CERIAS Tech Report 2014-9

The Indiana Cybersecurity Services Center (INCSC): A Cost-Benefit Analysis for K-12 Schools

by Vargas Silva, Hans
Center for Education and Research
Information Assurance and Security
Purdue University, West Lafayette, IN 47907-2086

Graduate School Form 30
(Revised 08/14)

PURDUE UNIVERSITY
GRADUATE SCHOOL
Thesis/Dissertation Acceptance &

This is to certify that the thesis/dissertation prepared

By HANS C. VARGAS SILVA

Entitled
THE INDIANA CYBERSECURITY SERVICES CENTER (INCSC):
A COST-BENEFIT ANALYSIS FOR K-12 SCHOOLS

For the degree of Master of Science

Is approved by the final examining committee:

DR. MELISSA JANE DARK

DR. JAMES ERIC DIETZ

DR. BRANDEIS H. MARSHALL

DR. SAMUEL P. LILES

To the best of my knowledge and as understood by the student in the Thesis/Dissertation Agreement, Publication Delay, and Certification/Disclaimer (Graduate School Form 32), this thesis/dissertation adheres to the provisions of Purdue University's "Policy on Integrity in Research" and the use of copyrighted material.

DR. MELISSA JANE DARK

Approved by Major Professor(s): _____

_____

Approved by: DR. EUGENE H. SPAFFORD 09/10/2014

Head of the Department Graduate Program Date

THE INDIANA CYBERSECURITY SERVICES CENTER (INCSC):

A COST-BENEFIT ANALYSIS FOR K-12 SCHOOLS. "

A Thesis "

Submitted to the Faculty "

of "

Purdue University "

by "

Hans C. Vargas Silva "

In Partial Fulfillment of the "

Requirements for the Degree "

of "

Master of Science "

December 2014 "

Purdue University "

West Lafayette, Indiana "

To my wife, for her unconditional love and support during these 2 years. "

To my parents and family, for their constant prayers and encouragement. "

To Hans de Groot, as an earlier financier of the dream of college education. "

To my kids, as this serves as example and encouragement for their own future. "

ACKNOWLEDGEMENTS

The opportunity to be a graduate student pursuing a Masters in Information Security is possible thanks to CERIAS at Purdue University, and to the SFS program, for that I am most grateful.

The timely encouragement and advice of professor, advisor, teacher and committee chair: Dr. Dark. I appreciate that you saw potential despite of difficulties during this journey. Thank you for your patience and mentorship.

To the rest of my committee, Dr. Marshall, Dr. Liles, Dr. Dietz, thank you for the lessons shared, I extend my deepest appreciation for your support, feedback and advice.

Thanks also to Paul Baltzell at Indiana Office of Technology for his continuous support to consider me part of different and challenging projects like the INCSC.

Thanks to all the school corporations who agreed to participate of this research.

Thank you Gina Sheets, for been instrumental in making timely connections.

TABLE OF CONTENTS "

Page

Page

Page

LIST OF TABLES "

LIST OF FIGURES

Figure Page

ABSTRACT "

Vargas Silva, Hans C. M.S. Purdue University, Decenber 2014. The Indiana Cybersecurity Services Center (INCSC): A Cost-Benefit Analysis for K-12 Schools. Mayor Professor: Melissa Dark.

The aim of this thesis is to determine if there are greater benefits than costs associated in the participation of public K-12 school corporations in the Indiana Cybersecurity Services Center (INCSC). This thesis is an *ex-ante* cost-benefit analysis policy assessment of the INCSC. The study consisted of a sample of 6 school corporations from which 5 were classified as small and 1 was large. Three methods were considered for data collection; however conducting interviews was the most effective method due to the interaction with IT personnel from each organization in order to analyze current costs related to 4 areas of interest: (a) networking hardware; (b) Antivirus software; (c) computer hardware; (d) IT personnel. These costs were compared to those potential costs if products and/or services would be procured through the INCSC.

School corporations, with the goal to enhance their level of information security, would only receive benefit from participating in the INCSC when procuring networking equipment and Antivirus software. The author also recommends exploring the costs and legal implications of data breaches as well as considering insurance products. "

CHAPTER 1. INTRODUCTION

1.1 Background

The pervasiveness of technology in society, regardless of its many benefits, has also made visible vulnerabilities from the common platforms and systems that are shared and accessible to others around the world. Today's cyber challenges have become analogous in many ways to an arms race or the mutual assured destruction concept, in which the "bad guys" have the same technology capabilities, the motivational edge, and have shown less reluctance to use their cyber capabilities against us under the non-attribution scheme.

We are attacked by well financed – since several state-sponsor actors operate under an enterprise model – trained and smart personnel. From an attacker perspective, they benefit from being right once in a while, on the other hand compared to the defensive side, having to be right every time. Statistics for attacks on US private industry can be hard to find; no one is eager to report a breach unless they have to disclose it. Statistics for the U.S. government sources are more accessible and revealing. The U.S. Cyber Command said in 2013 that there are on average around 250,000 probes/attacks on U.S. government networks an hour, or 6 million a day, and among the attackers are some 140 foreign spy organizations.

According to the federal Government Accountability Office (GAO-13-462T), the number of actual breaches grew from 5,503 in 2006 to 48,562 in 2012, or 882 percent. The cost of cyber-attacks and the cyber probes to the United States are astounding. Antivirus firm Symantec in its “2013 Norton Report” estimated the global direct cost of cybercrime at $ 113 billion (up from $110 billion the previous year) and the average cost per victim of cybercrime to $298 (from $197 in 2012).

There is lack of enterprises that accommodate both private and public sectors dedicated to cybersecurity. It seems that both sectors have remained isolated, only solving problems related to their sectors and not focusing on common or overlapping problems. The state of Indiana is proposing to develop an organization that is a public-private partnership to address public and private cyber security needs within the state. This initiative is called the Indiana Cyber Security Service Center (INCSC).

The state of Indiana currently has a centralized Information Technology department called IOT (Indiana Office of Technology) that serves all state agencies. IOT procures products and services on behalf of the state to serve the need of IT solutions for state agencies. IOT was created by the legislature in July 2005 with a goal of establishing standards for a technological infrastructure that improved and expanded the electronic services offered by the state. The mission is to “provide cost-effective, secure, consistent, reliable enterprise technology services to its partner agencies so they can better serve Hoosier taxpayers”.

The idea of creating the INCSC (Indiana Cybersecurity Services Center) responds to the need to prevent serious consequences from cyber-attacks that disrupt, steal, and "

damage state agencies, businesses, and individuals. The INCSC project represents the concept of a Public Broker of Private Services as the vehicle to dispense Security-as-a-Service. It would be created by the partnership and collaboration of several important actors: 1) The Board, formed by a selected group of institutions that have the responsibility to actively formulate the strategy, specify the common needs and deploy the solutions among their respective institutions and other customers; 2) Industry Partners, are key global providers of IT security products and services that will be offered to the customers in order to offer effective protection from cyber-intrusions, data breaches , and disruption of business operations; 3) Customers, formed by a diverse array of state and local government institutions, private businesses, schools (K-12), and universities.

Several organizational improvements are necessary across many governmental, educational, and private organizations before this plan is set in motion to effectively influence the way the State addresses cybersecurity. The creation of this new organization represents an alternative solution to current problems in the realm of cyber-insecurity for the State. The INCSC will provide statewide policies for the enforcement of a unified cybersecurity strategy against attacks, as well as provide affordable access to specialized security services, both in an effort to mitigate and defend against cyber-threats. Another focus of the INCSC would be to collaborate with higher education institutions to continue research in key areas of cybersecurity to strengthen Indiana protection against potential threats.

The State of Indiana already has a centralized information structure also known as IOT, which offers of infrastructure and software as a service to communication service. The mission of IOT is “providing cost-effective, secure, consistent, reliable enterprise technology services to its partner agencies so they can better serve Hoosier taxpayers”. This service model is adopted by all state agencies that contract and pay for subscribed services. A similar case would occur for services rendered by the INCSC, which would fall under the umbrella of IOT as a product/service provider; the majority of current security services offered by IOT will then fall under the new jurisdiction of INCSC.

The challenge presented is to convince state agencies and other actors (private enterprises and educational institutions) of the validity and novelty of the project in order to bring them aboard as participating customers on the INCSC, and by default, a part of Indiana cyber-strategic plan. A resulting benefit of joining in this partnership would be not only a deeper understanding of the variables in play related to cyber-attacks to Indiana state networks and other INCSC customers, but also that the delivery of centralized security services would provide more benefits than the current or future costs of cyber-defense. This is particularly acute when addressing the issue of affordability, especially when referring to K-12 school corporations, of which many may struggle allocating funds to improve their cybersecurity.

The development of the INCSC would occur in three phases. In phase one service will be provided to a core group members consisting of the “Board” (conformed by IDHS-Indiana Department of Homeland Security, IOT-Indiana Office of Technology, ING-

Indiana National Guard, ISP-Indiana State Police, Purdue University, Indiana University, and Indiana Executive Branch: Governor's Office); "Industry Partners": McAfee (Intel), Cisco, and HP among a few others; "other state agencies"; "local governments"; and "K-12 school corporations" (which are the primary focus of the author). Phase two would offer services to critical infrastructure businesses and security-as-a-service to businesses in Indiana. The final phase will attempt to provide educational resources and key services to the general public (i.e. identity theft protection).

This thesis is an *ex-ante* cost-benefit analysis policy assessment of the INCSC. This analysis is necessary in order to justify the relevance and importance of this project to Indiana's executive and legislative branches, heads of State agencies, local businesses, and constituents.

1.2 Research Question

Would participation in the INCSC provide more benefits than the costs associated with cybersecurity for K-12 Schools in Indiana?

1.3 Significance

Today our modern society relies deeply on the Internet and computer systems, for many of its day to day functions, including communications, transportation, finance, and medicine. Our government entities are not the exception, due to the collection and storage of citizens' personal identifying information such as: birth/death records, social security numbers, licensing, tax records, etcetera. "

The alarming increase in volume and sophistication of cyber security threats demand that we remain alert about securing our systems and information. From disclosed data breaches we've learned that hundreds of millions of records are compromised every year, and new attack methods are launched continuously.

The State of Indiana has taken notice of the eminent risk of compromised information systems and the impact that could have for the state of the economy. This sentiment is also shared by Indiana state agencies, which under the umbrella of the executive branch are ultimately responsible and the safe keepers of their information. Indiana's critical infrastructure, businesses and citizens have also taken notice of the current increasing trend of data breaches and identity theft, and see the need for advanced protection mechanisms.

IOT has centralized infrastructure and Information Technology services for state agencies; the existence of a dedicated cyber security center could set in motion policies that would further complement and improve the scope of security services through the implementation of the INCSC. This initiative would also facilitate the introduction and implementation of new security services that are currently not offered by the State. By partnering with industry leaders in this area these new services would not only available but also more affordable.

At the core of this effort are K-12 schools and local governments (city and county) who are especially sensitive when it comes to affordability, due to limitations and budget constraints, which vary from county to county or from school corporation to school corporation. K-12 schools face obstacles in their ability to afford enhanced

security products and/or services due to budget constraints. For that reason, performing a cost-benefit analysis (CBA) would potentially highlight the benefits of K-12 schools participating in the INCSC, as they may receive a higher number of benefits (realized and unrealized) than implementation costs; which would also increase the likelihood of their participation in the project. When referring to the participation, the author focuses on K-12 schools because – in contrast to state agencies that already make use of security services, have or intend to increase their spending towards security services – school corporations might not have the means or flexibility to do so. The decision to participate will have to be grounded on sound evidence that the benefits outperform the costs.

Centralization of resources, leveraging large-scale purchasing, and improving prevention through faster containment of threats could have an impact in reducing the costs of cyber security for state and participating organizations. The development of a cyber-security ecosystem throughout a public-private partnership in collaboration with higher education, the State, and leading technology companies would provide an opportunity not only of cost saving benefits, but perhaps the fostering of educational opportunities for students at multiple levels while providing hand-on job experience with real threats and cutting edge technical products. Creating a model to enable broader information sharing of threat data between state and federal agencies, educational and research institutions, and providers of Indiana Critical Infrastructure could enrich the State (INCSC) cyber-threat intelligence to enhance future decision making to better cyber-assets protection.

There is not previous reference point similar to this project; the importance of having a well thought-out plan is crucial, but it also enhances the relevance of using a CBA for this particular case. Indiana has definitely taken a proactive approach towards cybersecurity, attempting to become an active player in ways that positively impacts the level of cybersecurity of state agencies, business and citizens.

1.4 Limitations "

The limitations essential for this study were: "

1. " The study did not evaluate the wholeness of IT environment of school corporations; instead it was limited to the scope of the study.
2. " The study consisted of a small sample of school corporations in the state of Indiana and it might not allow broad generalizations.
3. " The study did not completely assess the IT personnel capacity in respect to specialized information security technologies and systems.
4. " The study response to interviews was limited and restricted to central Indiana (33 counties in the middle third of the state) school corporations.
5. " The study was limited by the high rejection rate of school corporations to be interviewed and/or share financial information.
6. " The study was limited by the scope of the interview questionnaire as it could have allowed for further discovery of computer hardware specific and also detailed personnel task tracking.

1.5 Delimitations

These are the delimitations under which the research would be carried out:

- The author will focus on cost-benefit associated to K-12 and not state agencies or businesses that may be part of the INCSC.
- For cost-benefit analysis, the researcher will be focusing on the variables described under methodology.
- The study was limited by scope to hardware, software and personnel; prevention and detection of intrusions; and confidentiality of information against network attacks. Details about those specific scopes will be described under methodology
- Private and charter schools will not be considered targets for the scope of this research, due to different models of budget funding.

CHAPTER 2. LITERATURE REVIEW

2.1 Cybersecurity

Though affairs of cybersecurity at the state level receive less attention than national cybersecurity, this does not mean that there are less acute than those at the national level or related to federal agencies. This section explores cybersecurity at the federal level as it will give us an idea of the nature of the problem and from there extrapolate down to the state level as the problems tend to be similar.

As reported by GAO, the Government Accountability Office in March of 2013 (GAO-13-34), the number of cyber incidents affecting computer systems and networks continues to rise. Over the past six years, the number of cyber incidents reported by federal agencies to the U.S. Computer Emergency Readiness Team (US-CERT) has increased from 5,503 in fiscal year 2006 to 48,562 in fiscal year 2012, an increase of 782 percent. Based on the incidents from 2012 it could be pointed out that improper usage, malicious code, and unauthorized access were the most widely reported types across the federal government; accounting for 55 percent of total incidents reported by federal agencies

Caplan (2013) argues that reports of incidents related to cybersecurity have a direct impact on national security, intellectual property, and individuals; the abundance

of those reports justified the need of measures to solidify the national security as represented by the Cyber-Security Act of 2012. Among these reports are data loss or theft, economic loss, computer intrusions, and privacy breaches. Incidents of this nature illustrate the impact that cyber-attacks could have on federal, state, and military operations; critical infrastructure enterprises; and the confidentiality, integrity, and availability of information from personal, public and private sectors. For example, according to GAO-14-34 (2013) based on US-CERT, the number of incidents -agency-reported- related to personally identifiable information increased 111 percent, from 10,481 incidents in 2009 to 22,156 incidents in 2012.

The federal government's information security responsibilities are established in law and policy. The Federal Information Security Management Act of 2002 (FISMA) sets forth a comprehensive risk-based framework for ensuring the effectiveness of information security controls over information resources that support federal operations and assets. In order to ensure the implementation of this framework, FISMA assigns specific responsibilities to agencies, the Office of Management and Budget (OMB), the National Institute of Standards and Technology (NIST), and inspector generals.

State governments comply with federal laws and also have the authority to legislate over other issues according to state law or by filling a void from federal law. The state data breach disclosure laws are a prime example of state legislation in the cyber security arena.

Cyber capabilities from a federal to a state level vary greatly. The federal government has multiple institutions designed to specifically address cybersecurity, while states typically do not. In the state of Indiana, the only institution with the same specific purpose is the IOT. For that reason, there is a growing need from states like Indiana to take action towards protecting their state agencies, critical infrastructure and citizens. It would be unfair to say that existing US federal resources are not available or do not serve U.S. states cyber-related issues. Perhaps the point is that those resources are ultimately shared among all 50 states and serve a national pool of inquiries. The idea behind the INCSC is to create a state administrated resource that provides information security services in a permanent and ongoing basis for the benefit of the state of Indiana, as well as functioning in collaboration with federal agencies.

2.2 Cybersecurity as a Polycentric Problem

The technological advancements that we currently enjoy are also the platform for the new cyber-warfare, hacktivism, and industrial espionage, to mention a few. The influence that cybersecurity has to multiple levels of our society does not get any easier to manage as it escalates from local, regional, national to international levels; this has the effect to hinder policymaking in the presence of the increasing economic and political cost of cyber-threats.

The Internet has become a shared resource for societies across the world, where information is shared and distributed as a common good; in contrast to that the Internet also allows for the isolation and restriction of access to information in many cases in "

protection of privacy, intellectual property and in advancement of commerce. How are we then addressing the issue of cybersecurity? The answer is not simple, but I would say that we are currently not doing enough to address the issue in a sustainable way, especially when there is a sense of isolation mentality of the roles and functions of public and private interests with respect to cybersecurity.

There is an initiative to reframe the cybersecurity away from the vulnerabilities that are unlikely to more concrete ones, mainly orientated towards cyber-peace (Nye 2012). This is based on the understanding of how the threats are evolving; and focus on building-up defenses from private and public sectors in order to effectively manage cyber-attacks.

According to Shackelford (2012) “cyberspace is at best a pseudo commons given that the realities of private and governmental control”, for that reason some of the principles of common analysis apply to cyberspace (i.e. the tragedy of the commons or collective action problems) but they behave in different ways; the understanding of these similarities and uniqueness provide action alternatives to better promote cybersecurity.

Polycentric regulation is at the core of a proposed governance framework. Elinor Ostrom (2008), argues that there are significant benefits from self-organization, leveraging levels to network problem-solving regulations, and the co-existence of public-private through communal management. In addition to that she also says that it would be insufficient that a single governmental unit could be capable to address global issues as cyber-attacks. The polycentric approach represents the participation of different "

organizations at multiple levels in order to create policies that promote cooperation, compliance, flexibility, and adaptability. This conceptual framework could be applied to a macro level, but it could also be used in smaller levels like in the case of the INCSC project sponsored by Indiana State.

The importance of this framework is shown when it is realized that cybersecurity is no longer a static and isolated problem; it's instead evolving in a dynamic environment and global in scale, delimited national borders and jurisdictional authority. The Internet has created the platform, according to some, to determine cybersecurity as a commons, as information becomes the common pool resource. This argument holds when the information to be accessed is intended as a public use, however the problem comes when either accessing information that is not for public consumption or in the case when overuse occurs through "information pollution" like in the case of spam messages or distributed denial of service (DDoS) attacks.

When referring to jurisdiction, this becomes very hard or nearly impossible to effectively be implemented, due to the lack of existent mechanisms to enforce regulations and prosecute offenders (to the commons). A solution will definitely have to come from the collaborative effort of several nations that agree upon international goals as they relate to cybersecurity. At a national level, it would then be necessary the creation of a bottom-up approach, by incentivizing systems where NGO's, small, medium and large governments engage in cooperative and competitive relationships, allowing the creation of new rules of engagement amongst participants. Drawbacks will

nevertheless relate to enforcement problems like free riders and the nature of the Internet.

At a lower (Indiana state) level –as a subsystem of a nation or international level– it could be stated that it would be possible to create a polycentric solution to cybersecurity problems in the state, by the participation of local parties (private and public) that want to develop better strategies to deal with the challenges presented by cybersecurity. The INCSC could very well represent the latest attempt to address the problem of cybersecurity from a polycentric perspective at a State level.

2.3 Collaborative Model

Accomplishing complete cybersecurity is a complex and difficult task; some venture to say that is an unrealistic expectation. Regardless of its complexity, solutions to cybersecurity do not rest only on a technology implementation level, but perhaps in a more important element: the human and social aspect of organizations. A great example of this paradigm is the initiative to address cybersecurity issues for the state of Indiana through the implementation of the INCSC.

The INCSC public-private paradigm is based on building collaborative organizations that can offer polycentric solutions to polycentric problems. Polycentric issues have many centers and/or several central parts. McGinnins (2005) said that a polycentric system of governance is a multi-level, multi-type, and multi-sector in scope, encompassing a wide array of organizations with complementary strengths and capabilities. The concept of polycentric governance refers to a variety of institutions

that provide favorable conditions for the use of a polycentric framework for governance, which enables aspects of solutions to be used together in order to achieve goals and help to solve problems.

McGinnis (2005) also stated that in a system of polycentric governance "a primary responsibility of central political authorities is to act and to support the capacity of self-governance for groups and communities at all levels of aggregation". Thinking about polycentric problems and approaches is difficult because of the inherent complexity.

According to Polski & Ostrom (1999) authors of the Institutional Analysis and Development (IAD) framework, such a framework "helps analysts comprehend complex social situations and break them down into manageable sets of practical activities. When applied rigorously to policy analysis and design; analysts and other interested participants have a better chance of avoiding the oversights and simplifications that lead to policy failures" (p 6). Cybersecurity as a polycentric problem requires a polycentric solution approach, and a model like the Institutional Analysis and Development (IAD) might provide the tools needed to formulate a robust and comprehensive solution with collaboration between Indiana State, private partners and participating members (customers), in order to provide state-of-the-art security services.

The INCSC very well fits this description given the fact that as proposed new organization (institution), it would draw its strength from the collaboration of its members, all united with the common goal to better defend and withstand cyber-attacks. The model of polycentric governance also will apply because different agencies

and businesses have to work in a collaborative environment. Another distinction worth mentioning is the desire of the State of Indiana to avoid imposing legislation on this new organization; instead it 1) pursues the dissemination of future benefits compared to the aftermath cost of a cyber-intrusion and 2) participation is not compulsory.

