DATA BACKUP SECURITY: BEST PRACTICES FOR K-12 INTERNATIONAL SCHOOLS IN SOUTH KOREA

A capstone project submitted

by

MONICA L. OTENG-BOATENG

to

DR. RAY KLUMP

(INFORMATION SECURITY PRACTICUM)

68-595K – SP11

in partial fulfillment of
the requirement for the
degree of

MASTER OF SCIENCE
in
INFORMATION SECURITY

LEWIS UNIVERSITY

May 3, 2011

Abstract

The benefits of data backup security for small business and organizations including schools are well established. In light of the fact that there are no known studies examining data backup security for K-12 international schools in South Korea, this study was an initial exploratory effort aimed at investigating the extent to which sensitive school data are committed to technology-based storage systems, how records are categorized regarding the need for security, and how existing systems are protected.

There were three investigative questions that shaped the foundation for the study:

1. To what extent do K-12 international schools in South Korea engage in technology-based applications to protect sensitive school data?
2. How are school records categorized regarding the need for secure storage?
3. How are existing backup systems protected?

The results of the findings showed a lack of secure systems, a lack of administrative level support, a lack of sufficient funding, a lack of data backup security policies and a lack of training in data backup security. Thus data collected from participants reflect the critical need to improve the overall security of backup systems in international schools in South Korea. However, the result must be interpreted with some caution due to the small number of participants (N=13).

While this study was a limited, exploratory effort, the investigation of data backup security practices in K-12 international schools yielded important patterns to be explored in future research.

This work is dedicated to my husband, Prince Charles, without whose immense support, I could not finish the MSIS program. I am truly blessed to married to this man whose valuable contribution to my life cannot be measured in anyway. Also to my wonderful children, Josiah, Josianne and Joelle for their patience in literally putting their short lives on hold just waiting for mom to graduate. I thank God for the inner strength to endure when the going got tough. Indeed, his strength is made perfect in our weakness. May the Lord receive all the glory that is due to Him alone.

CONTENTS

Abstract ii

Table of Figures vii

List of Tables viii

SECTION I INTRODUCTION 1

Background of the Study 2

Technology in the Learning Process 6

Protecting Data in Schools 7

Purpose of the Study 8

Research Questions 10

Definition of Terms 10

SECTION 2 LITERATURE REVIEW 12

Documentation 12

The Need for Data Backup 13

Classification and Sensitivity of School Data 14

Data Classification 16

Secure Management and Encryption of Data 18

Use of Back Strategies 19

Backup Tape Rotation Methods 21

Grandfather - Father - Son (GFS) 22

Tower of Hanoi 23

Types of Backups 23

Pitfalls to Avoid in a Tape Backup System 25

Steps to Implement a Tape Backup System 26

Remote and Cloud Data Backup 27

Considerations for Cloud Backup 27
Summary....32
SECTION 3 METHODOLOGY....33
Research Design 34
Appropriateness of the Research Design....34
Validity and Reliability 35
Internal Validity 36
External Validity....36
Research Questions 37
Pilot Study 37
Setting and Participants 38
Instrumentation....38
Data Collection....39
Data Analysis....40
Summary....40
SECTION 4 RESULTS 42
Findings 43
Analysis of Research Question 1....45
Analysis of Research Question 2....48
Analysis of Research Question 3....50
Summary....62
Conclusion....63
SECTION 5 DISCUSSION....64
Overview of Research Questions and Findings in the....65
Research Question 1: Applications for Backup Security....65

Research Question 2: Categorization of Records and the Security of Backup Data 66

Research Question 3: Protection of Backup Systems 68

Implications of the Findings 72

Data Backup Security Policies 72

Funding 77

Secure Data Categorization 77

Information Security 80

Physical Security 87

Legal and Ethical Issues 88

Support and Improvement 89

Methodological Issues and Limitations 93

Directions for Future Research 93

Risk Assessment 93

Measurement Issues 94

Security Policies 94

Data Protection Contractual Language 94

Summary and Conclusions 95

References 96

Appendix A Letter of Invitation and Consent Form 103

Appendix B Quantitative Survey 106

Table of Figures

Figure 1: Size of student population.....42

Figure 2: Backup applications used by schools.....43

Figure 3: Existence of data protection policies.....44

Figure 4: Percentage of IT budget for data protection and backup.....44

Figure 5: Importance of data backup.....45

Figure 6: Classification of school records.....46

Figure 7: Mode of data storage.....47

Figure 8: Security measures for data backup protection.....48

Figure 9: General security of facilities.....48

Figure 10: Security of backup systems.....49

Figure 11: Measures for protecting data from access by students and staff.....50

Figure 12: Security of shared data between divisions.....51

Figure 13: Importance of information security.....51

Figure 14: Maintenance of systems and networks.....52

Figure 15: Change of credentials for privileged accounts after personnel termination.....53

