Hubbard Decision Research

Information Technology Performance Management

A Case Study of the Applied Information Economics Methodology for an Infrastructure IT Investment

- **Conducted by the IT Performance Management Subcommittee**
- **For the Capital Planning and IT Management Committee**
- **Of the Federal Chief Information Officers Council**

This document is meant to serve as a summary of an actual case study Hubbard Decision Research performed for the Veterans Administration.

While some sections of the original document have been omitted and/or renumbered here, no information contained within has been edited.

Please contact us at info@hubbardresearch.com to request the document in its entirety.

Table of Contents

Host Agency Opinions about the AIE Methodology

The Applied Information Economics pilot was quite an eye-opener to the members of the VA Core Team who had no prior knowledge of the methodology. Initially, the task to develop mission performance measures appeared quite daunting to the VA Core Team. The VA had been looking for a concise and knowledgeable way to strategically evaluate the ISP. AIE provided just what was needed. The VA Core Team now looks at the ISP and its associated investments in a new and more confident light. In addition, the VA management has reinforced its commitment to the ISP as a result of the established of implementation priorities for the ISP investments and their projected cost avoidances. Overall, the VA considers the AIE experience a positive one and sees AIE as a powerful and profitable analytical tool.

Implementation of the AIE Recommendations

At the recommendation from the contractor, the VA has accelerated the anti-virus roll-out by six months, cancelled the optional intrusion detection investment, applied the formula for VAPKI roll-out for all facilities prior to VAPKI certificate distribution, and the training team leader is conducting further research into that optional investment area. The VA will implement the additional recommendations by completing a return on investment analysis of the Simplified Sign-on, TEAM and ITSCAP investments.

Additional Comments

As a result of this pilot, the VA was able to avoid making a $30,000,000 investment in intrusion detection, and that alone makes AIE pilot worthwhile for VA. But, the ISP and the VA Core Team members realized many other benefits, including the concept of minimal and optional investments, a focus on rollout strategies and usage statistics, and an appreciation for the value of information. It is the consensus of the VA Core Team that the model developed as a result of this study leads to measures that truly have an impact on the improvement of information security. The VA intends to use the results of this pilot also as input to the self-evaluation for ISP as required by the Government Information Security Reform Act (GISRA). Finally, the VA recommends that the AIE methodology be explored as a GISRA evaluation method for other Federal civilian agency information security program.

Executive Summary

Federal executive agencies face significant management and technical challenges when measuring the contribution of information technology investments to mission results as required by the Clinger-Cohen Act. There is a shortage of knowledge and examples of how to measure IT's contribution to mission results for government agencies with complex missions such as providing for the health and welfare of the citizens of the United States.

To close this knowledge gap and to improve Federal performance management practices, the Federal Chief Information Officers Council sponsored pilot demonstrations of two measurement methodologies, Applied Information Economics and Balanced Scorecard. Those pilots, which were completed in May 2001, proved that each methodology was applicable in the federal environment, provided the host agency with a useful performance measures, and provided lessons learned for other federal agencies to benefit.

This report presents the findings from the Applied Information Economics pilot. The Department of Veterans Affairs (VA) volunteered to participate in this pilot with its Information Security Program (ISP), which is an approved new infrastructure initiative that will mitigate information security-related risks across the department. The risks include reducing the cost and frequency of viruses, unauthorized access, fraud and other types of losses. The total cost for ISP over five years will be approximately $114 million.

Applied Information Economics (AIE) is an analytical methodology that applies proven and practical scientific and mathematical methods to the IT decision process. Although AIE is six years old and has been used commercially in many industries, this is the first major application of AIE in the Federal government. The creator of the AIE methodology claims that there are no intangibles such as "improved decision making," which cannot be measured. One of the principles of AIE is that measurement is for improving future decisions not for justifying past decisions. The only exception being compulsory reporting to satisfy the need for responsible oversight.

The AIE methodology determines what to measure by using a sophisticated cost-benefit analysis method that calculates the value of information for each variable using a formula familiar to decision analysts and statisticians for more than 50 years. The value of information depends upon two things, the certainty of an expert about a particular variable such as "the number of viruses per year" or "the cost of each investment," and the value of the decision to be made. If the value of information for a particular variable is $200K for example, then an organization, as a general rule, should expect to spend no more than 20 percent to take a measurement to gain additional information to improve the decision to be made. A high information value indicates that addition measurements would improve decision making.

There are two principal decisions that VA needs to make regarding the Information Security Program. One is which combination of its optional investments will reduce the

greatest losses at a reasonable cost. The second is what is the best rollout strategy for VA's Public Key Infrastructure (PKI) investment that will optimize the value of PKI. The AIE method determined that VA would make the best investment decision by taking seven key measurements. Those measurements will also allow VA to determine the effectiveness of the Information Security Program over time. The AIE method also determined a prioritization approach that will allow the VA to implement PKI for the high-risk areas first and defer implementation for the low-risk areas.

The AIE methodology also determined that:

- the Information Security Program should reduce by 75% to 95% the expected losses for all security incidents through 2006 estimated somewhere between $1.1 billion and $2.4 billion.

- one major optional investment (certain parts of Intrusion Detection) did not reduce losses and therefore should not be made. This is about a $30 million cost avoidance.

Considering only the cost avoidance of the Intrusion Detection investment, this pilot had a value of $30 million. The cost of the pilot, including all contractor fees and travel expenses plus the time of the VA staff, was less than $100,000. Even excluding the value of other strategy improvements, the AIE methodology provided a 300:1 payback. The total cost of the pilot was less than 0.1 percent of the investment size of VA's Information Security Program.

