, then they would be in a position to reallocate 3 FTE to the other IT projects thereby helping the IT department fulfill its mission which in turn helps the university better fulfill its mission.

Conduct Environmental Analysis

The environmental analysis was conducted to provide information about the work environment, the work processes, and the target performers. For each of 5 performance issues listed in table 1, tools and resources required for accomplishing the desired state were identified and then the associated work processes/responsibilities and knowledge/skill and motivation levels were identified and documented. The results of the environmental analysis are in table 2.

Tools/Resources	Work Processes	Knowledge/Skill/Motivation
Passwords	Creating strong passwords	Users know how to create strong passwords. Users choose to create strong passwords.
Security settings	Users change security settings to the highest level	Users know how to change security settings. Users choose to change security settings.
Disabling or discarding cookies	Users disable cookies or discard them when a website is closed	Users know how to disable cookies and discard them when closing a website. Users choose to disable cookies and discard them when closing a website.
Safe downloading	Users do not download unknown files or program from the Internet	Users know how to check to see if the file/program is safe. Users elect to not download files/programs that cannot be guaranteed as safe.
Firewalls	Installation and configuration	Users know how to select, install, and configure a firewall. Users choose to select, install, and configure a firewall.
Anti-virus software	Installation, configuration, and updating	Users know how to select, install, configure, and update anti-virus software Users choose to select, install, configure, and update anti-virus software
Patches and system updates	Installation and testing	Users know how to apply and test patches and system updated Users choose to apply and test patches and system updates

Table 2: Environmental Analysis

Workforce Performance Gap Analysis

Given these organizational performance gaps, the next step was to determine the workforce performance gaps. The workforce performance gap analysis sought to answer the following question:

- What are the actual and desired knowledge levels and performances of the students with regard to the tools/resources and work processes identified in column one of table four?

The data for the workforce performance gap analysis were collected via a survey. The results of the workforce performance gap analysis are reported in table 3 below.

Tool/Resource	Work Process	Knowledge/Skill Level	Performance Level
Passwords	Creating strong passwords	57% report they know how to create strong passwords	8.1% report creating strong passwords
Security settings	Users change security settings to the highest level	48.2% report they know how to change security settings	34.6% report they change security settings to the highest level
Disabling or discarding cookies	Users disable cookies or discard them when a website is closed	59.5% report they know how to disable cookies or set them to be discarded	44.2% disable cookies or set them to be discarded
Safe downloading	Users do not download unknown files or program from the Internet	77% report they know how to determine if a file/program is safe to download.	66.1% choose not to download unknown files or programs
Firewalls	Installation and configuration	54.8% report they know how to install and configure a firewall	50.9% use a firewall
Anti-virus software	Installation, configuration, and updating	76% report they know how to install, configure, and update anti-virus software	73.1% use anti-virus software 50.5% update anti-virus software once per week
Patches and system updates	Installation and testing	71% report they know how to apply and test system updates	65% apply and test system updated and patches

Table 3: Cause Analysis Results

The data generated from the workforce performance gap analysis were then 1) analyzed to determine more specific causes for the gaps in human performance and also 2) used to set performance goals and associated metrics for evaluating the HPT intervention. The more specific performance goals are shown in table 4. The metrics are described in a later section.

Work Process	Knowledge Current	Knowledge Desired	Performance Current	Performance Desired
Users create strong passwords	57%	100%	8.1%	100%
Users change security settings to the highest level	48.2%	100%	34.6%	100%
Users disable cookies or discard them when a website is closed	59.5%	100%	44.2%	100%
Users do not download unknown files or program from the Internet	77%	100%	66.1%	100%
Users install and configure firewalls	54.8%	100%	50.9%	100%
Users install, configure, and update anti-virus software	76%	100%	73.1% use 50.5% update	100%
Users install and test of system updates and patches	71%	100%	65%	100%

Table 4: Workforce Performance Gap Analysis

Cause Analysis

The next step was to analyze the human performance gaps to determine root causes for the gaps. By determining why the gap exists, solutions can be selected/designed that more effectively address the human performance gap. The data for the cause analysis were collected using the survey. Each content area on the survey (content areas include creating strong passwords, changing security settings, disabling cookies, etc.) had questions aimed at assessing 1) users' knowledge and 2) users' reasons for NOT taking the desired action. The latter was the data used for determining root cause. Table 5 shows sample questions items from the survey in the firewall content area and the corresponding coding to root cause categories.