2.4 Risk Management

Risk management (RM) is considered in this section with the purpose of serving as a tool that could be used by K-12 school corporations to assess their particular levels of security. If a basic level of risk management is done at each school, this could be beneficial as preparative work for a cost-benefit analysis in the basis of understanding the current status in respect to the risk of the schools.

Risk management looks at what could go wrong, and decides on ways to prevent or minimize potential problems. RM encompasses three processes: risk assessment, risk mitigation and evaluation (MSISAC, 2012). Risk is the probability of suffering harm or loss. It refers to an action, event or a natural occurrence that could cause an undesirable outcome, resulting in a negative impact or consequence. Risk Assessment is the process of identifying threats to information or information systems, determining the likelihood of occurrence of the threat, and identifying system vulnerabilities that could be exploited by the threat; as such, it also allows the evaluation of what needs to be protected related to operational needs and financial resources. Risk Management is the process of taking actions to assess risks and avoid or reduce risk to acceptable levels.

In information security risk management should be appropriate for the degree of risk associated with the organization's systems, networks, and information assets.

According to the GAO (GAO-13-462T), assessment and management of risks continues to be a difficult task for government agencies, especially in the development and implementation of security controls, as well as in the monitoring of results. For the fiscal year of 2012, 19 out of 24 major federal agencies reported information security control deficiencies of financial reporting, and inspector generals at 22 out of 24 agencies cited information security as a major management challenge for their agency. The majority of the agencies had information security weaknesses in most of five key control categories: 1) implementing agency-wide information security management programs that are critical to identifying control deficiencies, resolving problems, and managing risks on an ongoing basis; 2) limiting, preventing, and detecting inappropriate access to computer resources; 3) managing the configuration of software and hardware; 4) segregating duties to ensure that a single individual does not control all key aspects of a computer-related operation; and 5) planning for continuity of operations in the event of a disaster or disruption.

The allocation of resources in cybersecurity is influenced by the notion of risk; therefore, risk is an important factor when using cost-benefit analysis to determine the right investment level. As mentioned by Gordon and Loeb (2005), “making risk assessment decisions for cybersecurity projects; that is, the cost of a security measure is compared to the expected loss avoidance, and if it costs less to implement the measure, the measure is recommended to be implemented”. The most difficult part of this type of

analysis is to determine what the risks are, to measure, and to quantify costs. After risk assessments are done, decisions are made based on the results from the risk assessment.

There is not much evidence that education institutions in the State of Indiana are required to conduct, in any specific frequency, risk assessments to their networks in order to discover unknown or document known vulnerabilities, threats, the likelihood of occurrence, and quantify the impact to their institutions. The concept and realization of risk might be soon become imminent to these institutions, although the purpose of the INCSC at this point does not include the performance of a network risk assessment, it might be a service offered later offered; it is thought to assist in the enhancement of cybersecurity capabilities for its participating members.

2.5 Cost-Benefit Analysis (CBA)

Cost Benefit analysis is often used to show the superiority of a project with respect to alternatives. In Boardman et al. (2006), Brenht et al. (2012), Campbell et al. (2003), and Snell (2010) a practical approach to cost-benefit analysis (CBA) is presented in the form of "determining the net benefit of a proposal relative to the status quo" where *net social benefits* (NSB) are the resulting of all the benefits minus all the costs. In cybersecurity related projects NSB could also be represented as the *net present value* (NPV) of an alternative with relation to the status quo.

In a cybersecurity project like the INCSC, the benefits are often related to cost avoidance; i.e. avoiding the costs of security breaches. The net present value (NPV)

model's approach is useful when considering incremental investment towards cybersecurity; in order to determine that viability and acceptance of the project, the NPV must be positive. Hence, a Cost Benefit Analysis according to Boardman et al (2006) could be used as a "policy assessment method that quantifies in monetary terms the value of all consequences of a policy to all members of society", this then would interact in order to produce a satisfactory result: cost and benefits to society as a whole, in this case the for the State of Indiana. While the decision to create a new institution in Indiana falls under the responsibility of the state actors, the use of CBA role is to serve as an aid in the decision making process in the allocation of state resources to address a particular problem.

Boardman et al (2006) present 4 types of cost-benefit analyses, from which 2 are the major types. The first major type is *Ex Ante* or standard CBA, this analysis is conducted while a project or policy is at its conceptualization phase. Ex-ante analysis assists in the decision making process to allocate resources to a specific project or policy. The second major type is the *Ex Post* CBA, which is conducted at the end of a project; at this point this analysis serves the purpose of learning about the class(es) of interventions throughout the project, and as a learning tool about whether particular classes of projects are worthwhile in the future. A CBA performed during the course of a project is called *Medias Res*, this CBA has some elements of the previous types; in the form of ex ante, it might influence decisions about the continuation of the project, while behaving as ex post, medias res analysis might be based in observations rather than predictions of some costs and benefits. Nevertheless, medias res could also serve as an

analysis tool to predict costs and benefits in future ex ante analysis. The last type of CBA is the comparative CBA. This type of CBA has more relevance for policy makers when learning about the efficacy of CBA's as a decision-making and evaluation tool. This CBA could be the comparison of ex ante vs. ex post or ex-ante vs. medias-res.

This project qualifies under the *ex-ante* analysis also known as the standard CBA; used mainly to demonstrate the superiority and efficiency of a particular alternative compared to other alternatives or the status quo. *Ex-ante* CBA is used while the particular project is under consideration or not yet executed. The value of ex ante analysis comes when making decisions as to whether and how to allocate resources to a project that is under consideration. In this particular case, the InCSC is the alternative in comparison to the status quo of K-12 information cybersecurity status.

2.6 Cybersecurity Cost-Benefit Framework

The type and size of an organization will determine the organizational needs for making decisions about the allocation of resources. In the area of Cybersecurity this is not the exception, which is why cost-benefit analysis is a method that is widely used for managing the resources of an organization.

This section attempts to present the cost-benefit principles that would make a case for a framework that allows managing cybersecurity resources, as presented by Gordon el at. (2006) there are two costs considered important to be distinguished from each other, especially when they relate to cybersecurity expenditures: operational cost and capital investments. Operational cost include those that will benefit a single period

(perhaps a fiscal year) of operations (i.e. cost of patching a system due to a data-breach), while a capital investment are those costs that will benefit the organization for several periods, and they might need to added to the balance sheet (i.e. purchase of a new intrusion detection system to reduce the vulnerability or likelihood of a data-breach of the company's network. According to Gordon et al. a good way to analyze costs related to cybersecurity would be to "think of them as capital investments with varying time horizons", then a one-year capital investment could qualify as operating cost.

The benefits of cybersecurity are in direct proportion to the cost savings or avoidance resulting from preventing data-breached, infections, loss of customers' trust, or loss of intellectual property, among the most important. A desirable goal would be to implement a level of security where the "net benefits" (benefits – costs) are at a maximum, since further implementation and investment might not have the desirable effect due to increasing costs.

2.6.1 Net Present Value (NPV) model

This model represents a tool for financial analysis, when comparing anticipated benefits and costs over periods of time, allowing putting in practice CBA. The way this model works is by discounting all the realized benefits and costs to the *present value* (PV). To simplify the financial analysis, it is common to assume that future costs and benefits are realized at the end of a period (i.e. fiscal, calendar, or educational year).

It would be safe to also assume that organizations already have some level of cybersecurity infrastructure implemented, which could be determined by a Risk

Assessment. For that reason incremental investments should be the term to be used in order to compare incremental costs to incremental benefits associated with enhancing cybersecurity for the organization (K-12 schools in our case).

$$\sum (N \qquad)/(N \qquad)N$$

NPV = net present value

C_0 = cost of an initial incremental investment

t = time period

n = total number of periods

B = anticipated Benefits

C = anticipated Costs

k = discount rate (assumed to be average cost of capital)

A NPV greater than zero shows that the PV (present value) of anticipated benefits exceeds those of the costs; the opposite is true if NPV is less than zero.

2.6.2 Internal Rate of Return (IRR) model

The IRR, also known as the economic rate of return, equals the discount rate that makes the NPV of the investment equal to zero. For that reason the IRR takes the values of the *net cash flow*, including the initial investment, and uses the present value of all anticipated net benefits (benefits – costs), and solves for the discount rate that makes the equal. See equation below:

$$\sum (\quad) / (\quad) N \quad) N$$

C0 = Cost of an initial incremental investment "

t = time period "

n = total number of periods "

B = anticipated Benefits "

C = anticipated Costs "

k = discount rate (assumed to be average cost of capital) "

When making a sound decision, IRR usually complements the decision that is guided in first instance by the NPV.

CHAPTER 3. METHODOLOGICAL DESIGN

This section documents the designing, collecting, and analyzing of data related to the cost associated with cybersecurity spending from school corporations in Indiana. This study will attempt to present a qualitative approach to the data collection in order to quantify specific aspects of costs associated with cybersecurity levels at school corporations (Quinn, 2001). The overview of this chapter consists of the research bias, study approach, data collection, and data analysis. This chapter concludes with a data aggregation and correlation based on the data analysis section in order to demonstrate the possibility to extrapolate the results to all school corporations.

3.1 Research Bias

This study is about establishing a baseline understanding of the present state of school corporations' efforts in information security and to evaluate if they could potentially benefit from participating in a state initiative that could provide its participants cost-effective benefits. The researcher's professional background and experience relates to information security, and from that perspective, it will be helpful for understanding the level of security of school corporations, especially when examining school level of investment and implementation of information security

solutions according to their IT budget. Furthermore, the researcher must disclose that even though his spouse is a licensed teacher in the state of Indiana, he does not have ties to any school corporation, neither has he worked or consulted for one before. The data collection will be targeted to school corporations within the state of Indiana, and the data collection might reflect personal subjectivity in the way questions were presented in order to gain insight information about specific cost related to information security spending patterns.

3.2 Study Approach

The overarching research question is stated in section 1.1, and the questions that were derived from it are intended to guide the discovery of spending patterns in the area of information security for school corporations. The research field in this case will be the each school corporation IT department, and depending on the corporation size it was to target the head of department, IT director, or IT personnel in the case of small schools. The State of Indiana, according to its Department of Education (DoE), has 383 school corporations per calendar year 2014 (including private and charter schools). Private and charter schools will not be considered in the scope of this research, due to different models of budget funding.

From the pool of public schools only, the researcher determined three major classifications according to the school corporation size: small, medium, and large. For the small level corporations consisted of two to nine schools will be considered. The

medium level had from 10 to 19 schools, and the large level had 20 to 68 schools in their corporations.

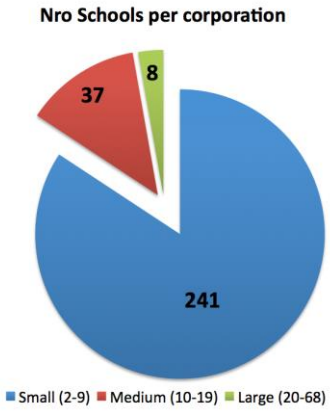


Figure 1. Indiana total schools (by size). [Indiana School Directory for 2013-2014]

3.3 Data Collection

The collection of data shall encompass the following three data collection instruments: budget template survey, interviews with school IT staff and the request of access to public school budget data. Financial data in the form of IT budgets are a very sensitive subject. For that reason resistance was expected in divulging such information to the extent of declining to participate from the project. Due to time constraints, the scope of the data collection was based on specific aspects of software, hardware and personnel in contrast with detection and prevention of network intrusions in school corporations (refer to Appendix A for more information).

3.3.1 Interviews

Interviews were the primary data collection method, as they provided the opportunity to further explore and understand the differences and similarities of school information security needs, strategies, and policies. An 'interview guide' was created to be used as a structure to be followed during interviews with school IT personnel, see Appendix B. The interview structure was used to fill-in specific information about the cost of products and services related to information security. To accomplish that the researcher, during the initial interview, asked general questions in order to get an idea of the overall strategy of the corporation with respect to their information security practices and/or compliance with existing laws (FISMA, FERPA/HIPAA). The structured and flexible guide was used in order to navigate the conversation towards the harvesting of budget expenditures line items. Due to distance, phone interviews or online meeting methods were permissible. A last component of the interview was to ask what product/services the corporation desires, or what would be purchased, updated, implemented if budget constraint was not an issue. This closing question helped to document IT staff response to, the now realized need of, information security improvements.

3.3.2 Budget Template Survey

A simple survey was created in the form of an IT budget template, which is used by the Indiana Department of Education to certify schools' technology plans, see Appendix B. This survey is intended to be another form of data collection, as it only requires school officials to respond with their consolidated IT budget line items for the

main categories as: personnel salaries, hardware, software, professional development, telecommunication, professional services/consulting, as well as any grants related to technology. This survey was administered by contacting directly schools or by the distribution of communication to school corporations through trusted channels.

3.3.3 Public Access to School Budget Data

The Indiana Department of Education (IDoE or Indiana DoE) under the Access to Public Record Act ("APRA") is required to generate and deliver a copy of those records that it maintains when formally requested; the contrary is also true ("If the records do not exist, certainly the [agency] could not be required to produce a copy….") according to Public Access Counselor 01-FC-61 and 08-FC-113 for the State of Indiana. This alternative avenue was explored as it could further complement the recollection of school corporations' spending behavior related to information technology. Indiana DoE, within its office of legal affairs, offers the service of access to data request for public records (See Appendix C).

3.4 Proposed Data Collection and School Classification

The collection of data was according to the proposed schedule (see Table 1) which included planned interviews, budget template survey, and requesting access to public budget data of schools as it related to IT spending.

Table 1. Proposed Data Collection Schedule

Type of data collection	Dates
Interviews	January 20, 2014 – February 20, 2014
Budget template	January 20, 2014 – February 20, 2014
Access to public records	January 20, 2014 – February 20, 2014

3.5 Analysis

The data analysis of interviews, surveys, and public records assisted in the discovery of specific cost and patterns of IT spending. The main interest is to find out the cost related to the protection and detection of school information security infrastructure (physical and logical). Some of the variables investigated are the number of IT personnel by school size, spending in networking hardware, computers, and spending in AV (antivirus) software as a trusted means of defense.

The researcher gained access to relevant information from the Indiana Office of Technology (IOT) personnel with respect to the potential discount rates for IOT sponsored services in the categories analyzed: HP for computers, Cisco Systems for network equipment and services; as well as, McAfee for enterprise antivirus solution and other services. These three IOT providers are currently working to include additional benefits (other related product and/or services) if school corporations decide to participate in the INCSC.

3.5.1 Aggregation and Correlation

This section attempted first to look for similarities amongst budget indicators, such as similar spending in a specific category (i.e. Software or specific subcategory

within software) aggregate data as well as allowed the grouping of school corporations when constructing a projection of potential benefits. Aggregation was beneficial in order to anonymize the source of information and to draw generalizations across schools. Aggregation was a technique used, since one of the parameters used to persuade schools to volunteer their IT budgets was that they would not be identified, the number of schools interviewed was not the number expected. Nevertheless, aggregation was still used.

Correlation represented a technique to determine spending ratios. For example it could be stated that small schools spend in average 10 USD for antivirus per student; compared to large schools that spend 7 USD per student. This will also support the premise for cost determination and generalization across the researcher pre-determining school's size. Based on the assumption of generalization of costs, then a base line of products/services will be determined and compared against positive or negative benefit findings resulting from the participation of the INCSC.

3.6 Cost-Benefit Analysis Planning

The approach to manage cybersecurity resources came from the appropriate comparison between cost and benefits. Benefits are in essence cost saving security controls implemented to avoid, minimize or deter cybersecurity incidents. As a descriptive ex-ante CBA, this project attempted to investigate the current costs ("without" scenario) and benefits ("with" scenario) that K-12 schools would potentially receive by participating of the INCSC, which represents a proposed model to enhance

cybersecurity capabilities. An important part of costs related to cybersecurity comes from adequately determining preventive and reactionary measures to address data breaches, such as unauthorized access or compromising the integrity of databases. Some of these actions respond to compliance with state and federal laws, and others relate to avoiding the impact from data breaches and losing the trust of the consumers.

By documenting current cost patterns and projecting real benefits associated with the access to enhanced delivery of information security, schools corporations have a better decision-making mechanism toward pursuing the improvement of their current state of cybersecurity. There is also the possibility that, depending of the school's size, the benefits may not be as attractive to a large school corporation as to a small one. A large corporation might have the budgetary means and capabilities to cultivate a direct relationship with providers and pursue enhanced benefits, given the number of users, servers, or represent larger contract accounts for technology providers. On the other hand, medium and small corporations might deal more often with budget constraints, and they might also potentially reap greater benefits from participating in a "consortium model" as it is represented by the INCSC. If, as result of this thesis, benefits are shown to exist in participating of the INCSC (an Indiana state project), then this document could be used to validate the novelty of the project.

Some of the possible findings could be through 1) providing similar benefits at lower costs, 2) providing enhanced benefits at the same cost, or ideally, 3) providing more benefits at lower costs.

3.6.1 Variables Considered

Some of the variables considered at this stage in order to help determine and quantify costs and project benefits for K-12 schools in Indiana are listed below. These variables will be used to guide the questions and could guide the scope of the survey and the interviews.

1. " The cost of Antivirus protection determined by cost-per-seat/node. Is the cost based on devices within a network or by another parameter? Is the cost tied to a contract length?
2. " The cost of computer network management (i.e. Active Directory or Novell e-Directory). Is the adoption of a particular solution based on price of solution or based on a standard across school corporations in the region?
3. " The cost of network infrastructure, in the form of managed firewalls and switches, could also include IP telephony. What is the cost associated to the implementation of network infrastructure? Does the corporation count on specialized/capable personnel to install and configure equipment? What is the planned renewal cycle and warranty expenses?
4. " The cost associated with data storage and restoration. What is (are) the backup solution(s) at school corporations? What is the backup capacity, and frequency?

5. " The potential unrealized cost of data breaches. Are there any measures in place to address potential liabilities (loss of reputation, loss of revenue, law-suits, cost of remedial actions, cost of investment on improvements)?
6. " The cost of IT personnel to perform information security tasks. What is the IT staff ratio compared to student-count, device-count, and other schools of same size. Do salary incentives seem to determine the level of expertise expected from IT personnel?
7. " The cost of internal and external information security audits. What is the frequency and cost of such audits? What are the costs associated with the implementation of recommendations? What are the most important security controls to be implemented?
8. " The cost of software licensing. What is the classification and costs (i.e. application licensing vs. operative system?) What percentage of corporations' technology budget is designated to recurring software costs?
9. " The cost of email solution. What is the corporation's strategy in respect to email delivery systems (i.e. in-house mail server, outsourced)? What are the costs associated with that solution?
10. " The cost of power backups. Are servers protected against power outages? Is the server room (datacenter) protected against contingencies?
11. " The cost associated with hardware. What is the renewal cycle and cost for computers (desktops, laptops, iPad's, servers)? What is the average cost budgeted? Are any of these purchases subsidized?

12. " The cost of technology projects setup, configuration, and integration. What are the costs? Are complex projects outsourced?
13. " The costs of compliance with state and federal laws. What are the costs related to content monitoring and Internet filtering management? Is this solution managed internally or outsourced to a third party?
14. " The cost of intrusion detection systems or data loss prevention. Are there any solutions implemented? Do corporations have plans to implement such solutions?
15. " The cost of insurance against information technology liabilities. What are the costs from policies in place to address the likelihood of: data breach, DDoS, loss of backup data, etcetera (if any).

CHAPTER 4. DATA ANALYSIS

As presented in the previous chapters, the main purpose of this research was to analyze if K-12 school corporations would receive more benefits than costs when participating in the INCSC project, and if such participation would allow those corporations to enhance their information security. In order to understand this problem, we first need to understand how schools operate with respect to their IT budget and how they get funded. A national view of this subject is provided by the US Department of Commerce (census.gov), where it confirms that schools as public institutions receive funds (revenue) from States through 'formula assistance monies', followed by property taxes paid to local governments, and lastly by federal sources.

This chapter discussed the data collected and the results from the individual interviews and surveys planned. From first showing the data collection schedule, followed by data collected from schools through interviewing their IT staff, reporting cost aggregation, potential benefits, and finally presenting and reporting on findings from the data collected in the form of a cost benefit analysis (CBA).

4.1 Data Collection Challenges

This section presents the *actual* schedule followed for data collection, which included interviews, the distribution of the budget template survey, and the request of access to public budget data of schools related to IT spending.

Table 2. Data Collection Timeline

Type of data collection	**Dates**
Interviews	January 20, 2014 – April 10, 2014
Budget template	January 20, 2014 – February 20, 2014
Access to public records	January 20, 2014 – March 20, 2014

The collection of data through the budget template (See Appendix C) was not successful. The main reasons were that school corporations do not provide such information via electronic format, or without the proper request and authorization. In one specific case the proper document was faxed requesting the superintendent office the release of that information; nevertheless, this attempt proved not to yield results. The budget template and the interview request were also sent out to a large number of school corporations through the Indiana School Safety Specialist Academy, inviting the participation of schools in this research. Those schools that responded were willing to be interviewed rather than filling out an IT budget template.

The researcher also contacted school corporations directly by email and phone. The researcher first addressed the superintendent's office and the IT Director or responsible person of that department. This attempt was also not as successful; only two schools responded to this approach, and out of them, one declined to participate

after deliberation. The second one refused to provide further data after the first interview, which usually only served to present the project as novel, and to get to know more about their current status in respect to IT services, as well as their greatest challenges and needs.

Another avenue to access information about school IT budgets was to formally request the Indiana Department of Education (IDoE) access to public data records respect to school corporation's budgets. A formal request was submitted and later granted in the form of access to all Indiana schools corporation financial reports, from where the researcher considered that the report: "Descriptive Listing by Fund and Account" was the most complete in terms of providing details (balance sheet). Unfortunately, this information did not contain any itemized costs that could be used to make comparisons amongst other school corporations.

The researcher was very optimistic about the willingness of school corporations to participate, especially given the number of corporations that fit the classification of small, medium, and large (see Table 4). Nevertheless, the number of schools corporations interviewed for data collection were 6 in total, these 6 corporation encompassed 85 different schools.