Purpose of the Pilot

The purpose of the pilot project was to compare two different methods for developing performance metrics for IT projects. Each of the methods was assigned a project within a Federal agency and observers from various other agencies commented on the process and the results.

Pilot Objectives

- Test applicability of methodology to measure contribution of IT to mission results,
- Provide a real government example and lessons learned
- Provide host agency with measures

Approach

The Information Technology (IT) Capital Planning Committee and the Sub-Committee on IT Performance Management of the Federal Chief Information Officers Council sponsored two pilot programs to demonstrate different IT measurement methodologies. This was done because many federal agencies have had difficulty in responding to the Clinger-Cohen Act of 1996 which requires Federal agencies to measure the contribution of IT investments to mission results. The objectives of these pilots were:

1. To test the applicability of two different methodologies to measure contribution of IT to mission results;
2. To provide examples of government organizations using the methodologies;
3. To present lessons that were learned to interested agencies; and
4. To provide the host agencies with IT measures

The two methodologies chosen for this pilot project were Applied Information Economics (AIE) and the Balanced Scorecard (BSC). The host agencies in the pilots were the Department of Veterans Affairs (VA) and the Department of Agriculture (USDA). Both host agencies provided the core team and resources necessary to complete the pilot.

The VA created a pilot team from its Information Security Program (ISP), which employed the AIE. The USDA's Food Acquisition Tracking Entitlement System (FATES) applied the BSC. The FATES team was a tri-agency partnership of Agriculture Marketing Service (AMS), Food and Nutrition Service (FNS) and Farm Service Agency) (FSA). In addition to the Core team members, the pilot team meetings were also open to interested observers from the CIO Council. The observers participated minimally in the workshops, occasionally asking questions for clarity, but rarely providing input to the core teams.

Description of Host Agency Business Needs

The Department of Veterans Affairs employs over 240,000 individuals to care for the needs of veterans - including medical, pensions and burial. Information systems security is necessary to support the goals of the VA both directly and indirectly. Security incidents affect the cost, quality and timeliness of virtually all areas of veterans care.

VA Mission Statement

"To care for him who shall have borne the battle, and for his widow and his orphan."
–Abraham Lincoln

The mission of the Department of Veterans Affairs is to Honor, Care and Compensate Veterans in Recognition of Their Sacrifices for America.

VA's responsibility is to serve America's veterans and their families with dignity and compassion and be their principal advocate in ensuring that they receive medical care, benefits, social support, and lasting memorial promoting the health, welfare and dignity of all veterans in recognition of their service to the United States.

VA Size

VA employs over 240,000 individuals – over 13 percent of the total federal workforce. Almost 98 percent of the staff are assigned to provide direct services to veterans and their families in VA field operations.

The delivery of veteran services is accomplished through 172 medical centers, 527 ambulatory and community-based outpatient clinics, 206 veterans centers, 57 regional offices, more than 24 discharge centers, additional out-based locations, and 119 national cemeteries.

VA provides services and benefits through facilities in all 50 states, the District of Columbia, Puerto Rico, the Virgin Islands, and the Philippines.

VA Business Lines

VA provides services and benefits through the following business lines:

- Medical Care
- Medical Education
- Medical Research
- Compensation
- Pension
- Vocational Rehabilitation and Counseling
- Education
- Housing
- Insurance
- Burial

Relevant Objectives

The VA Strategic Plan specifies performance and cost management objectives for all administrations within the VA. Many of them are adversely affected by security risks.

The VA has specific output-cost-reduction objectives such as cost per claim completed, cost per loan, etc. The costs of security risks adversely affects all of these objectives since security incidents affect productivity in all lines of business.

The productivity losses due to security incidents may also affect any of the numerous output-related objectives. Many of the VA objectives call for increased output and all of them are at risk of security incidents.

Summary

VA exists to give meaning, purpose, and reality to America's commitment to her veterans. The requirements, preferences, and expectations of veterans directly shape the services VA provides.

Description of Agency IT Initiative

The Information Security Program (ISP) is a five-year investment in the VA's security infrastructure. The total cost over five years will be approximately $114 million. It will address viruses, intrusion, fraud and other security risks through new systems, procedures and training.

Information Security Program (ISP) Overview

Information security has been a burgeoning discipline in Federal IT circles for years, but recent highly visible security breeches at other Federal agencies have made information security a matter of paramount urgency and importance. VA's current information security program is under close scrutiny by the U.S. General Accounting Office (GAO) and VA's own Inspector General (IG), with both organizations mandating that VA drastically improve information security throughout the Department. Furthermore, VA's information security program has been reported as a Departmental material weakness under the Federal Manager's Financial Integrity Act.

For these reasons, the Acting Assistant Secretary for Information and Technology, the VA Chief Information Officer (CIO), approved a protocol for a Department-wide information security program in February 1999. Subsequently, a team was formed to develop program requirements, responsibilities, and initiatives. This team worked in a group with security managers from each VA Administration and Staff Office to quickly develop a more robust information security program for VA. Speed in development of this program was a necessity to address Departmental material weaknesses and to satisfy the requirements of various statutes, OMB Circulars, and Presidential Decision Directives.

Background: VA Security Risks

The ISP will secure VA's information assets from known threats and vulnerabilities. Without risk management, these threats and vulnerabilities can have serious consequences for VA as an organization, and for individual veterans who entrust VA with their most private data. Sensitive information, e.g., financial transaction data, personal information in veteran's medical records and benefits payments, is vulnerable to inadvertent or deliberate misuse, fraudulent use, improper disclosure or destruction.