Question	Root Cause Categories
I have not installed a firewall on my computer because:	
a. I didn't know I needed to.	Expectations and feedback
b. I don't know what a firewall is.	Knowledge and skills
c. I don't have the firewall hardware or software.	Tools and resources
d. I don't know how to install a firewall.	Knowledge and skills
e. I don't want to install a firewall.	Desire
f. I don't know how to get help.	Tools and resources
g. I don't think it is worth it.	Rewards and Incentives

Table 5: Firewall Survey Questions and Root Cause Mapping

Using the data from the survey, a summary of root causes was developed. Figure 4 below shows the summary by cause category. Respondents were allowed to select as many reasons as applied.

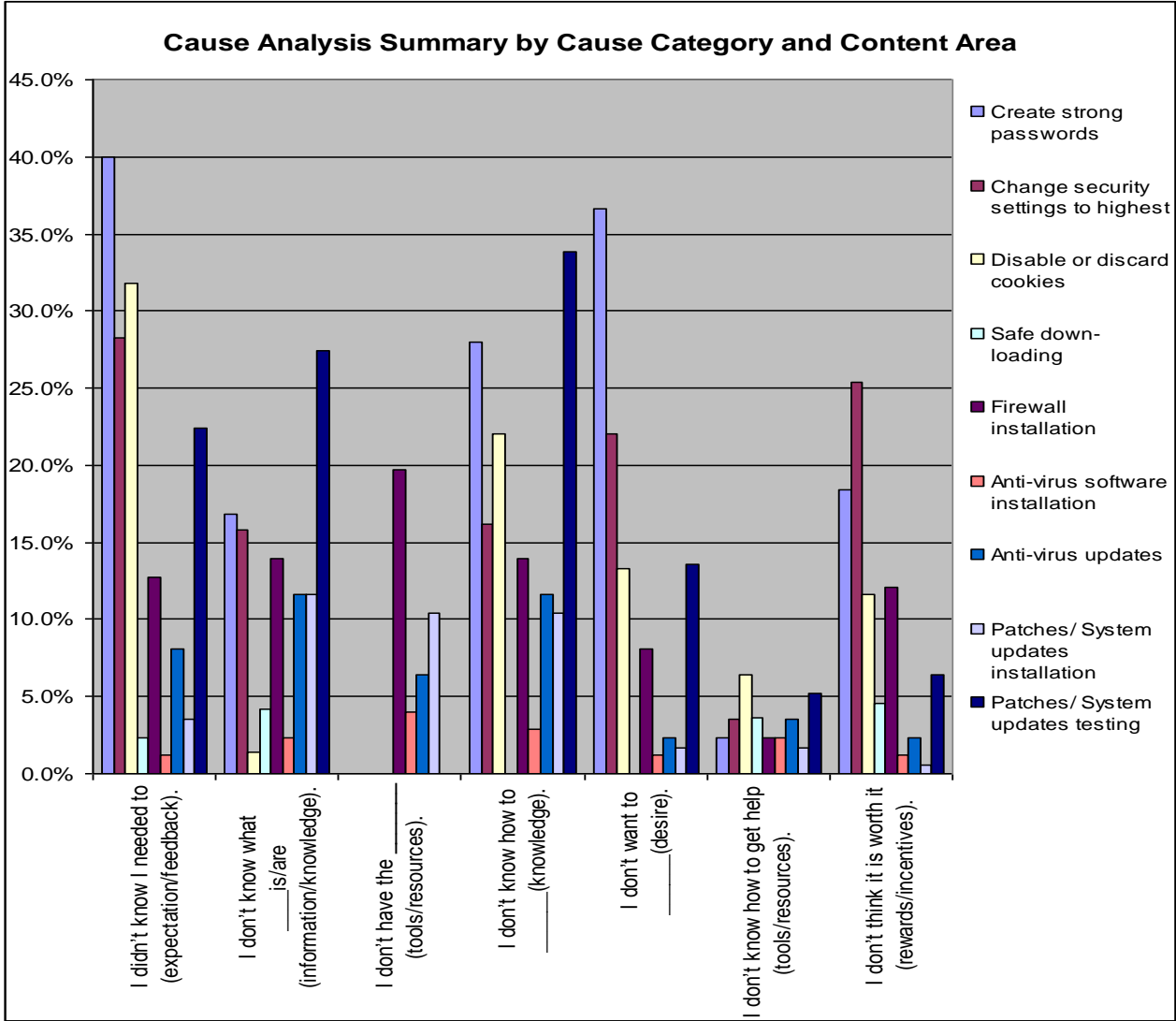


Figure 4: Cause Analysis Summary by Cause Category and Content Area

Averages were created for each category in order to make comparisons among the different root causes. Figure 5 shows the mean score across all content areas for each cause category. What these data show are that a lack of knowledge/skill is the largest cause of failure to take desired action, followed by lack of expectations/feedback, then desire, and so on. These data provide the human performance technologist with detailed information about the nature and focus of the intervention.