Table 3. Number of Corporations according Classification Criteria

Schools per Corp.	Classification	No. Corporations
2-9	**(S)** Small School Corporation	241
10-19	**(M)** Medium School Corporation	37
20-68	**(L)** Large School Corporation	8

In order to fulfill the agreement of non-disclosure of school corporation names or information that might identify them immediately, the following aliases (See Table 5) were created and assigned according to student count, based on 2013-2014 data from IDoE, and the number of schools in the corporation. As shown in Table 1, some of the challenges expected were that obtaining access to budget information wouldn't be an easy task. What the researcher didn't expect was that it would be very difficult to convince school corporations to accept to participate, and later provide detailed information about specific costs related to information security products and services; that is the reason why the interview schedule was significantly longer that the other two methods. Some schools offer open disclosure of their data, and while others agreed to participate at first, some later turned down the request about financial information. The offer of anonymization the reporting of the interviews was a mean for convincing schools corporation officials that the objective of this research was not to use individual school data to create a judgment of their information security level, but instead to use that knowledge to understand patterns across schools of similar conditions such as school count size, and school budget.

Table 4. Anonymization of School corporations

Alias	School Student Count	Number of Schools
SSC1	1473	3
SSC2	1005	3
SSC3	3110	5
SSC4	1049	3
SCS5	2280	4
LSC6	29803	68

Medium size school corporations were pursued, however none accepted to participate. From here going forward, the aliases will be used to make reference to the school corporation in question.

4.2 Description of Interviewed IT personnel

This section presents the interaction with those schools that agreed to be interviewed. The interviews were conducted in their majority on a one-to-one basis, with the occasional presence of another IT staff member in order to clarify or provide specific information related to a line budget item.

The interviews were conducted and the researcher interacted with a total of 5 males and 1 female. The following data will present a broad idea of the school corporation as background information that provides qualitative insight about the level of information security that each school has. The interviews were conducted according to an *interview template* (see Appendix B) that was used as a guiding tool. All interviewed participants had between 4 and 7 years working on that specific position and more than 10 years of experience working in a school setting in the same or similar capacity.

4.2.1 Interview with Small School Corporation 1

Small School Corporation 1 (SSC1) has 6 full-time IT staff and no part-time employee or consultant. The total IT budget for year 2013-2014 was $856,635 USDs (See table 5) and serving 1473 students. Besides salary expense, hardware lease is the

second largest expense with $275,000 corresponding to Apple related products like iPads and MacBook-Pros. This is the strategy followed by this corporation to enhance employees and students experience to technology.

Located within the school district are five different Novell Netware and four Linux servers spread out over four buildings connected via a wide area network (WAN). This “backbone” allows staff in each building (3 schools in total) to communicate with each other to share files and applications. Staff members in all three buildings communicate with each other via an intranet e-mail client running GroupWise (version 6.5) software. All classroom and individual workstations have access to the Internet through a T1 connection provided by education networks for America (ENA) as the main internet service provider (ISP), the school corporation has plans to add a second T1 connection in the near future. The district has Internet protection software that monitors all incoming and outgoing traffic to ensure that the district complies with the Children’s Internet Protection Act (CIPA) and FERPA. SSC1 current network runs at 100mbps, and they are budgeting to increase the capacity to 1000mbps in the next few years. Through a one-campus school setting, staff members at SSC1 are able to locate free labs that allow students to take tests in an effective and efficient manner. SSC1 is also planning to increase the purchasing of one-to-one devices (i.e. iPad charts or tablets) to serve students offering educational access to apps and programs. SSC1 currently has close to 2400 devices, of which around 700 are between desktops and laptops. The remaining are tablets or iPads.

In addition, all three schools have an Internet cable video network that provides the school system with the capability to distribute professional development videos and other images to each classroom within the district. SSC1 Middle School is a member of the Automated Weather Service (AWS) and provides the only professional quality weather station in their city. Between a Sonicwall firewall and the DHCP network, according to SSC1 assessment, they are able to ensure reasonable level of security for student management software and other important data. SSC1 also uses Microsoft (MS) Security Essentials as its current antivirus protection (previously it used Symantec Anti-virus software) and a MailWatch scanner to prevent virus infection of individual workstations or servers. Critical data is backed-up district-wide each evening on a separate server that has a RAID 5 configuration. The backup solution is an open source enterprise level backup system for heterogeneous networks called Bacula, taking advantage of the school corporation virtualization capabilities. Many of the new copy machines as well as network printers are connected to the local network to enable staff to scan documents and print to remote sites throughout the school district.

SSC1 does not have abundant Cisco equipment, instead it uses PFSense software and compatible hardware to provide firewall and router (open source) protection to its network. This also allows the activation of a feature called SNORT that allows a level of intrusion detection by logging and blocking events. Content Web filtering is provided by LightSpeed in compliance with FERPA regulations. Employees at the corporation have their email hosted and administrated within the network using MS Exchange 2010, and Barracuda for spam filtering. Students' email platform has been outsourced to Google

Apps for Education, as it provides free email and other apps for school corporations free of charge. When asked about needs and wants regarding the improvement of IT related projects, they conveyed that the datacenter might need some updates (room and equipment) because is now close to 10 years old, having the latest update in the form of replacing the cooling system 4 years ago. As the SSC1 moved forward with a non-Microsoft approach, a cost-saving measure was the decision to transition from a Symantec antivirus towards MS Security Essentials for those computers that still run Windows, reducing their Antivirus cost to zero, and under the assumption that "Apple products are not as susceptible to infections as Windows". They did disclose that in 2005, they had a virus infection contained within a Linus server, and that represents so far the only incident with Virus or malware. Significant savings allowed for the re-allocation of funds for more leased Apple products. Table 5 shows the structure of SSC1 IT budget:

Table 5. SCC1 IT budget

2013-2014 SCHOOL YEAR (budget category)	**SSC1**
Salary	$295,000.00
Hardware	$384,135.00
Software	$125,000.00
Professional Development (non-salary; expenditures as required)	$5,000.00
Telecommunications	$47,500.00
Contract / Professional Services for Technology	-
Sub Total by Source	$856,635.00
Category by school size	Small
2013 School year Student Count	1473

4.2.2 Interview with Small School Corporation 2 "

Small School Corporation 2 (SSC2) has two full-time IT staff, and one networking consultant, which represent an average cost of $20,000 per year. The total IT budget for year 2013-2014 was less than $350,000 USDs in order to serve 1005 students. SSC2 has a consolidated building for all their schools (3 schools in total) allowing them to maintain one network for all their needs. Their network is administrated using Active Directory and has 14 servers located at a centralized building. They recently switched antivirus from Symantec to Avast as a cost-saving strategy, going from around $5000 to $1000 per year. This AV provider offers a price per node of $1 USD for each licensed node (based on student school count). SSC2 reports no previous infection, although later admitted that they had detected that close to 30 lab computers were infected, but they infection was contained. Cisco is almost exclusively the main provider of network equipment, attributing this decision to “wanting to provide the ‘best’ possible solution that would last many years before it needs to be replaced”; in addition the corporation pays for Cisco SMARTnet program which allows them to address any equipment failure within 24 hours. A local telephone company provides them with Internet Access (100 Mgs) as main provider, and using ENA (e-rate State provider) as a backup alternative. The monthly costs associated with those services are $1,200 and $400 respectively.

SSC2 has a planned hardware renewal cycle of 4 years, and for this school calendar year, it has been the goal to renew existing computer hardware for the high school and middle school primarily, and then repurposing that equipment to renew older hardware from the elementary school. The planned expense for this upgrade is

$80000 in new computers and $30000 in software. The backup solution of SSC2 is Eversync with a server capacity of 4TB, and 2 mirror hard-drives, as well as the ability to take a copy over the weekend to an off-site location. Thanks to favorable licensing agreement with Microsoft, they are able to user several suites of products; based in that they have decided to host their email solution in-house using MS Exchange server.

Among the realized future needs and wants they expressed during the interview were: to implement a radius (like) solution to provide wireless access point authentication across their network; the overhaul the server room to better withstand power outages or fire hazard. When questioned about their interest in products/services related to network risk assessment, penetration testing, or network intrusion prevention; they expressed great interest, but their capacity to afford those services is cost prohibited at this point. They mentioned that they had applied to several grants in order to be able to implement solutions like those previously mentioned (server room improvements), they so far had not been granted any. Table 6 shows the structure of SSC2 IT budget:

Table 6. SSC2 IT budget

2013-2014 SCHOOL YEAR	**SSC2**
Salary	$132,000.00
Hardware	$107,000.00
Software	$44,500.00
Professional Development (non-salary; expenditures as required)	$3,000.00
Telecommunications	$23,800.00
Contract / Professional Services for Technology	$20,000.00
Sub Total by Source	**$330,300.00**
Category by school size	Small
2013 School year Student Count	1005

4.2.3 Interview with Small School Corporation 3

Small School Corporation 3 (SSC3) has two full-time IT employees and no networking consultant. The total IT budget for year 2013-2014 was less than 200,000 USDs in order to serve 3110 students. SSC3 has a consolidated building for all their schools (three schools in total) allowing them to maintain one network for all their needs. Their network is administrated using Active Directory, while defacing Novell. SSC3 has five (5) schools distributed across their district, and all of them are connected by fiber optic thanks to previous year investment in infrastructure. The newest building hosts two (2) schools, and within the building there is a centralized server room, where the main servers are secured.

Cisco is the main provider of networking equipment and IP telephony, and this school corporation has recently upgraded to ASA series Firewall, which is capable of intrusion detection. SSC3 has decided not to participate in the SMARTnet program as it is seem as an expensive solution, the last quote received for SMARTnet was $80,000; instead they keep onsite spare equipment for the most common critical sections of the network. The researcher did not inquire in detail about the configuration capabilities of the device in order to determine if it was configured to make use at capacity of its features, although it could represent an opportunity to enhance security if that is not the case. The main Internet service provider is ENA as Internet IaaS provider with a cost of $21,000 a year ($1,800 per month), and subsidized by the E-RATE (FCC website) program based on discounted and free lunches per corporation.

SSC3 has outsourced its email solution to a cloud provider because according to IT staff “it is offered as a free and reliable service”, although they do pay for the archiving ($6300 a year) of 533 email accounts and customer support services to a third-party company. There are no plans to host this service in the future. The planned renewal cycle is four (4) years and usually starts from high school down to elementary school. The current average price the corporation is willing to pay is $600 for a desktop, $700 for a laptop, and $650 for an iPad or tablet.

In compliance with FERPA, SSC3 uses Cisco firewalls and web content filtering provided by LightSpeed with an annual cost of $18,000 including support. It also has a file backup solution of 4TB that allow for a copy to be removed every weekend and stored off-site. The current antivirus solution is Kaspersky, from previous Avast, as it pursues to improve levels of virus and malware detection. The cost for antivirus protection is $32,000 for a 3-year contract. For next year they are evaluating the possibility of a new provider which presents a model that encompasses antivirus and other services that are attractive to the IT department such as: antivirus, asset management, remote control tool, patch management, and more for a slight increase in the current cost.

When asked about realized future needs and wants it was expressed the growing need to implement a wireless solution across all schools in order to meet educational approaches that the corporation and teachers are using due to the use of tablets and iPad products. The centralized server room also needs improvements. Although functionality is not an issue, there are aspects related to service continuity considered "

important: power independence from building, fire and water damage. Related to " network, they expressed the need for a risk assessment of the whole infrastructure, especially as it related to vulnerability scanning and malicious event management. Also, each school also has its own file servers and other applications running specifically for " that school needs; power backup are in need to be renewed, updated or acquired. These servers are non-critical, but important for administration and teachers use. " Table 7 shows the structure of SSC3 IT budget:

Table 7. SSC3 IT budget

2013-2014 SCHOOL YEAR	**SSC3**
Salary	$200,000.00
Hardware	$250,000.00
Software	$200,000.00
Professional Development (non-salary; expenditures as required)	$3,500.00
Telecommunications	$20,000.00
Contract / Professional Services for Technology	$1,800.00
Sub Total by Source	$675,300.00
Category by school size	Small
2013 School year Student Count	3110

4.2.4 Interview with Small School Corporation 4

Small School Corporation 4 (SSC4) has 2 full-time IT personnel out of approximately 100 school corporation employees. It also has a line item fund for other contractors or for professional services of $25,000 a year. The corporation has approximately 75 teachers and paraprofessionals, and 25 administrators. The total IT budget for academic year 2013-2014 was 340,500 USDs (see subtotal by source from Table 8). This corporation also has a consolidated building approach for its 3 schools

(high, middle and elementary) allowing them to have one network serviced by less equipment that otherwise would be distributed across different buildings. A fiber optic connection through a local phone company allows this corporation to enjoy high-speed connectivity and access to broadcast their own high school TV (MtcSports), while spending $15,000 per year and not having to use ENA as their ISP.

SSC4 finished a planned upgrade last year of their network infrastructure using Cisco as their main provider (from network to IP telephony), which cost them to maintain SMARTnet for $4,000 per year, which guarantees that the equipment will be replaced within 24 hours (unless spare is available) of failure.

Some of the expenses under software services are the outsourcing of the hosting of their website allowing them to keep it consistently available to users all year round for $1200 per year. The majority of their servers are virtualized using Citrix. The maintenance fee for HP SAN storage is $1500 per year; and it runs Unitrends backup software for four (4) Terabytes of backup capacity. In respect to SSC4 email solution; it has also adopted a cloud solution (SaaS) from Google Apps for Education, while only paying an archiving fee for $1,250 per year.

The cost associated with their antivirus solution is $4,000 per year with Kaspersky, in order to cover all their network connected devices, but the price is based on student count. Some other costs associated with hardware are related to the purchase of new computers, for example 23 new laptops were purchased at a total cost of $12,000, averaging $543 per laptop. The purchase of 30 refurbished desktops at $12,000 the cost per device was $400, and the cost of buying projectors has consistently "

stayed within $1,000 per projector. The current count of laptops is close to 300 units, 600 desktops and 75 iPads.

One of the growing needs is related to deploying a better solution for a wireless network. In the meantime this is done by buying and configuring Cisco wireless access points; last purchase was 4 devices for $3,500, nevertheless authentication through wireless would be a better way to monitor and control user consumption of this resource. They have reported the existence of a virus infection within a computer laboratory. It was contained and computers were reimaged, as well minor incidents have been reported due to spam. Table 8 shows the structure of SSC4 IT budget:

Table 8. SSC4 IT Budget

2013-2014 SCHOOL YEAR	**SSC4**
Salary	$105,000.00
Hardware	$82,500.00
Software	$88,000.00
Professional Development (non-salary; expenditures as required)	$15,000.00
Telecommunications	$25,000.00
Contract / Professional Services for Technology	$25,000.00
Sub Total by Source	$340,500.00
Category by school size	Small
2013 School year Student Count	1049

4.2.5 Interview with Small School Corporation 5

Small School Corporation 5 (SSC5) has four (4) full time IT staff, with a $10,000 budget line item allowance for contracted professional services per year (See Table 9). With a total academic budget year of $510,000, representing a decrease from last years; after salaries, hardware ($180,000) is the second highest expense, followed by software

($100,000). SSC5 has a consolidated building hosting 4 schools, 2280 students and approximately 180 teachers.

SSC5 has mainly Cisco networking equipment; however it does not pay SMARTnet fees, as it made the decision to purchase spares of equipment that would most frequently be needed across the network. Their antivirus solution is K7 computing with a 3-year contract for $12,000 or $4,000 per year (calculated based on 1500 devices).

The renewal of hardware in the form of computers is planned to happen every five to six years, and the last purchase of desktops was for the quantity of 50 desktops with a total cost of $33,000 or $660 a unit. The reason in the length of the renewal cycle for desktops is due to buying more tablets and iPads instead of conventional computers. In the previous academic year, a purchase of 708 iPads was made with a total cost of $340,000, or a unit cost of $480, and an allowance of $16,000 for replacement of one (1) iPad every month for 3 years. This represents the new strategy (one-to-one approach) to introduce tablets to the classroom for educational purposes, in addition to the existing 750 convertible tablets running Windows.

SSC5 participated of the state sponsor ISP (ENA) for connectivity as well for telephony. The cost for IP telephony was only the initial cost of investment with Cisco equipment; so calls within network are free, nevertheless network incoming and outgoing calls have a cost of $4,200 a year or $350 a month.

With an aggressive mobile computing strategy, wireless management is important, and SSC5 has decided to use Adtran as its wireless management solution,

from controllers to access points. No costs were disclosed for Adtram solution. Table 9 shows the structure of SSC5 IT budget:

Table 9. SSC5 IT Budget

2013-2014 SCHOOL YEAR	**SSC5**
Salary	$200,000.00
Hardware	$100,000.00
Software	$180,000.00
Professional Development (non-salary; expenditures as required)	$-
Telecommunications	$20,000.00
Contract / Professional Services for Technology	$10,000.00
Sub Total by Source	$510,000.00
Category by school size	Small
2013 School year Student Count	2280

4.2.6 Interview with Large School Corporation 1

Large School Corporation 1 (LSC1) has 38 full-time IT employees, pending budget approval for the opening of five (5) more network IT positions for next academic year. With a total "unrealized" IT budget of $3.5 million at the beginning of the interview process, I was later informed that due to an overhaul of the overall corporation budget in order to determine what the monies were used for regarding of funding source (i.e. grants), the "realized" final IT budget for 2013-2014 was instead 9,997,800 USDs. This is the amount reported (See Table 10). This particular corporation salary budget, compared to the rest of corporations, accounted for employee's benefits, which explains that the average salary per employee is higher than the others. The number of contractors per year fluctuates with an average of 7 corresponding to a budged amount of $50,000.

LSC1 has a large fiber optic network infrastructure between its 72 distributed locations (68 schools), which is leased to AT&T for $1,309,689.31 (Private Fiber Network). The majority of the networking equipment for network connectivity is Cisco, with already initial cost on investment and a Cisco SMARTnet annual cost of $85,000 per year that serves as warranty and support services rendered to the corporation network for service availability. The availability of the network connection is important since all IT servers and services are mainly located at one central hub (main building). ENA is the main Internet service provider (ISP) for Internet connection and also the content web filtering service; group wise funding is also based on e-rate funding based on “discounted and free lunches” ratio.

On the server side, LSC1 leverages its large server infrastructure to implement virtualization at server side (with 375 virtual servers) and also on the desktop side, deploying virtual desktops with secure access to storage to its more than 4000 concurrent users. The number of network connected devices like laptops and desktops are 16000 (around 9000 computers are Apple products), from which each teacher and administrative staff is assigned a desktop and laptop, with an average renewal cycle of 5 years. All desktops and laptops have installed Computrace-LoJack in order to protect data remote erase feature and to locate stolen equipment. Computers run Windows 7 (W7) on disk or are capable of running an older operative system and host a W7 virtual desktop when connectivity to the corporation network or the Internet is available. The virtualization platform runs over VMWare and secure connectivity over the Internet is made possible through AnyConnect (a Cisco VPN product). "

The Data Center network consisted of multiple layers of switching with multiple vendors. LSC1 utilized Nexus 5000 series switches as an access layer in conjunction with Nexus 2000 fabric extenders to provide the best solution without the management hassle of 2 switches per rack in a 30-rack environment. Two Catalyst-6509's were upgraded with single Supervisor 720-10G's per chassis and configured as a Virtual Switch System. All school VLAN's terminate at the core and all external connections (Internet) are delivered at this layer, while the 6509 VSS acts as the distribution layer switch for the Data Center. With the Nexus switches and fabric extenders providing access layer switching to servers and storage the distribution layer is used to terminate Data Center VLAN's and manage network security controls. Wireless controller services are also terminated at this layer as all wireless is encapsulated with CAPWAP back to the controllers.

An important part of the Data Center design included storage networks with a multi-tiered storage solution including SSD, SAS, and SATA drives, and potentially NAS (CIFS, NFS) and block level (iSCSI, FC) arrays. A significant investment existed with HP LeftHand iSCSI arrays. Nexus 5000 series switches with Nexus 2000 fabric extenders fit the problem best. The options in Nexus 2000 hardware with both Gigabit and 10-Gigabit networking allowed LSC1 to migrate from a single flat architecture to a tiered environment capable of supporting any storage solution necessary for deployment. The storage capacity is half (512 Terabytes) Petabyte with 10-gigabit bandwidth. The backups are performed by (IBM) Tiboli backup solution, with a capacity of 5 Terabytes, performed at the end of each day incrementally in IronMountain media.

In order to provide antivirus protection and compliance according to FERPA, several service protections were implemented from Barracuda Security Services. And in order to not repeat the network breach from 7 years ago (2008), several of the existing equipment is configured to detect and stop intrusion attempts. LSC1 conducts Network Security Assessments every year at a cost of $20,000 and another assessment every other year at a cost of $30,000 from different providers.

LSC1 recognizes that periodic and constant education is important for their IT staff, for that reason it has allocated $200,840.33 for professional development from an array of options to it personnel, this also included education and training for employees and students regarding information security seminars. Table 10 shows the structure of SSC1 IT budget:

Table 10. LSC1 IT Budget

2013-2014 SCHOOL YEAR	**LSC1**
Salary	$2,800,012.00
Hardware	$3,470,277.52
Software	$2,164,153.06
Professional Development (non-salary; expenditures as required)	$200,840.33
Telecommunications	$1,312,517.41
Contract / Professional Services for Technology	$50,000.00
Sub Total by Source	$9,997,800.32
Category by school size	Large
2013 School year Student Count	29803

4.3 Analysis of Current Costs

This section will present the costs associated with software (antivirus and cisco SMARTnet), hardware (desktops/laptops/iPads/tablets and cisco equipment), as well as, IT personnel salaries in order to draw comparisons. Such detailed analysis will be helpful when comparing with cost savings (benefits) corresponding to participating in information security related products/services offered through the INSCS project.

4.3.1 Antivirus Costs

This subsection will discuss the results derived from the calculation of the unit price (license) for antivirus, based from the antivirus total cost per year, and the number of students enrolled (student count) in which antivirus providers based their pricing scheme. Table 11 presents the results.