Vulnerabilities as a result of inadequate controls and oversight include unauthorized access to VA systems, lack of systems monitoring, inadequate physical security, inadequate segregation of duties, and no controls over changes to operating systems, and incomplete disaster recovery/contingency planning development and testing.

Mission of the ISP

The VA Information Security Program mission is to ensure the confidentiality, integrity, and availability of VA information assets. The VA ISP covers all VA information assets, including hardware, software and data. It applies to Departmental information resources located at VA facilities and those maintained at non-VA facilities. It encompasses all measures, including technical, administrative, personnel, and physical controls, necessary to protect information assets against unauthorized (accidental or intentional) disclosure, modification, destruction, and denial of services.

The VA ISP involves all VA employees, vendors, contractors, volunteers, veterans, service organizations, members of the general public, and anyone else with access to, or who uses VA information systems. It applies to data sharing agreements and similar understandings with other government agencies, commercial business partners, and the public.

The VA ISP supports VA's mission by protecting VA's information assets. In addition, the VA ISP proactively implements statutory and regulatory requirements and industry best practices, and adapts to technology infrastructure dynamics. The information assets required to execute departmental mission programs for health care, benefits delivery, national cemeteries, and

associated administrative support functions are themselves mission-critical.

Investment Area Definitions

The ISP has seven investment areas. Each of the investment areas has components that are considered minimum necessities. Some of the investments also have optional components that may or may not be added depending on the findings of this study and the subsequent metrics implemented. See Appendix 2 for detailed descriptions of minimum vs. optional components.

A. **IT Systems Certification and Accreditation Program (ITSCAP**). Certification is a technical evaluation of an information technology system to see how well security requirements are met. Accreditation is the official management authorization to process. This initiative also includes the development of a data sensitivity model. This initiative uses contractor support to meet its objectives. The mission of ITSCAP is to assure that the security controls of each individual system or application yield adequate security; where adequate security is an approximate balance of the cost of controls and the value of the information assets in the system or application. ITSCAP gives the public faith that VA achieves a standard of due diligence for the security of the system or application comparable to other private or government entities doing the same kind or kinds of business.

B. **Intrusion Detection**. Intrusion detection identifies intruders breaking into information systems or legitimate users misusing system resources. This initiative also includes developing secure gateway configurations. This assures that VA's networks, systems, and applications are adequately monitored for threats from persistent adversaries both internal and external. Intrusion detection gives the public faith that VA achieves a standard of due diligence for the security of the network or system or application comparable to other private or government entities doing the same kind or kinds of business.

C. **Simplified Sign-On.** Sign-on will simplify and improve the sign on event that regularly confronts employees, contractors, and other representatives granted access to VA's internal networks, systems, and applications. It will improve workforce productivity and strengthen access controls.

D. **VA Public Key Infrastructure (VAPKI).** A public key infrastructure is a combination of hardware, software, policies, and administrative procedures that provide a framework to use public key cryptography to transfer data in a secure and confidential manner. Currently, PKI is the only identification and encryption solution that provides all four components of a secure electronic transaction: strong authentication; data integrity; confidentiality; and, non-repudiation. PKI is an economic and simple way of implementing these security services in a system or application.

E. **VA Computer Incident Response Capability (VA-CIRC).** VA has established and maintains a computer security incident reporting and response capability to ensure that computer security incidents are detected, reported, and corrected as quickly as possible, and with minimal impact. Incident reporting and response is designed to: detect and respond to computer security incidents as they occur, assist in preventing future incidents from occurring through awareness, contain necessary response mechanisms to deal with incidents, and, support security controls and procedures.

F. **Antivirus.** Antivirus will protect VA's networks, systems, and applications from virus attacks. This will limit the costs related to loss of business-critical information, workforce productivity, or interruption in the services provided to VA beneficiaries.

G. **Training/Education/Awareness/Message Building (TEAM).** TEAM includes media development, conference planning, satellite broadcast development, brochures, posters, announcements, and the ISP public presence. TEAM will help ensure that the VA workforce is empowered to make their individual contributions to information security excellence.

Steps of the AIE Performance Metrics Approach

The AIE performance metrics approach consists of 4 phases. These phases focused on identifying metrics that have a high economic value compared to their costs.

Overview

The four phases of the AIE performance metrics approach were:

Phase 1: Compute measurement economics
Phase 2: Design measurement methods
Phase 3: Implement measurement methods
Phase 4: Collect and analyze results

Phase 1: Compute Measurement Economics

The objective of Phase 1 was to compute the economic value of potential measurement alternatives. AIE makes measurement decisions based on the economic value of the information from the proposed measurements. The major tasks of Phase 1 included the following:

1. Identify decisions
2. Model decisions
3. Compute information values

Identify Decisions

The major decisions that still needed to be made regarding the ISP had to be identified so that metrics could be identified that specifically supported them.

The specific types of decisions to be made would obviously affect the decision model. Is the decision about whether or not some investment should be made? Is the decision about choosing an optimal "portfolio" of combinations of investments? Is the decision about choosing the best of several implementation plans? The decision could be any of these or others.

Model Decisions

The decision model was a spreadsheet model that included all the relevant decision variables. The objective was to take a large complicated decision with lots of variables and represent it in an ordered, structured fashion that is as simple as possible to communicate. Once the spreadsheet was developed a set of initial estimates was provided based mostly on the knowledge of the VA Core Team. These estimates were not typical point values but "probability distributions" that represent the uncertainty of the estimator.

The process behind the initial estimates was based on the fact that *assessing uncertainty is a general skill that can be measured and refined*. In other words, experts can measure whether they are systematically "underconfident", "overconfident" or have other biases about their estimates. Once this self assessment has been conducted they can learn several techniques for achieving a *measurable improvement* in estimating.