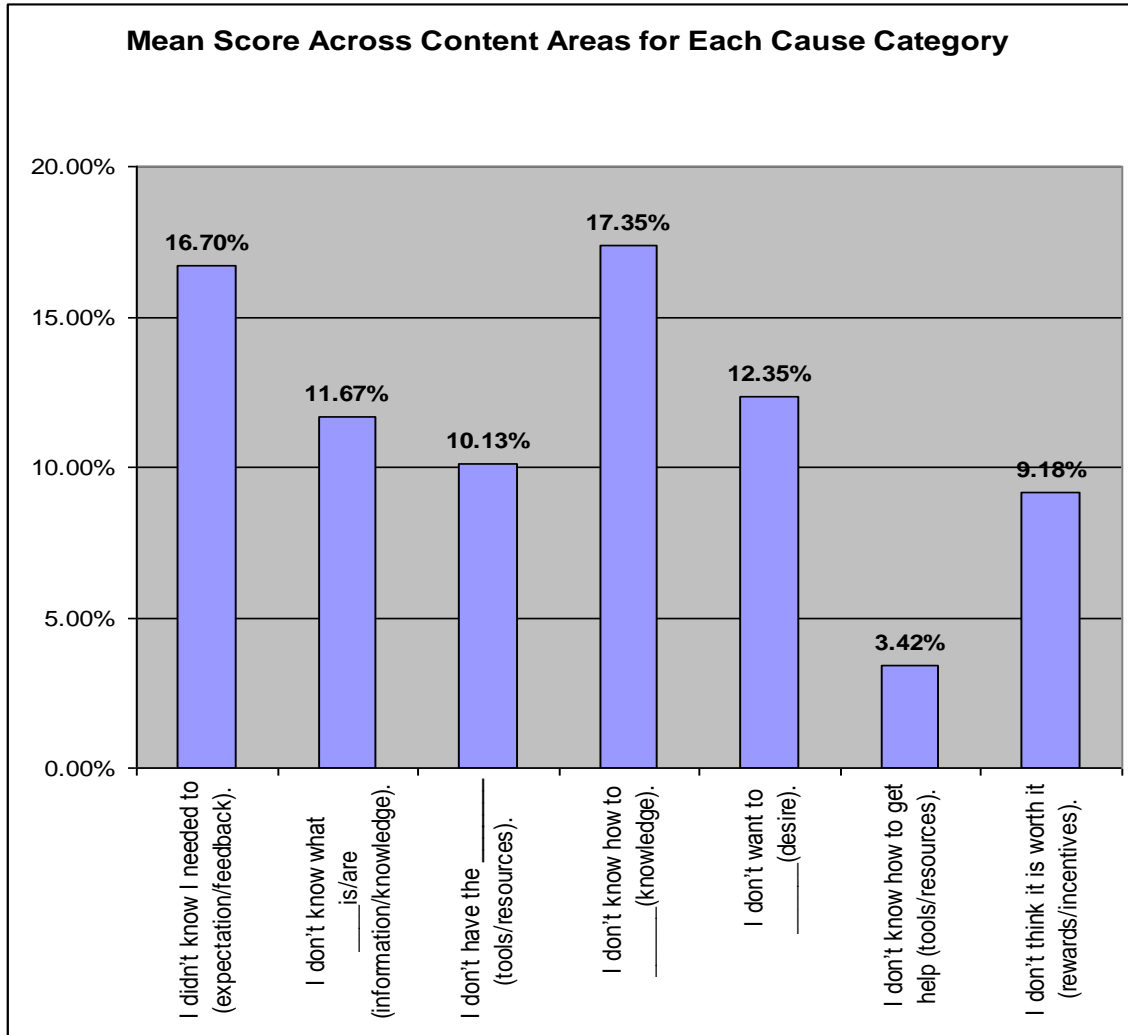


Figure 5: Mean Content Score for Each Cause Category

Intervention Selection, Design, and Development

Using the output of the cause analysis as a design blueprint for the performance intervention, the next step was to select or design/develop the intervention. In selecting or designing/developing interventions, the first task was developing a list of suggested solutions. Because resources were limited, a cause prioritization was conducted. This cause prioritization was based on the five factors. The first was coverage – this is the possibility for the solution to address multiple root causes. The second was capability – this is the capability of the IT department to execute the solution with given the skills/knowledge of their staff. The third was access and control – this was a rating of the ability of the IT department to directly cause the solution to be developed and implemented versus having to rely upon other parties. The fourth was efficacy – this is the belief that the solution will address the problem effectively. The fifth was cost – this is the projected cost of developing, implementing, and evaluating the solution. IT staff were asked to rate each solution based on these five factors using a scale of 1-5 with 5 being strongly agree and 1 being strongly disagree. Table 6 shows a sample of the suggested solutions for the ‘StudentNet Users Not Creating Strong Passwords’ performance gap (it was not possible to show all of the suggested solutions here). Table 7 shows the mean rating for the

suggested solutions presented in table 6; the solutions are ranked from highest to lowest scoring. The interventions that the university decided to design/develop and implement are highlighted in gray. Formative evaluation was conducted at this step to ensure that the interventions aligned to root causes and also to the criteria for managing change.

Performance Gap	Cause Statement	Cause Type	Solution Category	Specific Solution Suggestions
StudentNet Users Not Creating Strong Passwords	40% of users are not aware they need to create strong passwords	Expectation / feedback	Job aid Feedback system	<ol style="list-style-type: none"> 1. On the login in screen, post a message about the need and expectation for creating strong passwords. Highlight a scenario where a weak password has created hardship for a student and the university. 2. Make the tutorial on creating strong passwords mandatory for students. This sends the message that users need to do this and it is important. 3. Enforce the creation of strong passwords by rejecting weak passwords. 4. Hold a security awareness week once a year and include these expectations as part of the event. 5. Email a personalized reminder to each student about the importance of strong passwords.