Table 11. Antivirus Cost per School

Description \ School code	**SSC1**	**SSC2**	**SSC3**	**SSC4**	**SSC5**	**LSC1**
Antivirus Provider	Microsoft Essentials	Avast	Kaspersky	Kaspersky	K7 Computing	Barracuda
2013 School year Student Count	1,473	1,005	3,110	1,049	2,280	29,803
Antivirus Cost per year	$-	$1,005	$10,666	$3,200	$4,000	$60,000
Antivirus cost (by enrolment count)	$-	$1.00	$3.43	$3.05	$2.67*	$2.01

* This calculation was not based on student count; instead it was based on 1500 devices instead

4.3.2 Antivirus Cost Aggregation "

The antivirus cost for small corporations, except in the case of SSC1 that doesn't pay for antivirus, was $2.54 in comparison to the cost of $2.01 for LSC1. The antivirus maintenance cost per computer for the State of Indiana is $1.69, based on the cost of McAfee VSE desktop ($57,460 per year), which covers 34,000 systems. Nevertheless, in order to fully evaluate the cost of antivirus for IOT, it also has to be considered the perpetual license cost, which represents in this case a similar case of "initial cost of investment"; this means that the state of Indiana has committed long term to have McAfee (and other products) as their antivirus solution. The cost of perpetual license and first year of service costs $9.07 per license.

The INCSC is negotiating, through IOT, the possibility of a better price structure by using a quantity purchase agreements (QPA) with service providers, in the case for McAfee would result in a price (per node) that is potentially attractive to school corporations from what they are currently paying for antivirus protection. More details about the calculations mentioned here will be explained in following sections.

4.3.3 Cisco SMARTnet Costs

This subsection will discuss the results derived from reported costs associated with (software) SMARTnet support and replacement services (See Table 12). SSC1 does not pay for this service since its network doesn't have enough Cisco equipment to justify the cost. SSC3 and SSC5 have plenty of Cisco equipment; nevertheless, it they made the

choice to acquire spare equipment for replacement in case of failure and continue building a fund for network equipment from year to year.

Based on SSC2 and SSC4, the average cost is $5,000 per year. From that it could be inferred that the network size falls under a determinate size, which has a specific maximum for the equipment in order to qualify for that SMARTnet cost-range. The downside of this approach might be that the smaller the network size is (or equipment owned) it still has to pay the same amount than a network size bordering the maximum qualified network/equipment size for the range.

Another way to look at it would be when comparing the cost of SMARTnet based in school corporation number of schools (See Table 4) in order to determine the size of their network; for instance then LSC1 ($85,000) has 68 “decentralized” schools, compared with the average cost for small corporations ($5,000) with up to 9 schools. Then if the cost of LSC1 is divided by the cost of the average small corporations, we could determine that the large corporations would, in theory contain, 21.25 times of the small one in terms of cost. By doing the same with the number of schools, the large corporation would contain 7.55 times the small one. This calculation represents extrapolation, and might not represent the reality, due in part that some small corporations have consolidated buildings; hence the size of the network is even smaller. This validates the assumptions that schools with smaller and “consolidated” networks would save money during the initial investment cost of implementation of Cisco equipment, but when it comes to SMARTnet, the cost will be the same as those with

larger networks up to the threshold established by Cisco for qualifying networks to the $5,000 price limit.

Based on the account from SSC3, the key element in calculating the cost for SMARTnet has to do with the number of “centralized” or “decentralized” sub-networks a school corporation has. An accurate account of decentralized sub-networks connected with Cisco equipment would have been of great value for validating the assumption of SMARTnet pricing, but this information was not pursued at the time of the interviews were conducted. Information received from Cisco indicates that the cost of SMARTnet is calculated based on the original sale price of equipment; the ratio corresponds to 7% of the listed price to calculate the cost. An organization could choose to select what piece of equipment would like to protect with SMARTnet, and not necessarily all.

Table 12. CISCO SMARTnet Costs

	SSC1	SSC2	SSC3	SSC4	SSC5	LSC1
Networking Operational Cost (SMARTnet)	0	4000	0	9600	0	85000

4.3.4 Cisco SMARTnet Cost Aggregation

The researcher concluded that from the six (6) school corporations interviewed, only two small and one large corporations participated of the program (see Table 12), and that represents insufficient data to determinate an aggregation of costs. An observation about a characteristic in common of SSC2, SSC4, and LSC1 was that all of them have “centralized” networks or consolidated buildings; the information necessary to determine the cost for medium size school corporations was not available for this

analysis. Small corporation SSC3, which has five separated schools networks, reported that it was quoted a cost of $80,000 for SMARTnet, which indicates that they do have a decentralized building/sub-networks topology.

4.3.5 IT Employee Costs

The average salary for IT employees (See Table 13) for a "small" corporation is $63,890 compared to the average salary of $73,685 for a "large" corporation. The amounts corresponding to consultant budget is zero for SSC1 due to the reliance on the expertise of 3.5 IT employees, the average salary for this corporation is the highest of all. Also the reason why the consultant budget amount is so low in the case for SSC3, is due to the fact that IT employees that work for the corporation are subcontracted through a small IT company that charges $200,000 per year and provides 2 full-time employees, a third one is considered as part of the number of employees since this small company is responsible to provide expert consulting services related to IT needs at any time during the year.

Table 13. Number of IT Staff and average salaries*

Budget Desc \ Percentage	SSC1	SSC2	SSC3	SSC4	SSC5	LSC1
Salary total budget	$295,000	$132,000	$200,000	$105,000	$200,000	$2,800,012
Number of IT Employees	3.5	2	3	2	4	38
Average salary of IT Staff	**$84,286**	**$66,000**	**$66,667**	**$52,500**	**$50,000**	**$73,685**
Yearly cost of Consultants	$-	$20,000	$1,800	$25,000	$10,000	$50,000

* The amount for small corporations does not include benefits, as it does for the large corporation.

The average of consultant cost for small corporations, even without considering SSC1, is less than $15,000 ($14,200) when compared to $50,000of LSC1. Nevertheless,

when put in perspective of the cost of consultant per student count, then $50,000 does not seem as a great cost (See table 14) in comparison to SSC2 or SSC4.

Table 14. Average cost consultant vs. student count

	SSC1	SSC2	SSC3	SSC4	SSC5	LSC1
Average consultant cost ($) per student count	0	19.90	0.58	23.83	4.39	**1.68**

4.3.6 IT Employee Cost Aggregation

The average for small corporations' salary per IT personnel is $63,890.48 compared to the large corporation of $73,684.53 (See Table 13). The researcher once again has to clarify that the salaries for small corporations do not include benefits, as it is in the case of the large corporation, for that reason it could be inferred that the current difference of $9,794.05 might be less than expected due to benefits; another clarification needed is that the average from small corporations is based on a simple average calculation, and salaries do vary based on the rank and position of each employee, as do their benefits. The comparison presented only contributes a point of reference for analysis.

4.3.7 IT Budget in Percentages "

This section will present a different view of school budgets to show the percentage that a specific line item corresponds to the overall IT budget (See Table 15). " A comparison across all small corporations and LSC1 will be made. Some analysis could "

be elaborated based on the description detailed by school in section 4.2, as they explain the proportion in which the percentages are represented.

SSC2 has 40% of their budget designated to salaries of employees because it is a smaller budget in proportion to other small schools ($330,300). It does allow for some reliance on consultant services, and it does pay for SMARTnet. SSC1 has 45% of their budget on hardware, as this academic year it is purchasing and leasing a high number of Apple devices (~$275,000), it does rely (and pays better salaries) more in internal personnel expertize rather than consultants. It does not pay for SMARTnet. SSC4 spends more in proportion to software (26%) than its peers; SSC3 spends the least in Telecommunications (ISP) than its peers; and SCC4 relies more on consultant services.

Table 15. Percentages from total budget by category

Budget Desc. \ Percentage	SSC1	SSC2	SSC3	SSC4	SSC5	LSC1
Salary	34%	**40%**	30%	31%	39%	28% "
Hardware	**45%**	32%	37%	24%	35%	35% "
Software	15%	13%	30%	**26%**	20%	22% "
Professional Development	1%	1%	1%	4%	0%	2% "
Telecommunications	6%	7%	**3%**	7%	4%	13% "
Contract / Professional Services for Technology	0%	6%	0%	**7%**	2%	1% "
Sub Total by Source	100%	100%	100%	100%	100%	100% "

Table 16 compares the averaged budget percentages of small corporations in contrast with large corporations. There are differences, but overall those percentages are similar in proportion. The marked difference in telecommunications for the large corporation is due to the leasing of their fiber optic network infrastructure ($1,309,689.31).

Table 16. Expenditure percentage comparison: Small vs. Large

Budget Desc. \ Percentage	Average % for SMALL Corporations (5)	% Value for LARGE Corporation (1)
Salary	35%	28%
Hardware	35%	35%
Software	21%	22%
Professional Development	1%	2%
Telecommunications	5%	13%
Contract / Professional Services for Technology	3%	1%
Sub Total by Source	100%	100%

4.3.8 Computer Hardware Costs

This section will present price averages reported by school IT staff for the purchase of computer equipment, based on previous purchase requirement. It should be noted that hardware costs reported were approximations based on a similar but not identical hardware requirements, the reason behind that would be the variety and multiple configurations of computers purchased by the different school corporations; guidance was provide in order to provide information about costs that would be as close possible to each category. Latest pricing information would correspond to 2013. The column at the end represents the costs that Indiana Office of Technology (IOT) currently pays; which provides a reference to show if there is a benefit to participate within a State-purchasing program.

Table 17. Average prices for computer purchases*

Description \ School alias	SSC1	SSC2	SSC3	SSC4	SSC5	LSC1	IOT
Average Cost of New Laptop (Windows)	$850	$500	$750	$600	$629	$1,000	**$668**
Average Cost of New Laptop (OS X)	$1,500	$-	$1,300	$-	$1,300	$1,300	**$1,300**
Average Cost of Refurbished Laptop (Windows)	$500	$400	$550	$400	$600	$-	**$-**
Average Cost of New Desktop (Windows)	$700	$500	$750	$800	$750	$750	**$504**
Average Cost of New Desktop (OS X)	$800	$-	$800	$-	$850	$900	**$850**
Average Cost of Refurbished Desktop (Windows)	$500	$400	$450	$350	$450	$-	**$-**
Average Cost of New iPad	$500	$480	$480	$479	$479	$650	**$630**
Average Cost of New Tablet	$700	$650	$700	$600	$700	$750	**$730**

* These amounts do not necessarily correspond to the same purchasing period across school corporations

The need for computer equipment was generalized in terms of types and Operative System, this generalization originated from the lack of detail information regarding computer equipment purchases. The above chart provides a comparison of costs from all surveyed school corporations against IOT, as this would represent the approximate procurement cost that a school corporation would pay if purchase from IOT. If price is the main driver for purchasing, then in the case for the purchase of a new laptop, it might be beneficial to make that purchase through IOT when compared to individual corporation's costs. In the case for a Microsoft desktop, IOT offers a better price, unless commercial pricing and other characteristics might change the decision process. For example the average cost of an iPad for IOT is of $630 (iPad Air, 16GB LTE), and the characteristics required by other school corporations might be for iPads that do not necessarily are the Air version. There researcher acknowledges that there is a

disparity in the version of the technology purchased due to time of purchase and specifications.

One of the aspects of government procurement is that it seems complicated and it might become a difficult to manage through one single centralized location, unless school corporations were able to have access and utilize state pricing and also pay themselves for those purchases. This could allow them to take advantage of the price structure leveraged by the state, and hopefully also benefit from discounts or added perks, while independently making orders of computer equipment to their respective destinations. While the provider in this instance is considered HP, the researcher had a certain level of skepticism regarding the price structure tailored for the State of Indiana, mainly because of the information found on HP's website (See Appendix E). Nevertheless, I was informed by the Deputy CIO (Desktop and Support Services at IOT) that HP has a more cumbersome purchasing process already established with the State of Indiana for purchasing computers with preferential pricing and above average technical specifications. Once again this might work for IOT since it already has access to a dedicated HP representative or purchasing channel, however it is unclear how would this process could be extended to and leveraged by school corporations.

There are also two scenarios from which school corporations could benefit; the first instance is a multivendor approach for acquisition of computers, since price competition would always benefit school corporations in order to obtain the best possible price. The downside of this approach would be the plurality of brands to manage especially when dealing with keeping an updated set of Operative System

images for reformatting those devices. The second factor would be the convenience of instant comparison from online sources to make the decision of buying new equipment or the capacity to buy refurbished equipment for a fraction of the price of a new computer. Different strategies are chosen for each specific school corporation as shown on Table 17, where some schools might embrace the “refurbished” option, while it might not be considered in others. School policy and budget capacity are factors that greatly influence this decision. Specialized solutions for refurbished equipment is especially appealing to small school corporations when affordability is a factor in school finances; two examples of those services are companies like CDI Computers (based in Ontario, Canada) and VIG Solutions (Pflugerville, Texas) with highly competitive and affordable pricing.

4.3.9 Computer Hardware Cost Aggregation

In this section the researched acknowledges that the sample number of school corporations studied is small and this limits the extrapolation of results to all school corporations in Indiana. Nevertheless, an aggregation of computer hardware costs is conducted in order to provide an idea of the possible benefits when considering IOT pricing structure. Based on the information displayed in table 18, school corporations could consider using the State purchasing mechanism according to the following costs.

Table 18. Price comparison between schools and IOT

Description \ School alias	IOT average prices	Schools average prices
Average Cost of New Laptop (Windows)	$668	$722 "
Average Cost of New Laptop (OS X)	$1,300	$1,350 "
Average Cost of Refurbished Laptop (Windows)	$-	$490 "
Average Cost of New Desktop (Windows)	$504	$708 "
Average Cost of New Desktop (OS X)	$850	$838 "
Average Cost of Refurbished Desktop (Windows)	$-	$430 "
Average Cost of New iPad	$630	$511 "
Average Cost of New Tablet	$730	$683 "

4.3.10 Cisco Equipment and Support Costs

This section will discuss the planning process for acquisition of Cisco equipment, what SMARTnet is and how much it costs, as well as how INCSC plans to overhaul Cisco price strategy (including SMARTnet) for schools in Indiana as it impacts Cybersecurity. Schools did not report costs related to purchasing of their previous equipment strategy; nevertheless, they all agree that it was not cheap and it was not without careful planning and budgeting. There is the exception of SSC4 that provided information about bids presented by a Cisco partner for the implementation of upgrades of their network.

I will present a summary of those costs as they could represent an idea of how "Initial Cost of Investment" would look like in a cost-benefit analysis scenario.

Table 19. SSC4 Cisco Quote (from May 2012)

*Quotes based on 2012 prices	Hardware	Software	Service	Total
IP Telephony project and SMARTnet (software)	$49,231	$15,385	$9,000	$73,616
Main Distribution Frame (MDF) Hardware upgrade	$59,139	$-	$6,500	$65,639
Managed Switches upgrade and SMARTnet	$17,418	$1,481	$2,400	$21,298

School corporations, through state and federal regulation, have been led to implement minimum levels of security in order to protect information of individuals

(employees or students) within their organization. As a result of complying with regulations, corporations have implemented solutions such as firewalls, and web content filters, among the most important to mention. Cisco products are among the most used solution, as observed, enjoying high preference in networking products and services; there are, nevertheless, other products/solutions used providing similar or comparable levels of service. From the interviews (see Table 20) it was clear that the main provider of network equipment and firewalls was Cisco, as a trusted and known provider. The costs associated with acquiring such infrastructure, on the other hand, is a challenge for school corporations because while desiring the implementation of a stable and lasting implementation, it represents a high cost in their budgets. That is why from the majority of interviewed school corporations, this process had to be planned in advance as part of a strategic planning process of at least one academic year, bringing these technology plans to the floor of the school board for (next year) approval.

Table 20. Network Equipment Provider

School Alias	SSC1	SSC2	SSC3	SSC4	SSC5	LSC1
Network Equipment Provider	Multivendor	Cisco	Cisco	Cisco	Cisco	Cisco

As shown in Table 20, investments of this type could represent a great percentage of the IT budget for a small school corporation. For example, if SSC4 had proceeded with the quotes for this academic year, it would have represented $160,553 from its $340,500 IT budget (47%). That is almost half of its budget, which generally means that other needs would have to wait another year, for example renewing

computers. For those who have Cisco equipment, they already know that its equipment comes with 90-day warranty (Cisco Warranty):

> *"Cisco warrants to the original end-user customer that our hardware products are free from defects in material and workmanship under normal use for the duration of the warranty period. Our standard warranty period is 90 days from the date of shipment to the customer"*

And they highly encourage the adoption of a support/service product called SMARTnet, which is categorized as a software product and associated with an specific product (equipment). A detailed comparison from standard warranty vs. SMARTnet is show below (See Figure X). All the interviewed IT staff agrees with the value (benefit) of the product; however the cost in the majority of the cases represents a high cost for their budgets, as previously reported in one instance quoted up to $80,000 per year for a small school corporation.

	Equipment Covered	Duration	Hardware Replacement	Cisco OS Updates	Cisco TAC Support	Registered Access to Cisco.com
Cisco SMARTnet Service	All[1]	Renewable contracts	Advance hardware replacement: - 24x7x2 hour - 24x7x4 hour - 8x5x4 hour - 8x5xNBD Onsite options available Other: - RFR[2]	Yes, updates within the licensed feature set[5]	Yes	Yes
Cisco Standard Hardware Warranty	All[1]	Standard hardware: 90 days[3] Standard software: 90 days[3]	Advance replacement (10 days)[3]	No[4]	No	No

1. Some equipment exclusions might apply; consult a service sales representative for more details.
2. Return for Repair on select video products only.
3. Some products come with different warranties. Please see www.cisco.com/go/warranty for more information
4. Warranty only makes sure that software media is defect free and the software substantially conforms to published specifications.
5. Cisco Unified Computing System also includes ongoing downloads of BIOS, drivers, firmware, and Cisco Unified Computing System Manager (Cisco UCSM).

Figure 2. Cisco SMARTnet Service Comparison to Standard Warranty "

From Table 12 we see that half of the corporations reported participating in SMARTnet services. The other half determined that they could afford it and decided instead to purchase extra equipment as spare. The calculation of SMARTnet pricing was the topic of a conversation with the representative of Cisco Indiana (Public Sector Account Manager), whom acknowledged being aware of the INCSC project, explained the novelty of this solution for the protection of cisco infrastructure within an organization. When asked about how SMARTnet costs are calculated, he responded that it usually represents 7% of the original equipment price (See Table 21 as presents a real price example for a school corporation scenario).

Table 21. Example of price calculation for SMARTnet (ASA series)

Product Description	**Price in USD**		**45% discount**		**School price**		**SMARTnet (7%)**		**Total price w/disc**	**Total price no disc.**
ASA 5510 Appliance with AIP-SSM-10, SW, 5FE, 3DES/AES (ASA Low Price End)	$5,995	-	$2,698	=	$3,297	+	$420	=	**$3,717**	**$6,415**
ASA 5555-X with IPS, SW, 8GE Data, 1GE Mgmt, AC, 3DES/AES (ASA High Price End)	$44,995	-	$20,248	=	$24,748	+	$3,150	=	**$27,897**	**$48,145**

The previous example brings to light the fact that the cost structure for school corporations, under Cisco “educational pricing structure”, represents a 45% discount over the listed price. This offers a significant financial benefit for school corporations to embrace this technology solution. These types of educational discounts are a common commercial practice that is not unique or exclusive to the Cisco Systems price structure.

4.4 Analysis of Potential Benefits "

This section will explore the benefits associated with the participation of school corporations in the INCSC project, specifically related to networking equipment (Cisco and HP), software (McAfee and SMARTnet), and professionals services (outsource of specialized consulting services).

4.4.1 Projected INCSC Benefits

An initial assessment of benefits for school corporations was created (see Appendix E) in order to enumerate in a comprehensive way all possible benefits for school corporations when participating in the INCSC project. Due to time and scope constraints, a smaller subset of potential benefits were considered in this research; nevertheless, the list was attached as an appendix in order to provide guidance to future research that might expand the scope of this thesis. The specific areas considered to have potential benefits for school corporations were related to 1) hardware: networking (Cisco) and computers (HP), 2) software: antivirus (McAfee) and SMARTnet (Cisco); and consulting services (professional services).

4.4.2 Projected K-12 Information Security Benefits

The identification of current benefits for K-12 school corporations to implement and comply with security controls in order to protect employee and student data represents those upper bound benefits of information security. The lower bound benefits correspond to actions that further enhance existing upper bound benefits in

the form of providing a cost saving. Understanding the importance of these benefits highlights new ways to enhance them in the form of implementing state-of-the-art security solutions, as it could be by adopting one solution provider over another. This research presents a way to do that analysis, by considering that participating in the INCSC would help not only improve lower-bound cost savings but also upper-bound efficiency, as well as educate about the potential repercussions due to a negative information security incident. Striving to improve the information security level of school corporations so that they at least comply with State/Federal laws and regulations could represent elevating the corporation's level to a higher standard, especially when compared to other school corporations across the nation.

4.4.3 Upper-Bound Benefits

Forming part of the INCSC could mean that school corporations are able to select services that make sense to them in a relatively efficient method to increase their Information Security level. The upper bound estimates are based on the assumption that there are substantial benefits from complying with regulations that require the implementation of minimum safeguards to school networks. These benefits are acknowledged from an external (regulatory) perspective and from an internal (school corporation) perspective as well. For instance, a school corporation given the nature of their customers (mainly children) has to implement controlled access to the "world wide web" (the Internet) for academic use with the implementation of a web content manager. This particular case only applies to K-12 schools, as higher-level education

systems do not have this mandated requirement. The same could be said of other hardware and software that supports the infrastructure of the organization in order to provide a safe and productive environment to its users.