This initial "calibration" process was critical to the accuracy of the estimates later received about the project. The methods used during this "calibration" have been designed in the recent past by such well known academics as Dr. Shoemaker from the University of Chicago.

Few individuals tend to be naturally good estimators. Most of us tend to either be biased toward over or under confidence about our estimates. (see Definitions box)

Definitions

Overconfidence: The individual routinely puts too small of an "uncertainty" on estimated quantities and they are wrong much more often then they think. For example, when asked to make estimates with a 90% confidence interval much fewer than 90% of the true answers fall within the estimated ranges.

Underconfidence: The individual routinely puts too large of an "uncertainty" on estimated quantities and they are correct much more often then they think. For example, when asked to make estimates with a 90% confidence interval much more than 90% of the true answers fall within the estimated ranges.

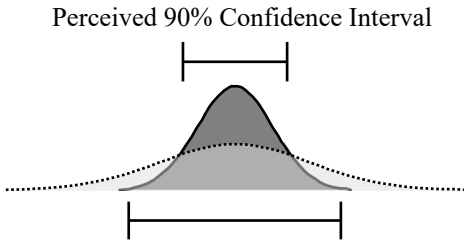
Academic studies by Dr. Shoemaker and others proved that better estimates are attainable when

estimators have been trained to remove their personal estimating biases. The contractor conducted a workshop for the Core Team where the participants recorded a low and high bound that represented a 90% confidence interval of their personal knowledge abouta given set of general knowledge questions.

Since the original estimates were made with a 90% confidence, an average of 1 in 10 should be incorrect. By reviewing the participants' answers to these questions we can derive and illustrate their over or under confidence. By performing this process of answer and review several times, participants become "calibrated" to the level of their personal confidence that corresponds to a 90% level of statistical confidence.

Calibrated Probability Assessments

When asked to provide a subjective 90% confidence interval, most managers provide a range that only has about a 40%-50% chance of being right



The initial set of estimates (all ranges) represented the current level of uncertainty of the team about the quantities involved. This provided the basis for the next step - computing information values.

Compute Information Values

Once the initial ranges were determined we asked if there was any value to reducing uncertainty and, if so, where. All measurements that have a value result in the reduction of uncertainty of some quantity that affects some decision. The variables vary by how uncertain they are and by how much they impact the final decision.

Phase 2: Design Measurement Methods

The objective of Phase 2 was to determine measurement methods that have the highest information value compared to their costs.

This involved the following major tasks:

- Identify alternative measurement methods
- Estimate costs of methods
- Choose methods based on cost vs. information value

Phase 3: Implement Measurement Methods

Phase 3 implemented the measurement methods identified in Phase 2. The VA Core Team conducted surveys and gathered data from research, passive measurements and the other measurement methods previously identified.

This included the implementation of any organizational procedures required for continuous and persistent execution of the measurement. The objective was not to create "one-time" measurements but on-going measurements that will be part of the culture and the continued decision-making process.

Phase 4: Collect & Present Results

Phase 4 captured data and reported results gathered from data in Phase 3. This was not the "end" of the measurement process since the measurement process is on-going. It is merely a snapshot of the measurements gathered so far and represents the nature and effectiveness of the measurements implemented.

Results

The productivity impact of viruses, frequency of intrusions, losses due to fraud and the cost of certain ISP investments were determined to be the critical measurements.

Phase 1 Results

Identify Decisions

The team felt that all the ISP initatives (see section 3) had certain necessary components that had to occur. These were called the minimum investments since there is no decision problem in regards to them and they simply must be implemented. However there are other components of each of the investment areas where the value is not certain. These are called the optional investments and the decisions to proceed with them depend on the results of future measurements.

The ISP investment decision:

What is the best combination of optional investments from each of the ISP initiatives?

The Decision Model

The team modeled the benefits of the ISP and each of its optional investments. First, a model of the total security losses was made so that we could see what security losses might look like without the ISP. This was called the "Loss Model" and it was a baseline for all the ISP investment initiatives. The Loss Model is a spreadsheet that estimates the cost of five basic types of security incidents:

Incident types

- Viruses
- Unauthorized internal logical access
- Unauthorized external logical access
- Unauthorized physical access
- Environmental events

Viruses -- Software designed and distributed for the purpose of causing damage to information systems assets, and that replicates and distributes automatically.

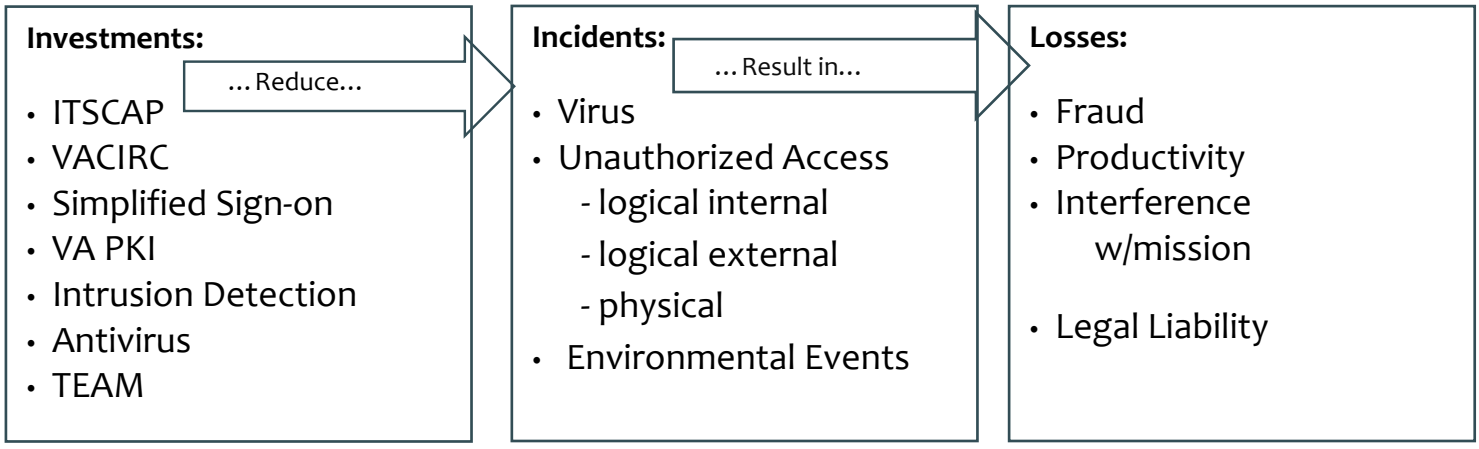
Unauthorized Internal Logical Access -- Access to VA information systems by unauthorized individuals, originating within VA's network perimeter.