	36.6% of users have no desire to create strong passwords	Desire	Reprimand system/reward system	<ol style="list-style-type: none"> 1. At the beginning of each month include a news release in the student e-newsletter that highlights how many computers were compromised the past month due to weak passwords and the effects it had on the students.
	28% of users do not know how to create strong passwords	Knowledge / skill	Tutorial/training	<ol style="list-style-type: none"> 1. Create a brief on-line tutorial on creating strong passwords. Make it mandatory for all students to get a career account.
	18.4% of users do not think creating strong passwords is worth-while	Rewards/incentives	Feedback system	<ol style="list-style-type: none"> 1. At the beginning of each month include a news release in the student e-newsletter that highlights how many computers were compromised the past month due to weak passwords and the effects it had on the students affected. 2. Email a personalized reminder to each student about the importance of strong passwords.
	16.8% of	Information	Tutorial/	<ol style="list-style-type: none"> 1. Create a brief on-line tutorial on creating

	users are not aware of what strong passwords are	/ knowledge	newsletter	strong passwords. 2. Reinforce the attributes of strong passwords in the e-newsletter to students. 3. Hold a security awareness week once a year and include these expectations as part of the event.
--	--	-------------	------------	---

Table 6: Partial Sample of Suggested Solutions

Solution	Coverage	Capability	Access and Control	Efficacy	Low Cost	Total Score
On the login in screen, post a message about the need and expectation for XXX. Highlight a scenario where XXX created hardship for a student and the university.	5	4.7	5	2	5	21.7
Enforce the creation of strong passwords by rejecting weak passwords.	1	5	5	5	5	21
At the beginning of each month include a news release in the student e-newsletter that highlights how many computers were compromised the past month due to XXX and the effects it had on the students.	5	5	3.4	3.4	3.3	20.1
Create a tutorial on XXX. Make the tutorial on XXX mandatory for students. This sends the message that users need to do this and it is important.	5	3.4	3.5	5	3	19.9
Email a personalized reminder to each student about the importance of XXX.	5	5	5	3	1.3	19.3
Hold a security awareness week once a year and include these expectations as part of the event.	4	4	4	4	2	18

Table 7: Solution Rating and Ranking

Intervention Implementation and Change

The next step was to develop a project/change management plan. The project/change management plan included a timeline with key milestones as well as a list of criteria for how the change process was to be managed. An excerpt from the larger project/change management plan is provided in table 8.