4.4.3.1 Networking Hardware/Software: Cisco

The benefits of having a firewall solution (one or more devices) across their network infrastructure allows school corporations to monitor incoming and outgoing traffic, which also allows them to determine what is considered normal and abnormal network traffic behavior. For example it could be determined that the network is under unusual incoming traffic (or under attack) on specific ports or it could also be determined the one or more computers are infected and sending “spam” from within the network. Several Firewall vendors attach various other features to a firewall (like virus scanners); nevertheless, the main objective of a firewall is to protect networks from vulnerable services, control access to network systems, concentrate security, enhance privacy, and enforce network policy.

The cost associated with not having a firewall would first be related to violation of compliance with regulation, followed by the consequences to the network of unrestricted access to/from the Internet, and rapid deterioration of network environment quality. Since the cost for a school corporation related to lack of IT services would be too great, it has been accepted that the benefits are greater than the costs.

The researcher will not address in more detail the case of lack of firewall, but instead will focus on types of firewall solutions chosen and also the lack of knowledge to properly configure it (or modify configuration). Five out of six corporations currently use Cisco firewalls; only one of then uses an open source solution. However, from the interview process, it was determined that the corporation using open source had IT personnel with the capacity to configure their open source firewall solution; with that they have “justified” the adoption of open source as a cost saving strategy that allows them to invest in other areas of IT (i.e. one-to-one devices). On the other hand those corporations with Cisco equipment, in some instances, have limited knowledge in administrating the configuration of their firewall, explaining the need for IT contractors to perform configuration tasks in a non-persistent mode.

Some of the benefits envisioned by participating in the INCSC would be primarily related to cost savings (lower-bound) but also corresponding to upper-bound benefits in the form of service. This service will be a managed firewall program for school corporations included with their SMARTnet program.

The realized benefits of allowing the vendor to provide firewall monitoring is high, since they could offer a better level of customization for the school corporation through 1) keeping the firewall (s) up to date and 2) monitoring continuously for threats, 3) saving money by eliminating the need to hire a contractor to consult when changes are required; 4) keeping up with firewall compliance with standards and regulations put in place by the government; 5) network and data protection are in place 24/7; 6) providing relevant information to school corporation IT staff in order to make decisions "

to secure and safeguard against hackers and cyber-attacks. Some of the benefits previously mentioned will be later reflected during the with/without cost-benefit analysis.

As a disclaimer, the researcher is not advocating for Cisco as the only firewall solution in the market; however, it is considered that a large percentage of school corporations rely on Cisco as their firewall solution, in addition to the fact that Cisco is the only available vendor (at this time) considered for the project (INSCS) at the State of Indiana.

4.4.3.2 Antivirus Software: McAfee

Costs associated with the absence of an antivirus solution for school corporations are directly related to the cost of remediating problems caused by an infection. In the worst case scenario to solve an infection, which is the reimaging the hard drive of a computer as a standard procedure in the case of the State of Indiana, to expenses for IT staff time, loss of productivity from teachers and students who wouldn't be able to use computers, access to network resources become too slow, computers without access to applications or without internet access. In the case of small school corporations, which have between two and four IT employees for networks that host an average of 1000 to 3000 network connected devices (desktops, laptops, "tablets"), managing a virus infection that would require remote or onsite attention would take a considerable amount of time to be addressed. On top of this the changes needed to be implemented in order to avoid similar problems in the future (i.e. making sure that the

devices have updated antivirus). One way to quantify this would be to calculate the loss of productive time multiplied by dollars per hour (based on the salary of an IT employee), and multiplied by the number of devices infected.

The researcher will not address the case of lack of antivirus, but instead will focus on the type of antivirus solution and the cost associated to the service as an influencer of its adoption. Five out of six corporations currently have and pay for antivirus service; one of them uses a free antivirus (Microsoft Essentials). However, the majority of them haven't currently considered using Indiana state antivirus solution (McAfee) due to cost (See Table 11 for details about antivirus per license) or had this solution before and switched to a cheaper alternative. In the case of tablets (iPads) antivirus is not a deployed solution at this moment for any school corporation. However, IOT issued iPads have installed a product called MobileIron, which is a mobile device management software that allows administrator to "flag" unapproved apps so as not to be installed and also prevents jail-broken devices from connecting to state resources. There is also an alternative for K-12 school corporations that would offer protection to tablets that are BYOD or issued by the organization, McAfee EMM (Enterprise Mobility Management) is provided without cost for schools.

Overall, when quantified, the benefits associated with having an antivirus solution overcomes the cost of dealing with remediating the problems created by viruses, worms, malware, spam outgoing traffic, etcetera. *As a disclaimer*, the researcher is not advocating for McAfee as the only antivirus solution in the market, however it was used as the only reference since it is the current provider considered

when participating in the INCSC, which is also the current Antivirus provider to IOT (State of Indiana). As previously mentioned in the case for the firewall, some of the benefits envisioned by participating in the INCSC would be primarily related to cost savings (lower-bound) but also corresponding to upper-bound benefits related to antivirus. Since IOT already has McAfee as "the" service provider for antivirus protection through McAfee ePolicy orchestrator (ePO), it has also implemented other solutions such as (McAfee) Enterprise Security Manager for intrusion detection, and (McAfee) Asset Manager being amongst the most relevant ones. The particular product that could be leveraged as an added-on service when participating in the INCSC would be McAfee Asset Manager.

4.4.3.3 IT Personnel

The importance of counting on the right people being capable to perform tasks that enhance the Information security is of vital importance to the well-being of an organization. This also applies to school corporations represented by the existence of dedicated IT staff within schools (see Table 13). The costs associated with not having them represent great harm to the organization as a whole, especially in the current environment where technology adoption in schools is growing at fast pace. From administering systems internally or managing outsourced resources, the IT staff also maintains server rooms and backups, student learning systems, payroll and human resources data. The dependence of school corporations on information systems is

growing as well, and the lack of adequate personnel may be detrimental for the organization. In many cases school corporations do not have the capacity to continue adding more personnel to address these issues, for that reason many rely on outsourcing certain tasks and/or transferring risk to external providers. This section presents an analysis of the benefit that IT personnel represent for the organizations because of the need to manage information technology products/ services. The cost presented in previously reported IT budgets determines the salary proportion to be paid to IT staff as well as the number of employees a corporation is able to afford at this particular time (see Table 13).

4.4.3.4 Other upper-bound benefits to be considered

Encryption is another solution that is overlooked when attempting to protect school corporation data –in transit to/from networks– against data loss. When asked about it, only one corporation admitted to use some level of encryption when transmitting data; and only doing so when sending sensitive information to outside networks under the request of third party). The lack of knowledge, funds, and the fact that is not required by regulation were main reasons why an encryption solution was not yet heavily considered or implemented. The researcher wants to note that in the state of Indiana, if data was breached or lost with an asset, as long as it can be proven with reasonable doubt that it was encrypted, data breach notification is avoided.

Data Storage & Recovery solutions are also widely used across school corporations; however all reported using different solutions (i.e. Eversync, IBM Tivoli backup) with different costs. When asked about how often they restore data from backups and if it is successfully accomplished, they all responded that they are successful, but did not offer details about frequency. Another concerning issue related to backups was that in 3 cases, small school corporations allowed their IT personnel to take a backup copy (stored in a case) to their residences during the weekend.

Power Backup systems for servers are considered upper-bound benefits because they offer a level of protection against power outages that will, in the worst-case scenario, allow servers to execute shutdown procedures in order to prevent sudden power interruptions that could compromise the integrity of the data. Besides that realization, four out of six school corporations expressed their need to first acquire more power backup equipment in order to replace those critical systems and use the older ones to replace other (non-critical) servers. Cost is the main factor to make this possible. Another realized need was to further equip their server's room with fire, water and power protection.

Information Security Framework Policy is a mechanism that was agreed upon as important, but the implementation in many cases doesn't transcend the corporation's policy manual for use of computers. LSC1 had a more educational approach to this matter because it allows its students to obtain virtual desktop images connecting from outside networks.

An Intrusion Detection/Prevention solution has not been implemented in any of the small corporations, due to being cost prohibited. LSC1 has some level of detection due to leveraging their large firewall, logs and server capabilities; and also in order to better protect their infrastructure they have chosen to contract network penetration tests.

4.4.4 Lower-bound Benefits

Lower-bound benefits are considered those cost saving measures to consolidate, effectively manage, and prevent losses related to Information Security. It might be important to mention that cost-saving decisions do not necessarily correspond to better information security levels, because the decision to comply with regulations could lead to do the bear minimum at an affordable price, without necessarily choosing the best possible alternative. Schools corporations due to yearly changes in IT budgets are confronted with financial decisions that might require them to make adjustments in the level of security solution implemented within their networks, striving to at least comply with state and federal regulation.

The other alternative is that they have not yet been the target of attacks and infections to such a level that justifies increase in spending in enhanced information security. The majority of the lower-bound benefits are related to the upper-bound benefits, and the proposed benefits in this section will necessarily include not only a financial benefit but also a security related benefit. This was done with the purpose of not just saving by switching to a cheaper provider that offers a level of compliance with regulations, but in which also meets higher levels of information security that further

validated the need to have them (upper-bound). Under those parameters, the following cost-savings are listed below:

4.4.4.1 Networking Hardware/Software: Cisco

Since the majority of school corporations reported already a preference for Cisco as their firewall provider (and also networking equipment), the cost saving advantages that they could receive for participating of the INCSC would be that they could qualify for IOT discounts on hardware and software. Other Cisco hardware is also subject to discounts; however the analysis was concentrated in firewall products instead of the rest of networking equipment.

Another benefit proposed is that when School corporations purchase Cisco products (hardware) and services (software) through the INCSC it would allow them to qualify for e-Rate funding as long as they are under a managed services model, meaning that Cisco would control the maintenance and administration of the firewalls through the INCSC. Another benefit would be that depending on the level of “poverty level” of the school corporation it could be granted 20% to 90% of requested infrastructure funding. Projects would have to fall under one of the following categories in order to be funded by e-Rate: telecommunications, telecommunications services, Internet access, internal connections, and basic maintenance of internal connections.

Indiana Office of Technology (IOT) has an established relationship with Cisco, for that reason it has leveraged a current discount rate in equipment of 49% and SMARTnet

is first calculated to approximately 14% of the listed price and then discounted 25% again (if calculated directly, it represents approximately 10% from the listed price). The table below shows an example of the pricing for a Firewall ASA 5515 series with and without IPS (Intrusion Prevention System). The IPS feature represents a significant increase in the price of the equipment as it leverages the full potential of the solution. This example presents both alternatives to upper and lower bound scenarios, where the same device is capable of intrusion prevention (an enhanced security feature that could be classified as upper-bound) and also the difference in the pricing structure in the existence or absence of discounts (lower-bound).

Table 22. Potential benefits under IOT-Cisco price structure (See Appendix F)

Description	List Price	% of Discount	Qty	Extended	Potential Savings
Sample ASA Quote w/IPS		(49% discount:)			
ASA 5515-X with IPS, SW, 6GE Data, 1GE Mgmt, AC, 3DES/AES	$8,495.00	$4,332.45	1	$4,332.45	$4,162.55
SMARTnet Quote (Estimated 25% Discount)		(25% discount :)			
IPS SIG AND SW ASA 5515-X with IPS SW 6GE Data 1GE	$1,154.00	$865.50	1	$865.50	$288.50
Quote Total				**$5,197.95**	**$4,451.05**
Sample ASA Quote Without IPS		(49% discount:)			
ASA 5515-X with SW 6GE Data 1 GE Mgmt AC 3DES/AES	$4,495.00	$2,292.45	1	$2,292.45	$2,202.55
SMARTnet Quote (Estimated 25% Discount)		(25% discount:)			
SMARTNET 8X5XNBD ASA 5515-X with SW	$599.00	$449.25	1	$449.25	$149.75
Quote Total				**$2,741.70**	**$2,352.30**

There are two levels of discounts considered (educational, and IOT) as well as three different pricing structures: standard, educational, and IOT (representing INCSC discounts). The following table presents an example of a price structure funded via e-rate based on poverty rates, numbers are reported for a scenario of 40% and 90% poverty level from school corporation's interviews.

Table 23. e-Rate funding calculation (scenario estimate for $20,000)

(IF) Poverty level	Project Cost	School pays	E-rate pays (poverty %)
40%	$20,000	$12,000	$8,000
90%	$20,000	$2,000	$18,000

4.4.4.2 Antivirus Software: McAfee

All school corporations reported having an antivirus solution for email, servers, and computers. The following analysis presents the current unit costs calculated based on student count as reported by the majority of corporations, except in the case for SSC5 where the calculation is based on 1500 devices.

As previously mentioned the antivirus provider for the state of Indiana is now McAfee (Intel Security). We will refer to Table 11 from which the initial information for this analysis is based upon. The cost per unit maintenance for antivirus reported by IOT is $1.69 (from a total cost of $57,460 divided by 34,000 computers). In addition to the maintenance cost there is a perpetual license cost of $9.07.

Table 24. School Corporations vs. Current IOT Antivirus Cost (alternative 1)

	School alias/school student count					
2013-2014 SCHOOL YEAR	SSC1	SSC2	SSC3	SSC4	SSC5	LSC1
2013 year student count	1473	1005	3110	1049	2280	29803
Current School Solution:						
School antivirus solution - Yr 1	$0	$1,005	$10,667	$3,200	$4,000	$60,000
School antivirus solution – Yr 2	$0	$1,005	$10,667	$3,200	$4,000	$60,000
School antivirus solution – Yr 3	$0	$1,005	$10,667	$3,200	$4,000	$60,000
NPV	$0	$2,686	$28,512	$8,554	$10,692	$160,381
IOT/McAfee (alternative 1):						
Perpetual license - Yr 1	$13,360	$9,115	$28,208	$9,514	$13,605	$270,313
Maintenance cost - Yr 2	$2,489	$1,698	$5,256	$1,773	$2,535	$50,367
Maintenance cost - Yr 3	$2,489	$1,698	$5,256	$1,773	$2,535	$50,367
NPV	$16,910	$11,537	$35,702	$12,042	$17,219	$342,128
Difference	$16,910	$8,851	$7,190	$3,489	$6,527	$181,747

NPV (net present value) with a 6% interest rate

Under this alternative, accessing the same product and price that IOT have, would represent a larger investment in year 1, this scenario presents a 3 year period which is a standard period offered for antivirus contracts. The NPV (net present value) for SSC1 at the end of 3 years with the alternative 1 would have to spend $16,910 (1473*9.07), and the same with the rest of the corporations. Alternative 1 does not provide cost savings to school corporations for a 3 year period.

Similar to the case of Cisco and other providers, McAfee has developed “distinct” pricing structure tailored for K-12 school corporations, which will represent alternative 2. After consultation with McAfee Account Manager for Indiana, it was highlighted as a product that does not require the high up-front cost of perpetual licensing like in alternative 1, but instead it delivers a license per node model including 1-year gold-support and requiring the order of a minimum of 100 nodes. The McAfee ESS (Endpoint-

Protection Secure Schools) Suite has a commercial value of $2.99 (CDW website) per licensed node; however the “approximated” price provided by the account manager was $1.83 for schools corporations in Indiana. See Figure 3 for more details about the product.

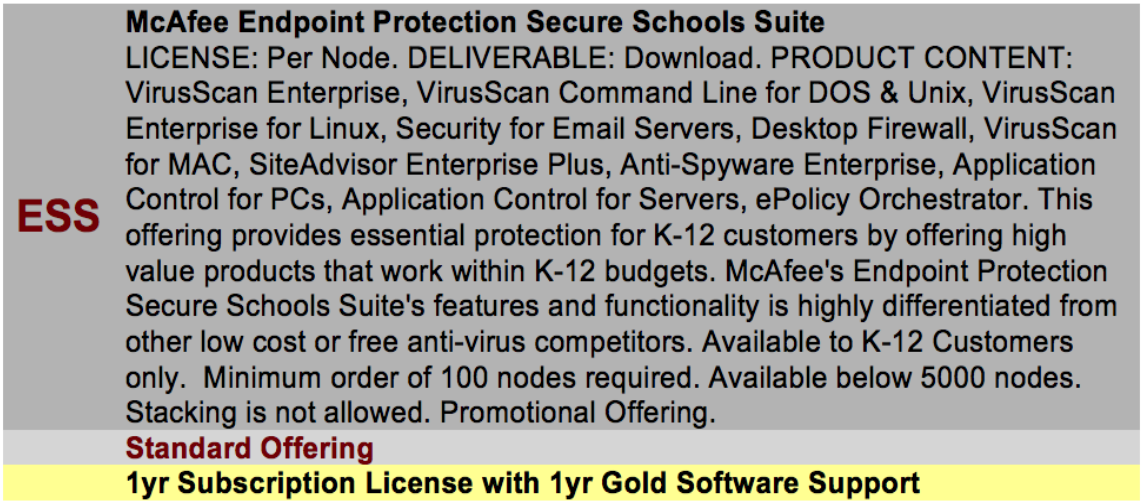


Figure 3McAfee EMM product detail (Source: McAfee) "

Table 25. Antivirus Savings Between School vs. Alternative 2 (one year) "

Antivirus Solution Provider	MS Essentials	Avast	Kaspersky	Kaspersky	K7	Barracuda
School alias	SSC1	SSC2	SSC3	SSC4	SSC5	LSC1
School Student Count	1,473	1,005	3,110	1,049	2,280	29,803
Antivirus Cost per year	$0.00	$1,005	$10,667	$3,200	$4,000	$60,000
Antivirus cost (by enrolment count)	$0.00	$1.00	$3.43	$3.05	$2.67	$2.01
Antivirus Difference with alternative 2	($1.83)	($0.83)	$1.60	$1.22	$0.94	$0.18
Antivirus Savings per Student Count (alt 2) based on difference	($2,695)	($834)	$4,975	$1,280	$1,255	$5,460

Based on the cost information provided for alternative 2, Table 25 presents the cost savings when comparing the current antivirus solution of school. For SSC1 and SSC2 the benefits are not self-evident due to the low cost antivirus that they currently have. The antivirus cost for SSC1 is $0 because it has a free antivirus. The cost provided for alternative 2 is $1.83 per licensed antivirus node. Since SSC1 and SSC2 have costs below alternative 2, then the negative amount represents what they would have to pay in addition to their current expense; these amounts are expressed in cost per unit and the total cost per antivirus. The decision to switch to McAfee through participating in the INCSC could not be merely based on cost savings, but also because of the added benefits mentioned on upper-bound benefits (accessing enterprise level antivirus security). Ultimately, each school corporation would have to assess their own willingness to switch to a provider like McAfee, provided that they could envision added benefits.

Table 26. School Corporation's Antivirus Cost vs. McAfee ESS (alternative 2)

	School alias/school student count					
2013-2014 SCHOOL YEAR	SSC1	SSC2	SSC3	SSC4	SSC5	LSC1
2013 School year Student Count	1473	1005	3110	1049	2280	29803
Current School Solution:						
Current school antivirus solution - Yr 1	$0	$1,005	$10,667	$3,200	$4,000	$60,000
Current school antivirus solution - Yr 2	$0	$1,005	$10,667	$3,200	$4,000	$60,000
Current school antivirus solution - Yr 3	$0	$1,005	$10,667	$3,200	$4,000	$60,000
NPV	$0	$2,686	$28,512	$8,554	$10,692	$160,381
McAfee ESS (alternative 2):						
Maintenance cost - Yr 1	$2,696	$1,839	$5,691	$1,920	$2,745	$54,539
Maintenance cost - Yr 2	$2,696	$1,839	$5,691	$1,920	$2,745	$54,539
Maintenance cost - Yr 3	$2,696	$1,839	$5,691	$1,920	$2,745	$54,539
NPV	$7,205	$4,916	$15,213	$5,131	$7,337	$145,785
[6% interest rate for NPV]						
Difference	**$7,205**	**$2,230**	**($13,299)**	**($3,422)**	**($3,355)**	**($14,596)**

The projection of switching to alternative 2 is presented in Table 26, in a projection of 3 years. The costs per year for this alternative were calculated by multiplying the cost of McAfee ESS of $1.83 by the number of student count per school in 2013 (except in the case of SSC5 = 1500 devices). As previously reported, SSC1 and SSC2 show to have the best price currently possible, nevertheless it will be a more detailed analysis from their part to determine if they are underpaying for antivirus security or if they would be willing to pay for the solution that McAfee ESS would offer them (See Figure 3). For the rest of the schools it seems by the numbers highlighted in blue that alternative 2 would potentially offer them cost saving benefits in a 3-year period.

4.4.4.3 IT Personnel

An observation across the small corporation spectrum could determine that they are understaffed; however the capacity of corporations to hire more IT staff might be out of scope. The researcher is not advocating for a cost saving strategy by reducing the number of IT employees, instead it proposes ways to effectively reduce in some percentage the need for outsource assistance during the year. The alternative presented would be that some of the procured services could have a level of managed support from part of the provider (allowing IT personnel to delegate the administration of those products and services to the provider) nevertheless managing the solution from a top-level view. This could also leverage savings in the area of contracting specialized

professional services. This might not be the case for Antivirus (McAfee) solution, as this usually does not require outsource assistance, but in the case of managing Cisco products and services, it might apply.

Table 27. Outsourced services spending by School Corporation

School Corporation	Contract / Professional Services for Technology	SMARTnet participation	Average salary (based on # of employees)
SSC1	$-	No	$84,285.71
SSC2	$20,000.00	Yes ($4000)	$66,000.00
SSC3	$1,800.00	No	$66,666.67
SSC4	$25,000.00	Yes ($9600)	$52,500.00
SSC5	$10,000.00	No	$50,000.00
LSC1	$50,000.00	Yes ($85000)	$73,684.53

Outsourced professional services for the configuration and maintenance of Cisco was not directly outlined during the interviews, and a direct correlation of those school corporations that do not pay for SMARTnet services and higher expenses in contractor services was not found. This could be attributed to the lack of a larger sample. For example SSC1, SSC3, and SSC5 do not pay for SMARTnet; however their expenses for contract services are not as high as expected. On the other hand, those corporations that pay for SMARTnet do show to spend more in outsourced services, perhaps due to limited expert knowledge of the products.