Unauthorized External Logical Access -- Access to VA information systems by unauthorized individuals, working outside VA's network perimeter, that bypass authentication mechanisms, exploit vulnerabilities in system services, eavesdrop, or monitor network activity.

Unauthorized Physical Access -- Access into a VA facility by unauthorized individuals that in turn causes denial of computer services, corruption of data, or compromise of confidentiality.

Environmental Events -- Events that are caused by circumstances out of the control of human forces, such as flood and fire, which result in denial of service to information security assets.

Major Components of the ISP Model



The frequency and severity of each of the security incidents was estimated. The severity of an incident is the total cost of one incident. The total costs included the following loss types:

Loss types

- Fraud
- Productivity
- Interference w/mission
- Legal Liability

The value of the ISP investments were the reduction in security incidents resulting in fewer losses. As expected, most of the initial quantities came from Calibrated Probability Assessments. The calibration training showed that most of the estimators were able to adequately represent their uncertainties with probability distributions. Most of their ranges were conservatively wide. The other source of data was Standard Metrics. See appendix 5 for the detailed spreadsheet model.

Initial Measurement Source Summary	
Source of Measurement	Number of variables
Calibrated Probability Assessments – probability distributions gathered from calibrated estimators	**104**
Financial Standard (Cost of Capital)	**1**
Total	**105**

For each of the 104 variables, the estimators provided ranges that best reflected their current level of uncertainty for each of the quantities.

For example, the average duration of the period of productivity loss due to a virus attack is not known exactly. But the estimators felt confident that the average duration must be between 4 and 12 hours.

Furthermore, they were willing to say that they were 90% certain the actual value falls between this upper and lower bound. Finally, they were willing to say that the distribution of possible results was a *normal* distribution. They could also have chosen other types of distributions (lognormal, uniform, beta and binary).

Each of the possible distribution types says something about the probability of various outcomes. In the case of the duration of the productivity impact of a virus attack, the estimators choice of a normal distribution says that there is a small chance of the value being outside their range (10%) and that the probability was symetrical (the true value is just as likely to be above 8 hours as below). The code for a normal distribution type is a 1. See the excerpt from the spreadsheet below to see how this data was recorded for the model.

The Productivity Impact of a Virus Attack

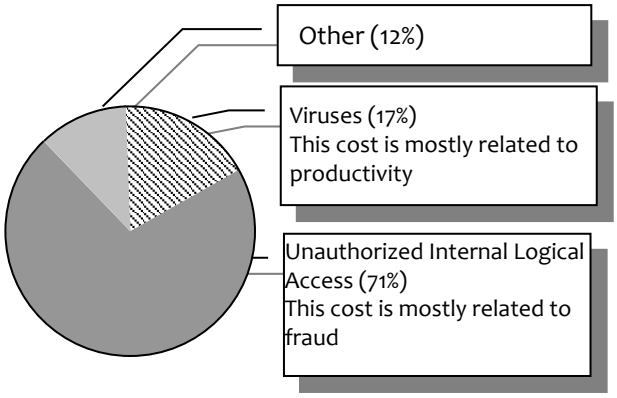
Variable Name	Lower Bound	Formulas & Best Estimate	Upper Bound	Distribution Type
Productivity				
Average number of people affected	25,000	45,000	65,000	1
Percentage productivity loss	15%	38%	60%	3
Average duration of productivity loss	4	8	12	1
Cost per person	$ 50,000	$75,000	$ 100,000	1
Total productivity loss per incident		$ 4,867,788		

Indicates the type (shape) of the probability distribution chosen for this variable. A (1) indicates a Normal

Preliminary Findings

The ranges were used to generate 50,000 random scenarios – each of which is a potential outcome of the ISP investment. This is called a Monte Carlo simulation. An average of the security losses from all these scenarios was produced to assess the likely costs of various potential security losses. This analysis produced the following distribution of security losses in the VA:

Relative Costs of Simulated Security Losses



Each of the security-related events was expected to result in different types of losses. The initial calibrated estimates indicated that the team believed most of the cost of unauthorized internal access was due to fraud losses while events like viruses resulted in productivity losses. But losses due to fraud were estimated to be over $100 million per year – much more than expected productivity losses from virus attacks. Therefore, unauthorized access is a much greater risk than virus attacks.

The *other* category in the above pie chart includes environmental events, unauthorized external access and unauthorized physical access. But, clearly, for the most impact the ISP should (and does) focus on mitigating the security risks of viruses and unauthorized internal logical access.