Solution	Subtask	Owner	Time	Change Management Criteria			
				Need for intervention - individuals	Need for intervention - Recognition of change	Reward for change/ consequence for lack of change	
On the login in screen, post a message about the need and expectation for XXX. Highlight a scenario where XXX created hardship for a student and the university.	Create login message and scenario	Bob	May 31	X	X		
	Review and revise	Policy expert	June 30				
	Execute	Mary	August 15				
Enforce the creation of strong passwords by rejecting weak passwords.	Change policy settings	Mary	August 15				X
At the beginning of each month include a news release in the student e-newsletter that highlights how many computers were compromised the past month due to XXX and the effects it had on the students including diminishing impacts over time.	Develop e-newsletter template	Lance	May 31	X	X	X	X
	Write newsletter content	Bob	2 nd Friday of every month beginning in June				
	Review and revise	Content and marketing experts	3 rd Friday of every month				
	Distribute	Mary	1 st Monday every month				
Create a tutorial on XXX. Make the tutorial on XXX mandatory for students. This sends the message that users need to do this and it is important. Students must score 85% or higher. Provide congratulatory feedback in the way of a free mouse pad to students who pass with a score of 85% or higher.	Create objectives	Sue	May 31	X	X	X	X
	Create assessment items	Sue	June 15				
	Develop materials	Sue	August 1				
	Pilot test and revise	Content and training experts	August 15				
	Implement tutorial	Sue	September 1				
	Evaluate	Committee	October 15				

Table 8: Project/Change Management Plan

Evaluation

The last step in completing the HPT process is the evaluation. The formative evaluation was actually started during the intervention selection, design, and development phase. The formative evaluation consisted of expert review. The experts selected to provide review included content experts, policy experts, training experts, and marketing/communications experts. The content experts provided feedback on the accuracy and completeness of the content included in the e-newsletter and the tutorial. The policy expert provided feedback on the structure and content of the policy posted on the log-in screen, the training expert provided feedback on the structure and elements of the tutorial, and the marketing/communication expert provided feedback on the design, layout, and readability of the e-newsletter. The formative evaluation was conducted using one-to-one evaluation with direct feedback being provided to the owner of that task.

The summative and confirmative evaluation consisted of several metrics. Table 9 below shows a sample of various metrics classified as summative, confirmative or both, the evaluation design, and corresponding data collection methods. Notice that the first four metrics listed are the direct results of the intervention, whereas the next three metrics are organizational impact type metrics.

Metric					Evaluation Design	Data Collections Method
	Summative	Confirmative	Baseline	Target		
Knowledge of how to create strong passwords	X		57%	100%	Pre-post survey	After the intervention was implemented, a post survey was used to determine how many students reported that they know how to create a strong password. Data were compared to the baseline data collected during the performance assessment.
Creation of strong passwords	X	X	8.1%	100%	Longitudinal (Pre-Post-Post...)	Ongoing periodic random sampling of passwords and testing for strength.
Knowledge of how to disable or discard cookies	X		59.5%	100%	Pre-post survey	After the intervention was implemented, a post survey was used to determine how many students reported that they know how to disable or discard cookies. Data were compared to the baseline data collected during the performance assessment.
Disabling and discarding cookies	X	X	44.2%	100%	Pre-post-post	After the intervention was implemented, a post survey was administered to determine how many students reported disabling or discard cookies. The survey was then repeated

						3 months later. Data were compared to the baseline data collected during the performance assessment.
% of machines compromised		X	28%	<5%	Pre-post-post	Data were collected 3, 6 and 12 months after the intervention and compared with baseline data.
# of machines infected by mailhub viruses		X	2,000 last 5 out-breaks	0	Pre-post-post	Data were collected 3, 6 and 12 months after the intervention and compared with baseline data.
# of IT FTE reallocated from security to other IT projects		X	7	3	Pre-post-post	Data were collected 12 and 24 months after the intervention and compared with baseline data.

Table 9: Summative and Confirmative Evaluation

Suggested Readings

Human Performance Technology Principles, International Society for Performance Improvement available at <http://www.ispi.org/>

Lei, K., Schmidt, T., Um, E. & Schaffer, S. (2004). Performance Analysis: A case study on computer security. *Proceedings of the Association for Educational Communications Technology conference*. Chicago, IL.

Performance Improvement Journal, available at <http://www.ispi.org/>

What is HPT?, International Society for Performance Improvement, available at <http://www.ispi.org/>