4.4.4.4 Computer Hardware

The information from Table 17 and 18 are the basis for the following table, which is a comparison between IOT and school corporations (small and large) averages for different type of devices. The number of computers (10, 30, and 100) were chosen arbitrarily based on suggested most frequent quantities to be purchased.

Table 28. Computer costs per breakpoints purchases (10, 30 and 100 devices)

Description \ Breakpoint purchase quantity	**10 Devices**		
(Purchaser)	**IOT**	**Small**	**Large**
Average Cost of New Laptop (Windows)	$6,680	$6,658	$10,000
Average Cost of New Laptop (OS X)	$13,000	$13,667	$13,000
Average Cost of New Desktop (Windows)	$5,040	$7,000	$7,500
Average Cost of New Desktop (OS X)	$8,500	$8,167	$9,000
Average Cost of New iPad	$6,300	$4,836	$6,500
Average Cost of New Tablet	$7,300	$6,700	$7,500
Description \ Breakpoint purchase quantity	**30 Devices**		
Average Cost of New Laptop (Windows)	$20,040	$19,974	$30,000
Average Cost of New Laptop (OS X)	$39,000	$41,000	$39,000
Average Cost of New Desktop (Windows)	$15,120	$21,000	$22,500
Average Cost of New Desktop (OS X)	$25,500	$24,500	$27,000
Average Cost of New iPad	$18,900	$14,508	$19,500
Average Cost of New Tablet	$21,900	$20,100	$22,500
Description \ Breakpoint purchase quantity	**100 Devices**		
Average Cost of New Laptop (Windows)	$66,800	$66,580	$100,000
Average Cost of New Laptop (OS X)	$130,000	$136,667	$130,000
Average Cost of New Desktop (Windows)	$50,400	$70,000	$75,000
Average Cost of New Desktop (OS X)	$85,000	$81,667	$90,000
Average Cost of New iPad	$63,000	$48,360	$65,000
Average Cost of New Tablet	$73,000	$67,000	$75,000

Table 28 shows a breakpoint structure based on the projected purchase of 10, 30 and 100 devices for each group (IOT, small and large) according to the different descriptions and the cost of each device. . The prices highlighted in blue represent the

best possible prices per description in that category. For example, in the purchase of a new Windows laptop, both IOT and the small corporation have very similar prices across all three breakpoints, indicating that the large corporation might benefit in participating of IOT purchasing program as it offer potential savings of $3,320, $9,960, and $33,200 accordingly. In the case for the estimated purchase of a new OS X base laptop, the price difference is almost indistinguishable across the breakpoints. For purchases of new Windows based desktops, IOT pricing offers the best projected price against small/large corporations, with a price difference of approximately $2,000 for 10 devices, $6,000 for 30 devices, and $22,000 for 100 devices.

In the last case for Apple desktops, iPad's and new Windows tablets, small corporations seem to have a better price overall; nevertheless, this could be because some of the device specifications might not be the same when compared to IOT and a large corporation. Even though IOT prices are still lower than the large corporation, the difference is also negligible when considering the breakpoint purchasing quantities.

There are also unrealized logistic issues involved in IOT purchasing, as it might become a complicated process to navigate for the school corporations when deciding how to proceed in their procurement of new equipment. When considering buying equipment through the INCSC project, the decision is by default limited to the offering of devices provided from HP, as it is the only authorized provider; and it might be a limitation for school corporations when wanting to compare with other providers. For more information about Hewlett-Packard (HP) pricing structure for the state of Indiana (See Appendix G).

4.5 INCSC projected Discount Rates

The Indiana Cybersecurity Services Center (INCSC as the code name designated for this project in the meantime) is a still a project in progress. EMC Corporation is currently responsible for the drafting and planning of the project; as such it is coordinating with stakeholders and proposed industry partners (i.e. McAfee, Cisco, and HP), as well as the guidelines and agreements needed to take place in order to facilitate the success of the project. One of those agreements is related to group pricing or discount rates for IOT (representing all Indiana state agencies) and projected participation of K-12 school corporations. While additional discounts for school corporations are currently considered when participating in the INCSC, those discounts were not available at the time of these analysis, for that reason it will be assumed that schools will receive the same discounts currently applied to IOT, since those percentages are current and real discounts.

The intention behind pursuing further discounts for K-12 schools is two-fold; the first one corresponds to the industry standard to offer deeper discounts for education in order to allow them afford industry products and services; the second reason is related to the interest expressed from providers to facilitate access to state-of-the-art IT security solutions for school corporations as well as capture a larger size of the school market in Indiana. (For more information about school corporations and “public” schools in Indiana, see Table 3, showing 286 public school corporations, representing 1,645 schools).

4.6 With/Without Cost-Benefit Analysis

In cost-benefit analysis, the without case does not necessarily mean without a solution, it instead represents “status quo” or another alternative that provides a solution but it might not be the most efficient alternative or use of resources. Under that presumption, then we could formulate a comparison between “without” versus “with”. The very same exercise of evaluating a current solution compared to a new alternative allows for the discovery of costs and benefits that were not anticipated or realized.

The case for *without* represents the current state of affairs at IT departments of school corporations across Indiana; and the case for *with* represents the participation in the INCSC offering of products and services. The researcher discovered a series of unrealized costs that could financially damage school corporations, benefits that could far outperform the current solutions, and unclear probabilities that something could go wrong due to the lack of historical data in relationship to K-12 IT spending effectiveness.

A clear understanding of the benefits of the *with* alternative would guide the decision to implement it, or reinforce the willingness to pay for an alternative that takes into consideration not only discounted values for cost, but also projected benefits in the near future. The difference, also called delta, between *with* and *without* cases represent those resulting benefits of the comparison of the “with” and “without” scenarios. This particular project has the possibility to isolate with/without scenario for each of the discussed security solutions (antivirus, networking, computers, and personnel) that the INCSC offers. Since the participation in the INCSC is not mandatory, and members are

allowed to select the services they are most interested or needed; then a cost-benefit analysis could be done for a with/without antivirus, networking, and/or computer provider.

4.6.1 Antivirus

The case for the antivirus with/without scenario presented two alternatives that are compared with the current solution or status quo. Alternative 2 represents a similar solution to the one that school corporations have embraced, in the sense that it provides a node licensing approach instead of a perpetual license, in contrast to alternative 1. The idea behind entertaining the idea of a different solution for antivirus at school corporations in Indiana comes from the need to increase the level of response to cyber threats to their network infrastructure. Alternative 1 and 2 attempt to do that while providing enterprise level protection from cyber threats and achieving an affordable pricing structure if possible, ultimately translating in the better use of current scarce financial resources.

4.6.2 Networking

The case for the networking scenario presents a nested with/without problem. The first situation deals with having a networking solution, with Cisco products or without, as is the case for a firewall and other networking hardware. The other iteration is included within having a Cisco solution, because so many school corporations already have Cisco equipment as their main provider, and the with/without scenario

corresponds to having technical support and extended warranty (SMARTnet) for managed services.

The first iteration corresponds to the decision to invest in Cisco as the main networking and Firewall provider, compared to a different provider. As shown before, there is at least one school (SSC1) that has implemented a different provider; nonetheless the majority has adopted Cisco. With Cisco instead of the alternative has its costs, as it represents a significant investment cost for school corporation in proportion to their yearly IT budget, although it could be offset in part by the discounts offered through educational pricing.

The second iteration of the with/without correspond to enhancing the services associated to Cisco hardware; from the standard warranty to the one offered by SMARTnet, which includes technical support, overnight replacement of equipment, managed services for configuration and monitoring of threats. This particular case might approximate closely to the reality of school corporations that have made their decision to acquire Cisco hardware, but fall short from affording SMARTnet. A development in this subject is that Cisco doesn't necessarily require all-or-nothing approach to the use of SMARTnet, which means that specific and strategic products could be selected to be covered; then corporations could select at least a few critical equipment to be protected in order to reduce the cost. Another aspect of this analysis was presented in the form of the upgrade of firewalls to an ASA model, which allows for managed Intrusion Prevention as part of those managed services covered under Cisco software (SMARTnet) agreement. "

4.6.3 Computers

The case of with/without for buying HP computer hardware (desktops, laptops, tablets) has some limited benefits, as shown in Table 28. The main benefits correspond to cost savings when purchasing equipment in increments of 10, 30 and 100 devices. Nevertheless, this comparison is limited to HP as the only provider for the state of Indiana. However, if this alternative is considered, it would provide significant cost savings only to large school corporations when purchasing Microsoft Windows based laptops and desktops.

4.6.4 Return of Investment Approach

Forrester Research has also created a framework to evaluate the financial impact of Cisco SMARTnet for organizations (their customers). This resource presents the case for a Return of Investment (ROI) or Return on Security Investment (ROSI) as it relates to networking equipment (Cisco) with the leverage of SMARTnet service. The researcher considered this resource a good guideline to evaluate the service; nevertheless it considers that there are other costs that were not included as well as other risk assessments missing. See Appendix I to access this research.

CHAPTER 5. CONCLUSIONS AND FUTURE RESEARCH

The thesis explored the current realities of K-12 school corporations IT spending as they relate to networking, antivirus, computer equipment, and IT personnel. This chapter will conclude with an encompassing recap of the findings related to those benefits corresponding to upper and lower bounds of K-12 school corporations for joining and participating in the products and services offered by the INSCS to enhance information security prevention and detection of cyber threats. This chapter will summarize the findings, present the alternatives as objective and unbiased results, and also propose recommendations for future research.

5.1 Revisiting Significance

From the interaction with school corporations, state actors, and technology providers, there is a clear agreement that information security is a very significant and increasingly relevant issue. The significance of the INCSC project could be further validated by enhancing information security of school corporations across Indiana, from where K-12 could receive more benefits than cost when participating in the INCSC project. This not only constitutes a proactive approach from the part of the state of Indiana (IOT), but also represents an opportunity for technology providers to make an example of this project to possibly be replicated across the

nation, increasing its impact to a regional or national level. If the level of security for K-12 school corporations is significantly enhanced by participating in the INCSC at a cost that is similar, equivalent or lower than the current solution; then this thesis could provide objective information to decision makers about how to access resources that would help them to better protect their networks.

5.2 Cost-Benefit Analysis Conclusions

This section will present conclusions related to the findings from the previous chapter as they relate to computer equipment, networking equipment, antivirus, and personnel.

5.2.1 Procurement of Computers

From the data collected based on average computer costs per OS (operating system) and type (desktop, laptop, tablet, iPad) it was determined that the most significant benefits are for large school corporations when it comes to the purchase of Windows based desktops and laptops. In any other categories, the costs through participating in the INCSC were similar or very close to the prices that school corporations are currently paying for those assets. In many categories small school corporations had a lower price; however, those corporations might require different specifications for devices' speed and capacity, which could lower the price when compared with IOT and large school corporations.

School corporations have different bidding procedures when procuring equipment; this aspect was not covered in detail by the researcher. Nor was the level of "

experience required to deal with Indiana state logistics when purchasing equipment. Unless there would be significant reduction in the current pricing structure of HP hardware, it would only be beneficial to large school corporations to purchase Windows base desktops and laptops through the INCSC (refer to Table 28).

5.2.2 Procurement of Networking Equipment

For those schools that have adopted Cisco technology as part of their firewall and internal networking solution, participating in the INCSC provides them with more benefits than costs. These benefits could be different depending on the level of product adoption stage school corporations currently have. Those stages could be 1) a corporation does not have Cisco (or very little) and is considering it as a significant investment, 2) a corporation has already Cisco equipment, but not SMARTnet, 3) a corporation has equipment and SMARTnet but not a managed solution for intrusion prevention (IPS). In the first case school corporations would have preferential discounts, just as they would if they purchase directly, with a 49% discount in hardware and an approximate SMARTnet cost of 10% from the listed price compared to a 45% and 7% when purchased directly. At this point, it might seem that both options are almost indistinguishable if hardware and software are acquired together, see table below for an example based on a $33,990 ASA series firewall.

Table 29. Calculation of Cisco costs with IOT and Educational discount

List Price		Hardware	Software	total
$33,990.0	(IOT Discounts)	$18,694.50	$2,379.30	$21,073.80
	(Educational Disc.)	$17,334.90	$3,399.00	$20,733.90

In the second case, school corporations would still be able to pick and choose what equipment to protect under SMARTnet. In the third case, the added benefit would be that in the case of firewall equipment (with IPS capable devices) would be under active management from Cisco at no additional cost. For all three cases, the benefit of acquiring Cisco products would also qualify for e-Rate reimbursement, if and only if, active management of the services is activated and the IPS feature is enabled. The reimbursement represents a great return on investment to school corporations because it subsidizes the cost of investment.

In conclusion, if a school corporation either decided to implement Cisco products, increase coverage or participate of SMARTnet services, doing so through the INCSC would be more beneficial. The greatest benefit apart from the cost savings on hardware and software would be the reimbursement of funds thought e-Rate and the managed services of firewall IPS (intrusion prevention system).

5.2.3 Procurement of Antivirus

The use of antivirus is widely accepted and utilized across school corporation's security practices in the state of Indiana. As shown in the previous chapter, different corporations have adopted different antivirus solutions for different terms of contracts. Participating in the INCSC would provide school corporations access to enterprise level antivirus service at a cost that is competitive to other products in the marketplace. The analysis of the antivirus presented two alternatives, the second one is presented by the researcher as the most optimal and competitive alternative. This alternative offers not

only lower-bound benefits (cost savings), but also it offers enterprise level antivirus tailored to school corporations with the possibility of a centralized threat monitoring.

In conclusion, McAfee antivirus as an INCSC product/service offers more benefits than costs for school corporations, with the constraint that the cost should not be lower than $1.83 per node license. If that constraint is not met, then each corporation should evaluate their willingness to pay for the combination of upper and lower bound benefits offered by antivirus alternative 2.

5.2.4 Personnel Contracting

This section cannot conclude in suggestions to hire more IT personnel or discontinue contracting services. What the researcher could say is that if school corporations decide to embrace some of the enhanced product/services offered by the INCSC, then there are benefits with respect to expertise in the management of the those products/services that are no longer required to be outsourced. The costs associated with contracting professional services, provide training for their IT staff, and other related expenses could be avoided in order to provide savings as well.

A lower-bound alternative to analyze the personnel component at school corporations would have been the cataloging of IT staff activities in order to determine, if some services were to be managed by the INCSC, how it would be beneficial to relocate their time towards other information security related tasks in benefit of their organizations. This alternative falls, unfortunately, out of scope for this research, however the INCSC could offers lower bound benefits to school corporations in Indiana

in the forms of decreasing the need for contracting services that could be provided by the INCSC.

5.3 Revisiting Research Question

Would participation in the INCSC provide more benefits than the costs associated with cybersecurity for K-12 Schools in Indiana?

Chapter four presents a compelling case for the benefits of participating in the INCSC as the option for school corporations to benefit from enhancing upper-bound as well as lower-bound one reflected in better information security for the former and cost savings for the later.

5.4 Future Research Proposed

Resistance to participate, share generic and specific cost related to information technology was the norm during the duration of the project. In the opinion of the researcher, this was due to the lack of interest in participating in this research after financial information was requested. Different avenues were used to contact school corporations and key personnel within the IT department.

As a result, the research sample size was smaller than planned, especially given the number of school corporations in Indiana. For that reason the researcher proposes a different approach to school corporations. This new approach requires the buy-in from the Indiana Department of Education (IDoE), and specifically from its Director of

Information Technology. He could help to promote this initiative statewide, as responsible of the creating of a Technology Budget for School Corporations when they receive funds for e-rate. See Appendix L for details regarding the certification of school technology plan.

The cost of a data breach is an unexplored issue for the majority of school corporations interviewed (Appendix H). For that reason the researcher suggest the use of resource like the one presented in Appendix J as an example of the itemized cost to be included when determining the potential costs of a data breach (DB), the only caveat is that it is based on a private enterprise model that uses revenue as the basis of the calculation, which is not the case for public school corporations. This resource is a compliance model for determining the cost of a DB, links to the original materials are also available there.

Appendix K on the other hand presents another strategy in order to avoid costs related to network intrusions and data corruption, this strategy comes in the form of insurance or risk transfer. There are also research that points out the need to seriously address Information Security costs according to Brecht and Nowey (2012), and communicating the economic value of security investments according to Hulthen (WEIS 2008). Both papers emphasize the need to quantify the impact of security in an organization.

When school corporations participate from the services provided by the INCSC, could that potentially improve the level of protection against threats and vulnerabilities?

It would be beneficial to determine how the risk levels change by, either investing in improving information security as a stand-alone corporation, in contrast to doing it through the INCSC. Thus, measuring the impact of investments in cybersecurity would be a beneficial endeavor.

REFERENCES "

LIST OF REFERENCES

Boardman, A., Greenberg, D., Vining, A., and Weimer, D. (2010). Cost-Benefit Analysis: Concepts and Practice. 4th Edition. ISBN-10: 0137002696 | ISBN-13: 978-0137002696

Brecht, M., and Nowey T. (2012) A closer look at information Security Costs. WEIS2012: workshop on the Economics of Information Security. Retrieved from: http://weis2012.econinfosec.org/papers/Brecht_WEIS2012.pdf

Campbell, H., and Brown R,. (2003). Benefit-Cost Analysis: Financial and Economic Appraisal Using Spreadsheets. Cambridge University Press. ISBN-10: 0521528984 | ISBN-13: 978-0521528986

Caplan N. (2013). Cyber War: the Challenge to National Security. University of North Carolina. Global Security Series. Volume 4. Issue 1. Retrieved from: http://globalsecuritystudies.com/Caplan%20Cyber.pdf

CDW website. McAfee Endpoint Protection Secure Schools Suite - subscription license. Retrieved from https://www.cdw.com/shop/products/McAfee-Endpoint-Protection-Secure-Schools-Suite-subscription-license-1/2556775.aspx

Census.GOV website. US Department of Commerce. Education Funding: Where do Schools Get Their Money? How do They Spend it?. (June 21, 2012). Retrieved from http://blogs.census.gov/2012/06/21/

Cisco Warranty. Retrieved from http://www.cisco.com/c/en/us/products/warranty_qa_guest.html, see also http://www.cisco.com/web/services/portfolio/product-technical-support/SMARTnet/index.html

Collins, J., Sainato, V. A., Khey D. N. (2011). Organizational Data Breaches 2006 – 2010: Applying SCP to the Healthcare and Education Sector. University of New Orleans. International Journal of Cyber Criminology (IJCC) ISSN: 0974-2891 Volume 5 (1): 794-810. Pg. 805.

Gordon, L,. and Loeb, M. (2005). Managing Cybersecurity Resources: A Cost-Benefit Analysis. New York: McGraw-Hill. ISBN-10: 0071452850 | ISBN-13: 978-0071452854 | Edition: 1

DoE - Department of Defense. The CyberDomain. (2013). Retrieved from: http://www.defense.gov/home/features/2013/0713_cyberdomain/

FCC Website. E-Rate - Schools & Libraries USF Program. (October 6, 2014). Retrieved from http://www.fcc.gov/encyclopedia/e-rate-schools-libraries-usf-program

GAO: Government Accountability Office. (2013). Cybersecurity – A better-defined and implemented national strategy is needed to address persistent challenges. Publication number: GAO-13-462. Released on March 7th, 2013. Retrieved from: http://www.gao.gov/assets/660/652817.pdf

GAO: Government Accountability Office. (2013). Information Security – Agency Responses to Breaches of Personally Identifiable Information Need to Be More Consistent. Publication number: GAO-13-34. Released on December 2013. Retrieved from: http://www.gao.gov/assets/660/659572.pdf

IDOE - Indiana Department of Education. Find a School and Corporation Data Reports. (10/13/2011). Retrieved from http://www.doe.in.gov/accountability/find-school-and-corporation-data-reports

IOT - Indiana Office of Technology. About us. Retrieved from http://www.in.gov/iot/2416.htm

McGinnis, M. D. (2005). Costs and Challenges of Polycentric Governance: An Equilibrium Concept and Examples from U.S. Health Care (May 2, 2011). Available at SSRN: http://ssrn.com/abstract=2206980 or http://dx.doi.org/10.2139/ssrn.2206980

MSISAC: Multi-State information Sharing & Analysis Center. (2012). Risk Management Guide. Retrieved from: http://msisac.cisecurity.org/resources/guides/documents/Risk-Management-Guide.pdf

Norton-Symantec. (2013) 2013 Norton Report of interviews conducted between July 4th, 2013 to August 1st, 2013. Retrieved from: http://www.symantec.com/about/news/resources/press_kits/detail.jsp?pkid=norton-report-2013

Nye J. S. (2012). Cyber War and Peace. Project Syndicate. Retrieved from http://www.project-syndicate.org/commentary/cyber-war-and-peace

Ostrom, E. (2008). Polycentric Systems as One Approach for Solving Collective-Action Problems. Indiana University, Bloomington: School of Public & Environmental Affairs Research Paper No. 2008-11-02. Available at SSRN: http://ssrn.com/abstract=1936061 or http://dx.doi.org/10.2139/ssrn.1936061

Polski, M. M., and Ostrom, E. (1999, February). An institutional framework for policy analysis and design. In Workshop in Political Theory and Policy Analysis Working Paper W98-27. Indiana University, Bloomington, IN. Retrieved from: http://mason.gmu.edu/~mpolski/documents/PolskiOstromIAD.pdf

Quinn Patton, M. (2001). Qualitative Research & Evaluation Methods. 3rd Edition. ISBN-10: 0761919716 | ISBN-13: 978-0761919711 | Edition: 3rd

Shackelford, S. (2012). Toward Cyber Peace: Managing Cyber Attacks Through Polycentric Governance. American University Law Review, 2013. Available at SSRN: http://ssrn.com/abstract=2132526 or http://dx.doi.org/10.2139/ssrn.2132526

Snell M. (2010). Cost-Benefit Analysis: A practical guide. Thomas Telford Publishers. ISBN-10: 0727741349 | ISBN-13: 978-0727741349 | Edition: 2

APPENDICES "

Appendix A: Scoping questioner prior to interview Template

Appendix A.1: Prevention

	Human	Hardware	Software
Prevention	Who is responsible for: - Installing/updating antivirus solution - Configuration of network devices Who creates and updates policies about password enforcement. Who controls the physical access to data is secured? Is there someone responsible for compliance with FERPA educational records?	What are the existing firewalls, routers, switches Servers: type and purpose Data Backup Appliances What is the size of the network? (from an inventory perspective) What type of devices ensure the physical safety of data What is the renewal period of technology equipment	What type of antivirus (management) software is used? Internet Filters Auto Backup software What type of domain controller is used? What is used to to authenticate and authorize network resources Are there policy driven software to detect unauthorized access to education records?
	Who are the implementers of policies related to access and authentication into the network		
	Who is responsible to setting-up and verifying data back-ups	What are the appliances to perform this task? How is the data storage?	Are backups automatically created by backup software?
	Has your personnel performed any of the following administration?	Do you have equipment that supports any of the following tasks?	Do you have software that supports any of the following tasks?
	Intrusion prevention, Firewalls/Routers/Witches and VPN configuration, Web and email filtering, Antivirus protection.		
	If contracting-out services, what are those services and what are the costs?		
	Who is responsible to secure student and employee records Who is responsible to secure financial records	What HW is used to secure student and employee records What HW is used to secure financial records	What software to secure student and employee records What software to secure financial records
	Has your personnel performed any of the following administration?	Do you have equipment that supports any of the following tasks?	Do you have software that supports any of the following tasks?