Since the pie chart was generated from a Monte Carlo simulation, it only shows an average of all potential outcomes. It does not show the exact distribution of what losses will be experienced. We did determine, however, that the losses due to unauthorized internal access are 99% probable to be the largest loss category.

The same Monte Carlo simulation was used to assess the expected impact of the entire ISP – including both the minimum required investments as well as the optional investments. The Monte Carlo simulation clearly showed that security related losses are significant and that the ISP will significantly reduce them. The graph below shows the expected reduction in security incident losses over the next six years.

The anticipated total costs due to security related incidents over six years are very uncertain but there is a 90% probability that the losses will be somewhere between $1.1 billion and $2.4 billion.

The ISP is expected to reduce this by 75% to 95%. This will most likely result in cost avoidance of several hundred million dollars over the next six years. This easily justifies the expense of the ISP.

The decision, therefore, is not about whether to proceed with the ISP. It is only about which of the various optional investments should proceed. The proposed ISP investments will reduce the severity and frequency of incidents that cause security-related losses. The contractor used this information to assess the viability of each of the optional investments of the ISP and determined which should be pursued and how those investments should be measured.

Compute Information Values

Initial measurements were based entirely on calibrated probability assessments by the Core Team. The following areas areas required additional measurements:

- Fraud
- Optional investment costs
- Frequency of logical intrusions
- Cost of viruses and reduction of viruses due to investments

The information value calculations clearly indicated that these four types of quantities easily justify additional measurement effort as can be seen in the Summary Results of Initial Value of Information Analysis table below.

The information value of each of these was computed with the "EVPI" method. In general, the Expected Value of Perfect Information (EVPI) represents the maximum value of additional information even if that information is perfect. This gives a good idea of the maximum cost that should be spent for an additional measurement.

EVPI is calculated by estimating the effect on a decision if there were no uncertainty in a particular variable. For example, if we knew exactly what the productivity impact of a virus impact would be, there should be a higher chance of making the right anti-virus investment decision. The difference between the expected outcome of an investment with this perfect information and the outcome without this information is the EVPI for that variable.

As a rule of thumb, 2% to 20% of the EVPI of each variable should be spent in further measurements. The table below shows recommended ways for expending effort in more measurements. In addition to the EVPI, the cost and feasibility of additional information gathering are considered when identifying measurement priorities.

For example, even though fraud costs had the highest EVPI the team felt that it was unlikely that an extensive measurement effort in this area would produce useful results. It was decided that any additional reduction in uncertainty would most likely come from a few additional interviews and phone calls with auditors and others that may track fraud losses. Therefore, the measurement effort was small although the EVPI was high.

Phase 2 Results

The Value of Information Analysis (VIA) indicated that further measurements were needed to reduce uncertainty on fraud losses, cost of logical intrusions, and productivity impact of viruses and the implementation costs of VAPKI. See Summary Results table for more information.

For fraud, the team engaged in additional research of any historically documented experiences including internal VA data as well as outside studies on cyberfraud.

The team also initiated a security survey of VA department IT staff to better estimate productivity losses and possible fraud losses due to security incidents.

Finally, the team further analyzed the cost of implementing VAPKI since this cost was fairly uncertain.

Measurement Maxims

- You have more data than you think: Be resourceful in finding existing information
- You need less data than you think: Be resourceful in making useful conclusions from limited information
- Measurement is usually easier than you think: the first measurement method you think of is probably "the hard way", think of the more resourceful, simple method

Summary Results of Initial Value of Information Analysis (VIA)			
Set of Variables	Expected Value of Perfect Information	Justified Effort (cost of the effort should be 2-20% of EVPI)	Measurement Approach
Fraud, property loss, legal liabilities	**$787,763**	Several work-weeks	The team felt that uncertainty would be difficult to reduce significantly regardless of effort expended. We then decided to at least attempt to make calls within the audit function of the VA and determine what information is available.
Optional investment costs	**$286,162**	A few work-weeks	This is limited to the costs of the VAPKI, TEAM and Simpilfied Sign-on. The team members will proceed with more detailed design in those areas to make better cost estimates.
Logical intrusions	**$241,790**	A few work-weeks	This will be a passive measure from the minimum investment of the Instrusion Detection initiative. This system will produce these results anyway but the results will now be analyzed specifically to support this metric.
Total effect of viruses and reduction of viruses due to investments	**$151,910**	Two work-weeks or less	A post-incident survey will be implemented that will focus on productivity losses from a virus shortly after the virus occurs. Anti-virus software will report on the difference in virus occurances due to other initatives.
All other variables	**Under $1,000**	None	

Phase 3 Results

The research of historical data help to significantly modify the range for annual fraud losses. The internal data was not as much help as external studies that went into much more detail.

One external study in particular had a significant effect on the opinions of the estimators. A report from the office of Senator Fred Thompson "Government Waste, Fraud & Abuse at Federal Agencies" claims to have found $220 Billion in federal government funds lost (see inset). The estimators realize that not all of this is due to unauthorized computer access but it still caused them to increase their estimate of fraud losses due to this reason. But they also realize that the VA represents a large percentage of the federal government budget and a similar proportion of these losses may be due to the VA.

No advanced statistical method was required to interpret the impact of the Thompson Report.

The estimators simply considered the information and provided a new (subjective) calibrated estimate. From calibration training, the estimators learned they could consider qualitative data or incomplete quantitative data and modify their subjectively evaluated uncertainty. In this case, the information from the report caused the estimators to modify the range for annual fraud losses due to internal unauthorized access (see Summary of Phase 3 Measurement Results table).

The security survey got 11 responses out of about 50 surveys distributed. The survey form distributed is shown in Appendix 1. This is a small sample size but it still managed to reduce uncertainty since some of the initial ranges were already very wide. The survey focused on the productivity impact of virus attacks but it also asked questions about fraud losses. Although the results were somewhat indefinite for some variables, the ranges of other variables were modified as a result of the survey.

Excerpts from the Sen. Thompson Report
(www.senate.gov/~thompson/pr012600.html)

WASHINGTON, DC - Senate Governmental Affairs Committee Chairman Fred Thompson (R-TN) today released an alarming compilation of government waste detailing $220 billion in taxpayer losses. In 1998 alone, $35 billion in taxpayer dollars was lost due to government waste, fraud, abuse and mismanagement.

It's difficult to track exactly how much the federal government loses to waste, fraud, abuse and mismanagement primarily because federal agencies are not required to keep this information and most don't. With input from the agencies' Inspectors General, the Committee was able to uncover $35 billion in wasted 1998 taxpayer dollars and $220 billion overall.

The Committee's compilation of government waste includes:

- Defense Dept. maintained $11 billion in inventory it didn't need;
- Energy Dept. invested $10 billion in projects that they never completed;
- Education Dept. paid out $3.3 billion in student loans that students failed to repay;
- Agriculture Dept. sent out $1.4 billion in food stamps to ineligible recipients.

Finally, the more detailed cost estimate for VAPKI resulted in a significant modification to ranges for VAPKI initial and ongoing costs.

Each of these new ranges replaced the wider existing ranges in the model. This is how observations are used to improve an existing model. Every observation results in less uncertainty, i.e. more narrow ranges, about each of the quantities observed. The narrower ranges result in a model with less uncertainty.

See the following table (Summary of Phase 3 Measurement Results) for a summary of modifications made to the ranges of specific variables.

Summary of Phase 3 Measurement Results

	Initial Range	Adjusted Range
Annual Fraud losses due to internal unauthorized access	$10M to $100M	$80M to $180M
Number of pandemic virus attacks per year	1 to 4	2 to 4
Average number of people affected by a virus	30k to 80k	25k to 60k
Percentage productivity loss due to virus outbreak	12% to 80%	15% to 60%
Percentage of veterans affected	2% to 8%	2% to 15%
VAPKI initial costs of VA-wide roll-out	$2.5M to $4.5M	$1.3M to $2M
VAPKI annual costs of VA-wide roll-out	$1.2M to $1.6M	$1.1M to $1.3M

Phase 4 Results

Key Strategies

The analysis of the Phase 3 measurements clearly pointed to the following strategies for the performance metrics of the ISP:

- Put a high priority on implementing Anti-virus and the minimum component of Intrusion Detection
- Do not proceed with the defined "optional" component of Intrusion Detection (a savings of at least $30M, a small % of which should be reallocated to pure metrics efforts)
- Roll-out VAPKI on a security-priority basis based on passive feedback (see VAPKI roll-out criterion)

- Defer investment in optional TEAM investment until passive feedback can be used to update its CBA
- Implement measures for the Seven Key Metrics (below)

Seven Key Metrics

There are over 100 variables in the model, about 20 are unique and only seven are critical for future metrics (i.e., they have the highest information value)

- Fraud losses per year
- Intrusions per year
- Pandemic virus events per year
- Number of VA personnel affected per virus outbreak
- Duration of productivity impact per virus outbreak
- Average annual cost per affected person
- Productivity loss during duration of outbreak

Detailed Metrics Information

Metric: Fraud losses per year
Method : Continued analysis of reported frauds is critical. Every step should be taken to encourage fraud reporting (emphasize in TEAM). Ultimately, diligent reporting and periodic audits are the best measure of fraud losses.

Metric: Intrusions per year
Method : Intrusion Detection should report

intrusions per year by VA area so that the following can be compared:

- Groups that have been trained under TEAM vs. groups that have not
- Groups that have rolled out VAPKI vs. groups that have not
- Groups that have implemented a simplified sign-on solution vs. groups that have not

This is the basis for measuring impact of these initiatives on intrusions per year: "Reduction in Logical Unauthorized Intrusions".

Metric: Pandemic virus events per year
Method : Anti-virus should report virus outbreaks by VA area so that groups that have been trained under TEAM vs. groups that have not can be compared. This is the basis for measuring impact of TEAM initiatives on virus outbreaks.

Metrics: Virus productivity impact – specifically:

- Number of VA personnel affected per virus outbreak
- Duration of productivity impact per virus outbreak
- Average annual cost per affected person
- Productivity loss during duration of outbreak

Method : A random post-event survey of the affected areas should assess each of these (only minor rewording of the current survey is needed). The VIA indicates that a phone survey of 50 to 80 respondents should be sufficient (this should be possible in two days just after the event). Anti-virus reports will also help to put ranges on number affected and duration.

VAPKI Roll-out Criterion

The roll-out of VAPKI should occur in a particular order and it should only be implemented when a certain criterion is met. The main effect of VAPKI is to reduce unauthorized intrusions and the main cost of unauthorized intrusions is fraud.

Putting a priority on rolling-out VAPKI where fraud is the highest ensures the maximum impact of VAPKI. Wherever possible, VAPKI roll-out should be prioritized by "Annual fraud losses per person". The cost of implementing VAPKI is on a per-person basis therefore implementing on an annual fraud per person basis would be optimal. The following formula should be used to test if a particular group of individuals should have VAPKI:

VAPKI Roll-out Criterion

$$\frac{1.1\% \times (\text{group fraud costs/yr})}{(\text{number of people in group})} > \text{VAPKI cost/person}$$

The quantity 1.1% is the expected reduction in fraud costs per person where VAPKI is implemented. In other words, if the annual fraud costs per person were $500 then the VAPKI costs per person must be less than $5.50 per person to justify rolling it out. Any group that does not

meet this rule should be low priority for VAPKI or not receive it at all.