Appendix A.2: Detection

	Human	Hardware	Software
Detection	What are the processes done by internal personnel? What are those processes that are outsourced? Who performs the monitoring of Antivirus Who performs the monitoring of firewalls, routers, switches Who manages email solution Who manages Internet Filters? Have you experienced in the past a malware/virus infection, to what rate?	What type of appliances have dedicated to detection of intrusions What provider is used for Is your email solution hosted internally or externally? Would you consider that your HW responds to your speed needs?	What type of intrusion detection software (IDS) is used? What type of intrusion prevention software (IPS) is used? What is the type of file system used? Are the firewall(s), router(s), switch(es) What platform is Would you consider that current AV solution was/is appropriate?
	Has your personnel performed any of the following administration?	Do you have equipment that supports any of the following tasks?	Do you have software that supports any of the following tasks?
	Event Management, Vulnerability Scanning		
	Who is responsible for ensuring compliance to state and federal regulations (ei: FERPA, FSMA, and HIPAA) Who is responsible detecting leakage of records	Do you count with devices/appliances to detect unauthorized access to resources?	Do you count with any SIM, ePO tools? Do you count with software products that detect data leakage?

Appendix B: Interview Template

Confidentiality,VS,Personnel/Hardware/Software,VS,Prevention/Detection,solutions,
!

Indiana!School!Corporations!–!Interview!Template!

School!Name:

! _____!

IT!representative:

! _____!

GENERAL!Questions:!

1. What!is!the!number!of!schools!within!your!corporation?!
    a. How!many!elementary,!middle,!high!schools?!
    b. Are!there!other!"programs"!that!utilize!your!IT!services?!
2. What!is!the!approximate!number!of!children!served?!
    a. Do!they!have!user!accounts?!
        i. Is!it!dependent!on!their!age?!
        ii. Is!it!limited!to!school!network!perimeter?!
3. What!is!the!approximate!number!of!employees!!(teachers,!staff,!aids,!…)!with!granted!access!to!your!network!resources.!
    a. Approximate!number!of!teachers!
    b. Approximate!number!of!staff!
    c. Approximate!number!of!aids!
    d. Specific!number!of!IT!staff!
        i. Are!they!segregated!in!function/location?!Y/N!
        ii. What!is!the!budget!for!IT!Staff?!!
            1. Is!your!school!corp.!planning!to!increase!the!number!of!fullXtime!IT!staff?!!

Complete list of questions as follows:

Indiana School Corporations – Interview Template
School Name: _____

IT representative: _____

GENERAL Questions:

1. What is the number of schools within your corporation?
    a. How many elementary, middle, high schools?
    b. Are there other "programs" that utilize your IT services?
2. What is the approximate number of children served?
    a. Do they have user accounts?
        i. Is it dependent on their age?
        ii. Is it limited to school network perimeter?
3. What is the approximate number of employees (teachers, staff, aids, …) with granted access to your network resources.
    a. Approximate number of teachers
    b. Approximate number of staff
    c. Approximate number of aids
    d. Specific number of IT staff
        i. Are they segregated in function/location? Y/N
        ii. What is the budget for IT Staff?
            1. Is your school corp. planning to increase the number of full-time IT staff?
            2. Or it plans to increase consultants?
        iii. What are the main tasks performed by IT staff?
    e. What are the specific areas of IT that are contracted out?
        i. How many contractors/consultants do you have?
        ii. How much do you pay a month/year?
        iii. Do they render services remotely or in-person
        iv. What are the main tasks contracted out?
            1. Are they related to a product or a service
            2. What are the cost associated to those product/services
        v. Are you satisfied with the service received? Y/N
            1. How long have you done business with this provider?
            2. Are you planning to change providers?
            3. What would be the reason to consider changing providers? Cost / Bad service
        vi. When looking for a contractor, what type of search do you conduct? Online/ask other schools/national board/etc

HARDWARE questions:

4. Approximately how many computers do you manage?
    a. Have you received grants for purchase of technology equipment?
    b. Number of Desktops
        i. What is the predominant brand?
        ii. What is the average cost?
        iii. Do you buy them as needed or according to a renewal cycle?
            1. What is your planned and real renewal cycle?

    c. Number of Laptops
        i. What is the most common type? Chrome books, macs, windows.
        ii. Are they for staff? How many
        iii. Are they students? How many
        iv. Do you buy them as needed or according to a renewal cycle
            1. What is your planned and real renewal cycle?
        v. Do you pay for recovery services? Computrace/other.
    d. What is the average cost of a computer/laptop when you buy?
        i. New Laptop (type)
        ii. New Desktop (type)
        iii. New iPad
        iv. Refurbish Laptop
        v. Refurbish Desktop
5. Do you have a 'one-to-one device" policy? Y/N
    a. Number of iPad's or other touch screen devices (tablets or convertible laptops)
    b. Are they purchased or leased (at what cost)
    c. What is your planned and real renewal cycle? (why?)
6. Number of Servers
    a. Do you have a dedicated datacenter/server room? Y/N
        i. Do you have power protection/redundancy?
        ii. Do you have fire protection?
        iii. Do you have water damage protection?
    b. Have you implemented virtualization? Y/N
        i. Have you outsourced the initial installation/configuration?
        ii. What technology have you used? (What is the cost?)
    c. How many servers do you maintain?
    d. What is your planned and real renewal cycle?
7. Connectivity
    a. What is the network connection between buildings? T1s/ Fiber/ other
    b. What is the network speed?
    c. Do you use VPNs or encrypted communication?
8. ISP
    a. Do you subscribe to e-rate ISP services? Y/N
        i. Y: What is your discounted/reduced (lunch) ratio?
    b. What is your main ISP?
    c. What is the yearly cost?
    d. Do you have a secondary ISP? And Cost?
    e. Are you satisfied with your current ISP?
9. Networking
    a. What type of networking equipment do you have?
    b. What is the mayor provider of that equipment
    c. Do you purchase/lease/purchase + maintenance?
        i. How much it costs to maintaining a year?
        ii. What is your planned and real renewal cycle?
    d. Are you satisfied with your current solution/provider?
    e. How often do you renew this equipment(s) or entire solution?
10. Telephony
    a. Do you have IP telephony? Y/N
        i. Y: How much did it cost? How long ago?

ii. N: Are you planning to implement it?

11. Surveillance
    a. Do you have analog/digital surveillance cameras?
    b. Are they remotely accessed? By administrator or law enforcement?
    c. Are they backed-up with your regular data-backups?

12. Backup solution
    a. Do you have a dedicated backup solution?
    b. Is the Backup performed by IT staff or a third party?
    c. What was the cost of implementation of THIS solution(s)?
    d. What is the capacity and frequency?
    e. Do you have a storage contingency plan? (Outside storage) explain.

SOFTWARE questions:

13. Antivirus
    a. What type of Antivirus do you currently use?
    b. What is the cost? (Is it per seat or student count).
    c. What is the term of the contract?
    d. Are you satisfied with your current provider?
        i. Y: Why?
        ii. N: Are you considering changing to a different provider?
14. What network directory administration solutions do you have implemented?
    a. Do you have a software agreement with the provider?
    b. How do you assess authentication on your network?
15. Software Spending
    a. What is the percentage of your IT budget spent on software-related products?

SERVICES questions:

16. If you were to be granted an important amount of money for IT expenses, what would you spend it? (According to you priorities, needs, wants) LIST:

17. Would you be interested in products/services that help enhance your detection and prevention of threats to your network?

Appendix C: Information Request Form to School Corporation

[Faxed to Superintendent requesting access to IT Budget]

Request for Access to Public Records

Date of Request: March 1, 2014 Time of Request: 12 pm

Name of Person Requesting Record: [redacted]

Representing: Information Security Graduate Student – Purdue University

Telephone Number: 765-[redacted] Email Address: [redacted]@purdue.edu

Address: [redacted] Oval Drive (Street) West Lafayette (City) IN 47907 (State/Zip)

Please identify with reasonable particularity the record(s) being requested:

The request of access to [redacted] school corporation budget records, as it relates to IT spending, will serve to be used in my Graduate Thesis project that attempts to evaluate cost-benefits to school corporations of participating of a State initiative to procure and provide access to enhanced information security products/services.
Even though, full access to IT budget would be desirable, there are specific budget line items that are very important for me to obtain:

- Number of IT personnel and the overall (total sum) salary budget.
- Cost of Antivirus software to protect user computers and servers (what is the provider's name and for how long was the contract, is the cost based on computers or student count?)
- What is the main provider of networking equipment and what is the recurrent cost of warranty/support services (is it a monthly or yearly cost)
- What is the budget assigned to computer purchases? What is the average cost that you are willing to pay for a new computer, laptop, "tablet"? What is the main provider you buy from? Do you buy directly from manufacturer or use a retailer?
- What are cost associated with contracting IT services? What are the areas most commonly outsourced?

[I submit this request under the advise of Mr. [redacted], in order to formalize it]

Signature of Person Making Request: _____

The fee for copying documents is ten cents ($.10) per page for non-color, and twenty-five ($.25) cents per page for color copies. Fees are payable when any record is duplicated and may be paid by cash or money order – payable to [redacted] School Corporation.

FOR OFFICE USE ONLY

Date and Time Request Received:
Name of Person Receiving Request:
Request Filled by: Date:
Items Not Filled On Request with Reason Listed:

Appendix D: IT budget template (Excel format)

Appendix D.1: Budget template email introduction by IDOE:

Email Introduction by the Director of Indiana School of Safety Specialist Academy – Indiana Department of Education to all participating schools in Indiana:

From: noreply@doe.in.gov [mailto:noreply@doe.in.gov]
Sent: Friday, February 14, 2014 10:14 AM
Subject: LC: IDOE - School Safety Specialist Academy: Forum

Ryan Stewart has posted a new forum posting to forum thread Information Security Project for the community IDOE - School Safety Specialist Academy. View and Respond Online

A graduate student at Purdue is looking for school corporations that would agree to facilitate access to data and to their IT staff for interviews as part of a thesis. The purpose of the thesis is to provide an understanding of the current solutions adopted by K-12 schools networks in Indiana. Information from participating schools would generate a map of what services are most used, needed and desired by schools. In order to facilitate the release of this type of school data and because the goal of the thesis is not the rating of specific schools regarding their cybersecurity, the sources would be aggregated and anonymized. This research fits into a larger project from the state of Indiana to promote and facilitate security services assistance to K-12.

If you would like to participate, or have more questions, please contact:

Appendix D.2: Budget template email introduction by Researcher "

[redacted]

My name is [redacted] and I am a graduate student at Purdue University pursuing a Masters in Information Security. As I mentioned before, my thesis relates to a project in development targeted to improve cybersecurity in the State of Indiana, an initiative from IOT (Indiana Office of Technology), from which I became involved during my internship last summer. My thesis attempts to measure the current costs associated with maintaining confidentiality in the intersection between prevention/detection and human/hardware/software.

The project of creating a cybersecurity center for Indiana is undergoing in partnership with leading technology providers in the country; one of the realized benefits during the conceptualization of this project was that it could also offer enhanced security services to K-12 schools. Using a model that the state already has implemented (a centralized procurement of services for state agencies), which potentially lowers the cost and provides a wider range of services to its participating organizations. The reasons why there is an interest to include K-12 schools in this project obeys three factors; the first one is the believe that there is a need to improve schools readiness and resilience against cyber-attacks; the second one is the affordability factor since many schools might not have the capacity to fully implement security solutions due to budget or staff constraints; the last one has to do with education, as there is consensus in developing cybersecurity awareness programs for kids at schools, this is of course a future goal after the schools are better protected.

In that pursue, I am looking for school corporations that would agree to be part of this early evaluation phase, facilitate information and access to interview employees with direct influence over IT, this will help me provide a deeper understanding of the state of cybersecurity of K-12 schools in Indiana, based on that it would allow me to map what services and most needed and desired by schools to be offered by the Indiana cybersecurity services center (InCSC). In order to facilitate the release of this type of school data, I would make sure that the sources are anonymized for the thesis document, I will only share this information with my thesis committee while they guide me in the process of this work. The purpose is not the rating of specific schools regarding their cybersecurity levels, instead is to make a case for the development of an affordable and attractive offer of products and services to schools in order to enhance their protection. Ultimately, the InCSC would act as a public broker of private services of security-as-a-service.

I hope this short explanation has presented the idea clearly, and I am more than willing to answer any further questions, you could also contact my thesis advisor and committee chair, professor [redacted] could verify my statements. Thank you for your time.

Regards,

[redacted]

Appendix D.3: Excel budget template. "

Once contact was established, the budget template would be send as shown: "

School Corporation _&&&&&&&&&&&
Contact _&&&&&&&&&&&
Email _&&&&&&&&&&&

2013%2014'SCHOOL'YEAR	Capital& Projects	Technology& Fund	Textbook& Funds	Grants	Other&	Other&	Other&	Subtotal'by' catergory	%&of&total&by& category
Salary									#DIV/0! #DIV/0!
Hardware									#DIV/0! #DIV/0!
Software									#DIV/0! #DIV/0!
Professional&Development& (non&salary;&expenditures&s& required)									#DIV/0! #DIV/0!
Telecommunications									#DIV/0! #DIV/0!
Contract&&Professional& Services&for&Technology									#DIV/0! #DIV/0!
Sub&Total&by&Source	$&	$&	$&	$&	$&	$&	$&	$&	
%&of&Total&by&Source	#DIV/0!	#DIV/0!	#DIV/0!	#DIV/0!	#DIV/0!	#DIV/0!	#DIV/0!		

ADDITIONAL INFORMATION **~COST**

Building distribution Consolidated in one building
Staff (Admins, Teachers, Aids)
Number of Elementary Schools kids
Number of Middle Schools kids
Number of High Schools kids
kids

Approximated number of computers Desktops/laptops
IT Staff (onsite)
IT Contractors (outsource)

Software total per year
Previous AV
Current AV

Computers

Renewal of Desktops years each desktop
Renewal of Laptops years each Laptop
Renewal of Mobile Devices each Mobile Device
Renewal of HW by state surplus and grants

Infrastructure
ISP providers year

Backups capacity recurrent? Or one time

NEEDS IMPROVEMENT / NICE TO HAVE

Appendix E: HP pricing information for STATE-OF-INDIANA (public sector) "

United States-English

» HP Home | » Products & Services | » Support & Drivers | » Solutions | » How to Buy

» Contact HP | Buy online or call **1-800-727-2472** & | Search: | Part Number Search

Systems & Hardware &

| » Store home | » Computing | » Printing and digital imaging | » Supplies & Accessories

Public Sector home > Laptops > HP Notebook PC > -New-Configurable-HP 350 G1 Notebook PC

Laptops

-New-Configurable-HP 350 G1 Notebook PC

HP recommends Windows.

» **K-12 education**

Shopping cart

Your cart is empty

» Login/register '
» Retrieve saved quote '
» Order history '
» Order status '
» Standards

Add Item to cart

enter part numbe

» Product search/compare
» View contract price list '

» Ordering information '

Accessibility
» Section 508 accessibility

Support & Drivers
» Customer service '
» Get drivers, promotional ' newsletters, & updates '

Download the latest Adobe® Reader®.

Follow us on: &

Current selection: & IN -STATE OF INDIANA

Change selection: Select a contract and click the button to the right

Displaying 1-5 of 5 products Display ALL products per page

Previous 1 Next

Bases/Features &	» Configurable - HP 350 G1 Notebook PC w/ Intel Celereon F6P39AV	» Configurable - HP 350 G1 Notebook PC w/Intel i3-4005U F6P40AV	» Configurable - HP 350 G1 Notebook PC w/Intel i5-4200U F6P41AV	» Configurable - HP 350 G1 Notebook PC w/Intel i7-4500U F6P42AV	» Configurable - HP 350 G1 Notebook PC w/Intel Pentium & 3558U & F6P43AV
BaseId	Customize »	Customize »	Customize »	Customize »	Customize »
Price &	**$815.50**	**$859.50**	**$903.50**	**$1,123.50**	**$791.20**
Operating system	Windows 7 Professional 64 (available through downgrade rights from Windows 8.1 Pro)	Windows 7 Professional 64 (available through downgrade rights from Windows 8.1 Pro)	Windows 7 Professional 64 (available through downgrade rights from Windows 8.1 Pro)	Windows 7 Professional 64 (available ' through ' downgrade ' rights from ' Windows 8.1 ' Pro) '	Windows 8.1 64-bit
Processor &	Intel® Celeron® 2957U (1.4GHz, 2MB Cache) Processor, and Intel HD Graphics	Intel® Core™ i3-4005U (1.7GHz, 3MB Cache) Processor, and Intel HD Graphics 4400 '	Intel® Core™ i5-4200U (1.6GHz w/ Turbo, 3MB Cache) Processor and Intel HD Graphics 4400	Intel® Core™ i7-4500U (1.8GHz, 4MB Cache) Processor, and Intel HD Graphics 4400	Intel® Pentium® 3558U (1.7GHz, 2MB Cache) Processor, and Intel HD Graphics
Display &	15.6-inch diagonal LED-backlit HD anti-glare SVA (1366x768)	15.6-inch diagonal LED-backlit HD anti-glare SVA (1366x768)	15.6-inch diagonal LED-backlit HD anti-glare SVA (1366x768)	15.6-inch diagonal LED-backlit HD anti-glare SVA (1366x768)	15.6-inch diagonal LED-backlit HD anti-glare SVA (1366x768)
Integrated camera	Integrated HD Webcam	Integrated HD Webcam	Integrated HD Webcam	Integrated HD Webcam	Integrated HD Webcam
Memory &	4 GB 1600 MHz DDR3 SDRAM (1D)	4 GB 1600 MHz DDR3 SDRAM (1D)	4 GB 1600 MHz DDR3 SDRAM (1D)	4 GB 1600 MHz DDR3 SDRAM (1D)	4 GB 1600 MHz DDR3 SDRAM (1D)
Internal Storage &	500 GB 7200 rpm SATA hard drive	500 GB 7200 rpm SATA hard drive	500 GB 7200 rpm SATA hard drive	500 GB 7200 rpm SATA hard drive	500 GB 7200 rpm SATA hard drive
Optical Drive Bay	DVD±RW SuperMulti DL Drive	DVD±RW SuperMulti DL Drive	DVD±RW SuperMulti DL Drive	DVD±RW SuperMulti DL Drive	DVD±RW SuperMulti DL Drive

Appendix F: Cisco Quote for ASA with/without IPS (Intrusion Prevention System) and " SMARTnet cost for School Corporations. "

From: , Account Manager
Indiana K-12 and Local Government
Cisco Systems, Inc.
11711 North Meridian Street, Suite 700
Carmel, IN 46032
(317)
@cisco.com

Description	List Price	49% Discount	Qty	Extended
Sample ASA Quote w/IPS				
ASA 5515-X with IPS, SW, 6GE Data, 1GE Mgmt, AC, 3DES/AES	$8,495.00	$4,332.45	1	$4,332.45
SMARTnet Quote (Estimated 25% Discount)				
IPS SIG AND SW ASA 5515-X with IPS SW 6GE Data 1GE	$1,154.00	$865.50	1	$865.50
Quote Total	13.58%			**$5,197.95**
Sample ASA Quote				
ASA 5515-X with SW 6GE Data 1 GE Mgmt AC 3DES/AES	$4,495.00	$2,292.45	1	$2,292.45
SMARTnet Quote (Estimated 25% Discount)				
SMARTNET 8X5XNBD ASA 5515-X with SW	$599.00	$449.25	1	$449.25
Quote Total	13.33%			**$2,741.70**

Appendix G: Enumeration of possible benefits

Benefits for School Corporations

- Potentially minimize your liability in the event of a lawsuit. If you are successfully attacked, the attacker may have access to your computers and network. In a distributed denial of service attack, this attacker uses your resources to attack yet another company. How well your systems were protected is part of the discussion in determining who is liable for the attack. Any attack is a crime, but if you do not properly secure your business, it could be held partially responsible.
- Access to highly specialized consultants that are affordable, monitoring the health of your network might not be a priority over functionality. Access to this resource could prove cost-effective in the long term, especially when considering the cost of hiring a permanent specialist for your company, keeping them trained, and paying them a full time salary and benefits. Hiring is not discourage, but perhaps by hiring a consultant initially might fit school budgets, for example in order to avoid vulnerabilities hat could lead to a denial of service attack.
- Secure computing habits will transfer across environments. Educational programs could be extended to students and their parents. This could represent a great benefit to a much larger audience.
- Rewarding schools good security behaviors and those who stand up for good information security. Recognition for doing something well boosts morale of school corporations and to serve as examples to others. “InfoSec School Corporation of the month/year award”.
- Reducing the number and extent of information security breaches. The sooner vulnerabilities are identified, the lower the cost of addressing it will be. Direct costs (e.g., cost to recover data lost or altered during an incident, cost to notify customers of breaches, fines for non-compliance) and indirect costs (e.g., lost

customers, lost productivity, time spent investigating/resolving breaches and hoaxes) will decrease. Preventing the negative press that can result from security breaches would also become an added benefit.

- Reducing systems' costs by allowing control measures to be designed into systems solutions rather than adding them to installed systems. (It is significantly more expensive to retrofit a control than to design it into an application or system.) It seems like some corporations have implemented specific solutions for each need, and there is an opportunity to implement solutions that are deployed to cover several areas with one centralized management reporting tool.
- Providing savings through coordination and measurement of all security awareness, training, and educational activities while reducing duplication of efforts.
- Proved compliance. Allowing school corporations to demonstrate compliance with regulations that require information security awareness and privacy training (such as the Federal Information Security Management Act, the Health Insurance Portability and Accountability Act, the Gramm-Leach-Bliley Act, the Sarbanes-Oxley Act)

Benefits for IT personnel and other employees

- Access to training for IT staff in management of new tools and services, as well as Industry certifications related to Information Security practices. A better-managed network could allow personnel to pursue specialized education (possibly at a special rate) in information security related areas.
- Helping employees to identify and respond appropriately to real and potential security concerns that might be overlooked by providing updated information related to new risks and what to do about them.

- Helping in promoting awareness of employees, contractors, and business partners about the significance of data on their computers and mobile devices (PDAs, thumb drives, smart phones, etc.) are valuable and vulnerable.
- Disseminating proper information to staff, such as how to avoid scams, fraud, phishing, and ID theft. Information on how to protect home PCs and how to use e-mail and the Internet safely lets employees know that your organization cares about them. Building good computing habits at home is as important as building those behaviors at work.
- Ensuring that they understand that they are legally responsible for the integrity of the organization's information assets.

SW Security

- Access to specialized DDoS monitoring.
- Access to network monitoring capabilities (traffic, unauthorized access, unusual outgoing traffic)
- Access to integrated and centralized security management solutions that offer an enterprise level access to antivirus, assets management, end-point encryption.
- Development of new or updated security policies, procedures and training for staff members within school corporations, i.e. to avoid sending confidential (employees or student) data through unauthorized/untrusted mechanism. To create new or enhance outdated requirements for the use of school technology assets.
- Centralized patch management for operative systems, in order to reduce outgoing network traffic.
- Reduce the cost of multiple server purchases by consolidating hardware and the use of Virtual servers. There are currently several providers for such solutions and various requirements that fit each specific need; the best solution with the best possible price creates an opportunity to update existing solutions.

- Virtualization also represents not only a benefit for the server side, but also it could be a benefit for the end user by the deployment of virtual desktops, allowing the delay of computer renewals while still delivering the latest operating system, updated patched OS, complete office suite, secure access to data storage, and the avoidance of externally storage of school data. Some school corporations even provide virtual desktops to their students from any location with Internet Access.

Physical Security

- Enhancement of surveillance solutions, in some cases to provide secure external access for law enforcement, in the event of a threat scenario inside school property.
- Access to discounted prices for the enhancement or implementation of secure solution for the protection of servers (centralized or distributed) of schools corporations. From solutions for Fire and water damage, as well as sustainable and independent access to power supply.
- Access to tracing software for missing or stolen equipment (laptops), in order to recuperate assets and to identify culprits (inside/outside the organization)

Hardware

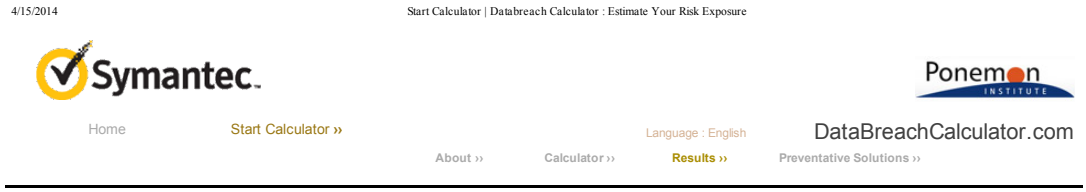
- Access to further discounted pricing for network equipment, support and warranty services. Offering the options of lease and/or purchases.
- Access to (local/remote) consultants (when needed) for configurations and administration services of managed firewalls, gateways, switches.
- Capacity to access to better purchasing channels for the acquisition of new equipment (desktops, laptops, mobile devices, etcetera) at any time during the year, thanks to the agreements made by INCSC with manufactures. Allowing

school corporations to reduce the period of renewal cycle due to budget constraints.

Benefits for State

- Schools corporations, in their majority, are funded by local taxes revenues distributed by the state. A leakage of personal data, network failure, denial of service, etcetera, would more likely represent an expense to the state government in the future, since it would have to supplement financial support to repair/restore capabilities damaged by created cyber-incident. A better-prepared school corporation would represent a less likely target/victim of such events. (Determine a probabilistic approach to DDoS, Virus infection, data breach, etcetera)
- For the state government, it would help deter and resist attacks by keeping important information and capabilities out of terrorist and enemy nation's hands, protecting vital private and public information out of the wrong hands.

Appendix H: Data Breach Calculator

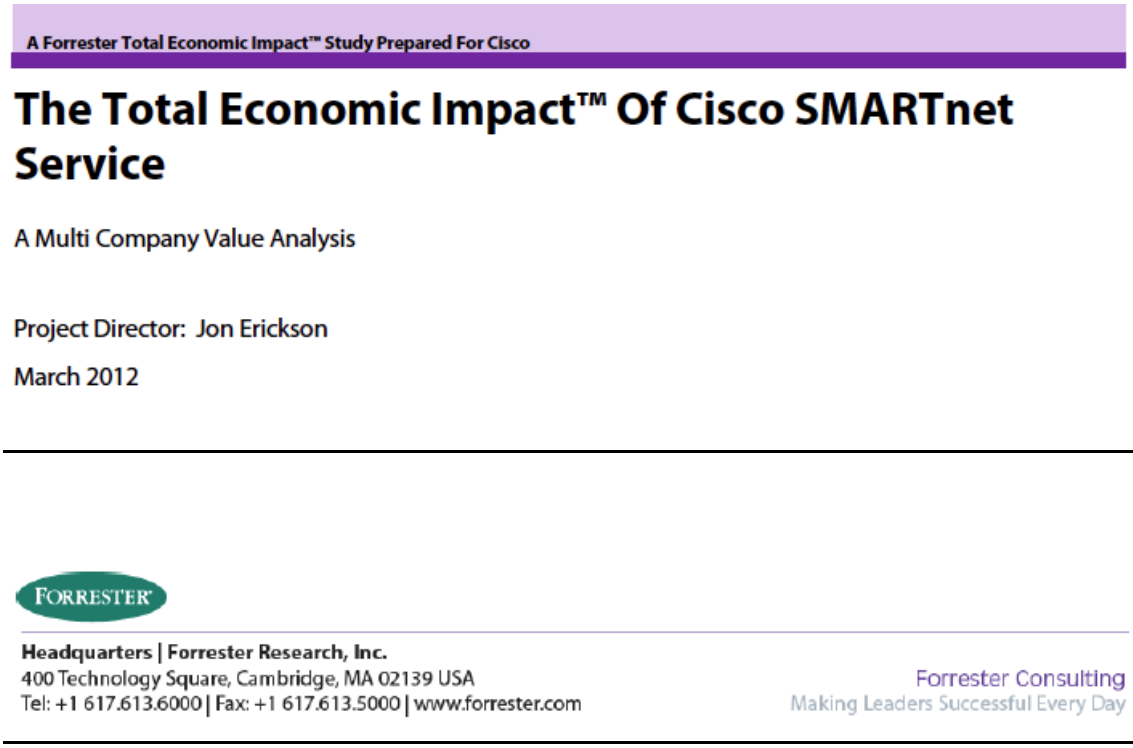


Results

Based on your inputs and our trend data, your risk exposure is:

- Companies in your industry with your risk profile have a likelihood of experiencing a data breach in the next 12 months of **9.7%**
- Your average cost per record is **$ 196**
- Your average cost per breach is **$ 588,667**

Appendix I: Economic Impact of Cisco SMARTnet – Forrester Research.



A Forrester Total Economic Impact™ Study Prepared For Cisco

The Total Economic Impact™ Of Cisco SMARTnet Service

A Multi Company Value Analysis

Project Director: Jon Erickson

March 2012

FORRESTER®

Headquarters | Forrester Research, Inc.
400 Technology Square, Cambridge, MA 02139 USA
Tel: +1 617.613.6000 | Fax: +1 617.613.5000 | www.forrester.com

Forrester Consulting
Making Leaders Successful Every Day

Resource retrieved from:

http://www.cisco.com/en/US/services/ps2827/ps2978/services_cisco_smartnet_tei_study.pdf

Appendix J: Compliance Model to determinate DB cost

Retrieved from http://clearwatercompliance.com/on-demand-webinars/how-to-calculate-the-cost-of-a-data-breach-and-how-to-get-the-budget-for-your-hipaa-hitech-compliance-program/

This model is not a boilerplate spreadsheet that can be used universally. Organizations will need to identify their own cost categories and customized spreadsheet depending upon their situation.

Annual Revenues	**$ 250,000,000**	high	medium	low	
# of records breached	**10,000**	25,000	10,000	5,000	
Reputational Repercussions					
Loss of Revenues and related Margin					
a Loss of Current Revenues:		high	medium	low	
Annual Revenues	$250,000,000				
Patient or member churn due to reputational harm	6.0%	10.0%	6.0%	4.2%	
Loss of Current Revenues	$ 15,000,000				
b Loss of New Revenues:					
Forecast $ of new revenues next year	$15,000,000	$50,000,000	$ 15,000,000	$ 8,000,000	
% new revenue loss due to negative publicity	10.0%	15.0%	10.0%	5.0%	
Loss of Forecast New Revenues	$ 1,500,000				
c Loss of Revenues from Strategic Partners:					
Forecast $ of new revenues next year	$3,000,000	$ 8,000,000	$ 3,000,000	$ 1,000,000	
% new revenue loss due to negative publicity	6.0%	10.0%	6.0%	4.2%	
Loss of Revenues from Strategic Partners	$ 180,000				
d Total Estimated Loss of Annual Revenues	$ 16,680,000				
% Variable Margin associated with Revenues	5.0%	7.0%	5.0%	3.0%	
Total Estimated Loss of Margin due to Revenue Loss	$ 834,000				
Cost of Replacing Staff Leaving due to Reputational Damage:					
# of Staff Leaving	2	3	2	1	
Average Cost-Per-Hire (advertising, travel, relocation and recruiter costs)	$ 4,285	$ 5,582	$ 4,285	$ 3,079	
Cost of Replacing Staff	$ 8,570				
# of Days Lost Margin due to New Staff Search and Training	43	57	43	29	
Average Gross Margin per Staff per Day	$ 500	$750	$500	$250	
Lost of Gross Margin due to New Staff Search	$ 21,500				
Total Estimated Cost or Margin due to Loss of Staff	$ 30,070				
Total Reputation Repercussions	$ 864,070				
	0.35%	of Annual Revenues			
Financial Repercussions					
Cost of Remediation		high	medium	low	
a Detection/Escalation Cost: (forensic-investigation-assessment-audit-crisis management)					
# of records breached	10,000				
Detection/Escalation Cost per record	$ 15.11	$ 18.13	$ 15.11	$ 12.09	
Cost of Detection/Escalation	$ 151,100				
b1 Credit and Identity Theft Monitoring					
# of records breached	10,000				
Cost of ID Theft and Credit Monitoring per month	$ 11.25	$ 15.00	$ 11.25	$ 10.00	
# of Months Provided	12	24	12	6	
% of victims taking advantage of Id Theft and Credit Monitoring	20%	25%	20%	15%	
Cost of Credit & ID Theft Monitoring	$ 270,000				
b2 Cost of Identity Theft					
# of records breached	10,000				
% of Records Exploited	25%	30%	25%	20%	
# of Victims	2,500				
Average cost per victim	$ 500	$ 1,000	$ 500	$ 250	
Total Cost of Identity Theft	$ -				
c Cost of Mitigation/Remediation (internally determined)					
(1) Cost of Encryption					
# of laptops to be encrypted	50	100	50	5	

	cost/month/laptop	$	155	$	15.00	$	12.95	$ 10.00
	Cost of Encrypting Laptops	$	7,770					
(2)	Cost of replacing lost or stolen asset	$	10,000	$	20,000	$	10,000	$ 5,000
(3)	Cost of Workforce Retraining							
	Number of Staff Requiring Retraining		50		100		50	25
	Required # Hours for Training		1.00		1.25		1.00	0.50
	Average Hourly Pay per Trainee	$	50	$	65.00	$	50.00	$ 37.50
	Cost of Workforce Retraining	$	2,500					
	Total Cost of Mitigation (internally determined)	$	20,270					
d	Cost of Lost Productivity							
	# of Records Breached		10,000					
	Cost of Loss Productivity due to a Breach	$	30.00	$	45.00	$	30.00	$ 15.00
	Total Cost of Lost Productivity	$	300,000					
	Total Cost of Remediation	$	741,370					
	Cost of Notification				high		medium	low
	# of records breached		10,000					
a	Customer Notification (certified mail)							
	per record cost of notification	$	13.90	$	15.26	$	13.90	$ 10.18
	per record cost of call center support	$	9.00	$	10.80	$	9.00	$ 7.20
	Total Notification Cost to Affected Individuals	$	229,000					
b	Notification to Media							
	per record cost of Crisis Management Consulting	$	5.04	$	6.05	$	5.04	$ 4.03
	per record cost of Media Management	$	1.00	$	1.20	$	1.00	$ 0.80
	Total NotificationCosts to Media	$	60,360					
c	Attorney Fees							
	per record cost of Attorney's Fees	$	7.00	$	8.40	$	7.00	$ 56.00
	Total Attorney Fees	$	69,960					
	Total Cost of Notification	$	359,320					
	Cost of Cyber Liability Insurance (new policy or deductible)							
a	Premium	$	200,000	$	225,000	$	200,000	$ 175,000
b	Broker Fees	$	25,000		15%		12.5%	10%
	Total Cost of Cyber Liability Insurance (if new)	$	225,000					
	OR							
	Cyber Liability Insurance Deductible	$	375,000	$	500,000	$	375,000	$ 250,000
	Deductible of Cost of Notification	$	-	company specific to coverage if carrying cyber liability i				
	Cost of Changing Business Associate (if applicable)							
a	Cost of Time on RFP and Due Diligence on New Vendor	$	-	as applicable, company specific				
b	Cost of Transition to new BA							
	# of months of transition		-					
	Duplicated Cost per Month		-					
	Duplicate Cost during Transition to New Vendor	$	-					
c	Incremental Higher Annual Cost of New Vendor	$	-					
	Total Cost of Changing Business Associate	$	-					
	Total Financial Repercussions	$	1,325,690					
			0.53%	of Annual Revenues				
	Legal & Regulatory Repercussions							
	Cost of OCR Fines, Penalties and CAP costs							
a1	Civil Monetary Penalty			willful neglect		willful neglect		reasonable
	# of Breached Records		10,000	uncorrected		corrected		cause
	Civil monetary penalty	$	-	$	1,500,000	$	250,000	$ 100,000
	OR							
a2	Settlement with OCR	$	1,000,000	$	1,500,000	$	1,000,000	$ 500,000
b	Cost of OCR Corrective Action Plan							
	(1) Develop and document updated/new Policies & Procedures	$	15,000	$	20,000	$	15,000	$ 10,000

(2) Develop updated training for workforce	$ 10,000	$ 15,000	$ 10,000	$ 8,000
(3) Implement New Procedures and Train Workforce				
% of hour required for training	50%	100%	50%	25%
Average Hourly Wage	$ 40	##	$ 40	$ 20
# of Workforce Members requiring Training	1,500	####	1,500	1,000
Cost of Training Workforce (loss of productivity)	$ 30,000			
(4) # of new Staff Hired as needed to comply with Corrective Action Plan	3	5	3	1
Average Salary + Benefits per New Hire	$ 96,010	$ 118,640	$ 96,010	$ 65,000
Cost of Hire	$ 5,582	$ 11,864	$ 5,582	$ 2,302
Cost of New Hires	$ 304,776			
(5) Implement New Safeguards	$ 50,000	$ 100,000	$ 50,000	$ 25,000
(6) Conduct a Risk Analysis	$ 50,000	$ 80,000	$ 50,000	$ 30,000
(7) Hire Independent Monitor and Annual reports on progress	$ 100,000	$ 125,000	$ 100,000	$ 75,000
Total Cost of OCR Corrective Action Plan	$ 549,776			
Total OCR Fines, Penalties and CAP costs	$ 1,549,776			
State Fines and Penalties				
a Penalty				
# of Breached Records	10,000			
Total State Penalties (Maximum assumed)	$ 100,000	$ 250,000	$ 100,000	$ 50,000
b Fine	$ 500,000	$ 1,000,000	$ 500,000	$ 250,000
c Cost of State Corrective Action Plan (additional reporting requirements)	$ 25,000	$ 50,000	$ 25,000	$ 10,000
Total State Fines & Penalties	$ 625,000			
Class-Action Lawsuit				
a Settlement Costs				
# of Breached Records				
Fine per Breached Record		$ 2,500	$ 1,000	$ 500
Settlement Costs				
% Covered by Insurance		80%	90%	100%
Total Settlement Costs to Company	$ -			
b Insurance Deductible		$ 500,000	$ 300,000	$ 100,000
c % of Settlement Paid for Legal Support	10%	15%	10%	8%
Legal Costs	$ -			
Total Lawsuit Costs	$ -			
Total Legal and Regulatory Repercussions	$ 2,174,776			
	0.87%	% of Annual Revenues		
Operational Repercussions				
Cost of Hiring Additional Staff (not included in CAP)				
a Additional Staff needed to Improved Security/Privacy (not included in CAP)				
Number of Staff Needed	5	10	5	2
Average Annual Salary + Benefits per New Staff Member	$ 75,000	$ 90,000	$ 75,000	$ 60,000
Incremental Cost of New Hires	$ 375,000			
b Cost of Recruiting and Training new Hires				
Average Cost of Recruiting and Training per New Staff Member	$ 7,500	$ 10,000	$ 7,500	$ 5,000
Total Cost of Recruiting & Training New Hires	$ 37,500			
Total Cost of Hiring Additional Staff (not included in CAP or mitigation plan)	$ 412,500			
Cost of Reorganization	$ -			
Total Operational Repercussions	$ 412,500			
	0.17%	% of Annual Revenues		
Total Impact of Data Breach	**$ 4,777,036**			
	1.9%	% of revenue		
	$478	average cost/record		

Appendix K: Data Breach insurance questioner "

ACE Privacy Protection®
Privacy & Network Liability Insurance Program
Application

NOTICE

The Policy for which you are applying is written on a claims made and reported basis. Only claims first made against the Insured and reported to the Insurer during the Policy Period or Extended Reporting Period, if applicable, are covered subject to the Policy Provisions. The Limits of Liability stated in the Policy are reduced, and may be exhausted, by Claims Expenses. Claims Expenses are also applied against your Retention, if any. If you have any questions about coverage, please discuss them with your insurance agent.

INSTRUCTIONS

Completion of this application may require input from your organization's risk management, information technology, finance, and legal departments. Additional space may be needed to provide complete answers.

Please type or print answers clearly.
Answer **ALL** questions completely, leaving no blanks. If any questions, or part thereof, do not apply, print "N/A" in the space.
Provide any supporting information on a separate sheet using your letterhead and reference the applicable question number.
Check Yes or No answers
This form must be dated and signed by the CEO, CFO, President, Risk Manager, or General Counsel of your company.

Underwriters will rely on all statements made in this application.

PLEASE ANSWER ALL QUESTIONS APPLICABLE TO COVERAGE FOR WHICH YOU ARE APPLYING.

All applicants must complete sections **I – IV** and **VII** of this application.

If coverage extension **D**, Electronic Media Liability, is required, please also complete section **V**, Internet Media Activities, which should be completed with the assistance of the applicant's legal department.

ADDITIONAL INFORMATION REQUIRED

Please submit the following documentation with the application:

1. Most recent annual report or 10K.
2. List of all material litigation threatened or pending (including plaintiff, cause of action and potential damages detail), which could potentially affect the coverage for which applicant is applying.
3. Loss runs for the last five years.
4. Copy of the privacy policy(ies) currently in use.
5. Executive summary of most recent network security assessment and/or PCI DSS audit, self-assessment, and/or scan.

Link to original 13-page document:

http://www.acegroup.com/us-en/businesses/ace-privacy-protection-privacy-network-liability.aspx

Appendix L: Tech Plan – IDoE Sponsored IT Budget (example)

CERTIFICATION OF SCHOOL TECHNOLOGY PLAN

IMAGINING the possibilities MAKING THEM HAPPEN

Indiana Department of Education

PRESENTED TO

[redacted]

7/1/2013 - 6/30/2016

The above referenced school corporation's technology plan is hereby certified for purposes of participation in the Universal Service Fund (USF) discount program. This means that the technology plan meets or exceeds the requirements set forth by the Schools and Libraries Division of the Universal Services Administrative Company (USAC).* The plan includes:

- Clear goals and a realistic strategy for using telecommunications and information technology to improve education;
- A professional development strategy that ensures staff know how to use the technologies to improve education;
- An assessment of the telecommunications services, hardware, software, and other services that will be needed to implement the strategy;
- Provisions for sufficient budget to acquire and maintain the hardware, software, professional development, and other services needed to implement the strategy; and
- Evaluation processes designed to monitor progress toward the specified goals and that allow mid-course corrections in response to developments and opportunities.

Joshua Towns

Joshua Towns, Director of Information Technology

May 17, 2013

SEAL OF THE STATE OF INDIANA 1816