According to the estimates average fraud costs per person per year may be between $330 to $750. Differences among groups within the VA will vary by even more than this. In some groups fraud costs per person per year may be thousands of dollars. In such high risk groups the costs of implementing VAPKI is easily justified. However, many groups will not be able to justify the per person license fee for VAPKI by this rule and therefore, should not have VAPKI.

Six-month Review

A review of all reports generated by VA CIRC, Anti-virus, and Intrusion Detection should occur twice a year. Each of the Key Seven Metrics should be updated with all information available. The spreadsheet model should be updated to reflect these findings. Key decisions on continued roll-outs will be affected

A method will be used to assess the total number of viruses and intrusions based on cross-referencing reports from anti-virus, intrusion detection, and VA CIRC. The following formula insert shows how to aggregate VACIRC and intrusion detection but, intrusion detection could be substituted by anti-virus and the method would be the same.

Formula for aggregating reported incidents

$$X=(A+B)/A*C-C$$
$$\text{Estimated total} = A+B+C+X$$

A = number of incidents reported by both VACIRC and intrusion detection

B = number of incidents reported by VACIRC but not by intrusion detection

C = number of incidents reported by intrusion detection but not by VACIRC

X = estimated number of incidents unreported

Additional Recommendations

The contractor also made recommendations in the following investment areas :

Investment Area : Simplified Sign-on

When specific solutions in Simplified Sign-on are formulated they should be given a full risk/return analysis. Currently, no specific investments are identified for the "optional" piece of Simplified Sign-on. A variety of bio-metric technologies and other solutions must still be assessed. When particular plans are defined then they should be given a separate risk/return analysis with the AIE approach. This will ensure that the investment is economically justified. The only reason a risk/return analysis cannot be done at this time is because no specific investment has been defined in this area. Without a specific project scope and purpose identified, it will not be possible to do the proper risk/return analysis of the investment.

Investment Area : Training, Education, Awareness and Message Building (TEAM)

As more accurate costs for specific optional TEAM solutions are identified, they should go through a risk/return analysis with the AIE approach. As with Simplified Sign-On, this will ensure that the investment is economically justified. But, again, this cannot proceed until a specific project scope is identified.

Investment Area : IT Systems Certification and Accreditation Program (ITSCAP)

The VA plans to develop an ITSCAP scoring model to assess the security of a system before it is put into production. The current approach consists of a checklist of attributes that will be assessed for each system under the assumption that the attributes say something about the security of the system. The checklist would create a score or report card which VA would use to determine if the system is safe. The scoring model will be more accurate if it is based on a real statistical analysis that predicts security risks based upon system attributes and weights the factors according to actual security risks instead of an arbitrary scoring method.

Appendix 1: Summary of Minimum vs. Optional Investments

Investment	Minimum	Optional
VA Public Key Infrastructure (VAPKI)	VAPKI certificate licenses, VAPKI help desk, training and documentation, and consulting.	N/A
VA Computer Incident Response Capability (VA-CIRC)	Ensure that there is a capability to provide help to users when a security incident occurs in the system and to share information concerning common vulnerabilities and threats. This capability shall share information with other organizations, consistent with NIST coordination, and should assist the agency in pursuing appropriate legal action, consistent with Department of Justice guidance	Procure a full-time, dedicated VA-CIRC contractor staff with increased responsibilities and capability to: Evaluate, prepare, and distribute Security Alerts, Notifications, Patches, and Fixes; Coordinate vulnerability and incident response data via secure communications; and Proactively share IT security information, tools, and techniques.
Antivirus	Protect VA's networks, systems, desktops and applications from virus attacks.	N/A
Training, Education, Awareness and Message Building (TEAM)	Provides for the mandatory periodic training in computer security awareness and accepted computer security practice of all employees who are involved with the management, use or operation of a VA computer system within or under the supervision of the VA.	Provides for the following additional investments: a. Web-Based Modules addressing non-security IT subject areas b. Web-Based modules addressing ISP product releases c. Log-On Bulleting Development/distribution d. Computer Security Day e. Message Building Project (public relations) f. Reaction to Ad Hoc security related events (e.g., Computer Stand Down Day) g. ISP information booth h. Expanded training i. Professional certification j. VA InfoSec2001 Conference k. Awareness Brochures and Posters l. Participation in VA Information Technology Conference
VA IT Systems Certification and Accreditation Program (ITSCAP)	Certification it a technical evaluation of an IT system to see how well the security requirements are met. Accreditation is the official management authorization to proceed. The minimum investment is required to complete this process.	N/A
Intrusion Detection (IDS)	Includes coordinated detection along VA's network perimeter, which has today roughly seventy points of presence to public or external networks such as the Internet. Also includes detection surrounding the few core financial disbursing systems, which can be implemented at the application- or host-based IDS level.	Detection on the interior of VA's network more generally, and the distributed mission-critical systems, particularly VA's distributed hospital management information system.
Simplified Sign-On	Provide simplified sign-on technology for the roughly thirty thousand caregiver staff of the Veterans Health Administration (physicians, nurses, etc.), whose productivity is most harmed by repetitive and time-consuming sign-on events. Caregiver staff are most in need of a sign-on that is "hands free", while still being adequately secure and providing for individual accountability	Provide for other cadres of VA staff who will benefit from such sign-on technologies, but not to the extent that caregivers do.