Figure 16: Challenges to security of backup systems.....54

Figure 17: Legal issues of backup security.....55

Figure 18: Familiarity with data protection laws in South Korea.....56

Figure 19: Compliance with data protection laws.....57

Figure 20: Support from school administration for data security.....58

Figure 21: Ways to improve security of backup systems.....59

List of Tables

Table 1: Sensitivity and Protection Levels……..15

Table 2: Data Classification……16

Table 3: Backup Strategies……..19

Table 4: Tape Rotation System……21

Table 5: Grandfather – Father- Son Tape Rotation System…….22

Table 6: Range of History Backup……...23

Table 7: Types of Backups……...24

Table 8: New Amazon EC2 Reserved Instances Pricing……..29

Table 9: Demographic Information of International Schools……...43

Table 10: Guidelines for Risk Assessment…….…..73

Table 11: Training Outline…….…..91

SECTION I

INTRODUCTION

Data loss is an inescapable reality in the modern business world (Data, 2007). The costs associated with the loss of data makes data backup security an important issue of consideration for businesses and organizations including K-12 schools. For K-12 schools, the rapid development and use of technology in the classroom has not necessarily resulted in the growth and understanding of the management of school data. A recent study (Data, 2007) reported the "precarious position" of small business backups: 30% lack formal data backup and storage procedures, 39% review storage procedures only after a problem occurs, 34% admit to only fair or poor performance in storing backup data offsite, 17% don't consistently perform incremental data backups, and 55% rate their prevailing disaster recovery plan as fair or poor. The disaster recovery study (Data, 2007) revealed nearly half the companies that are unable to fully restore their data after a disaster will go out of business.

The proposed qualitative study was focused on exploring data backup security practices for K-12 schools in South Korea. Procedures examined how K-12 schools (a) protect data, specifically related to backup strategies, (b) provide protection from physical damage and other attacks, (c) establish an appropriate disaster recovery, and (d) provide plans and recommendations for best practices. Information from literature was gathered with which to support the proposed study. As well, a preliminary qualitative investigation was conducted into the premise that small and medium size businesses and K-12 schools do not implement adequate backup strategies or the need for privacy and security for school data. Additionally, literature about how the security of data and

technology in education facilitates the process of teaching and learning, both for teachers and students, was explored and their implications identified.

Background of the Study

The lack of adequate data protection was evidenced by a survey conducted by *eWeek* that concluded half of small business professionals are inclined to rely on insecure methods to store information, such as CDs, DVDs and USB thumb drives (Wilson, 2010). Lack of data protection could put data important to the conduct of business in jeopardy when no adequate disaster recovery system is in place in the event of data loss. Lenovo-AMD Small Business Tech Survey indicated that, "many small businesses are backing up critical data using disposable, insecure methods. While 40% of small businesses back up files to external hard drives, 50% of respondents said they or their company use USB thumb drives and CDs/DVDs to backup important information. Secure cloud-based storage is rarely used" (Wilson, 2010). Forrester Research surveyed 1,272 businesses, of which only 16% of responding organizations used online backup. The Forrester Research survey also found 10% of respondents were planning to use a backup, but had not as yet taken action (Data, 2007). The intention to create an online backup of data, but failure to act on the intention, was noted among small business IT professionals (including K-12 schools), as well as larger businesses. This unfortunate situation was further confirmed by TechRepublc (2011), which, concluded, that "the loss of critical data can be crippling to any business; still many small and mid-size companies do not adequately back up their data" (Republic, 2011). Lack of data protection could put data

important to the conduct of business in jeopardy when no adequate disaster recovery system is in place in the event of data loss.

An independent study conducted by Rubicon (2008) also observed the pitfalls of poorly implemented backup strategies and the real world consequences of unexpected data loss. Results of the study indicated that although small and medium-sized businesses worry about losing data, their backup practices might not be sufficient. "The survey showed a high level of concern about potential data loss. Companies rated backup as their #2 computing priority, after defense against viruses and other malware, and ahead of issues like reducing costs and deploying new computers" (Rubicon, 2008). The authors (anon.) contended, "Although most companies do some form of backup, the backup practices they have chosen leave holes in their coverage" (Rubicon, 2008). Many small and medium-sized businesses rely on manual backup practices that can be forgotten by employees, or even subverted if an employee is disgruntled. In addition, companies may store their backup files in the same location as the computer that was backed up, making them vulnerable to loss through natural disasters or theft (Rubicon, 2008).

The key findings in the Rubicon (2008) study regarded the impact of data loss on small businesses, and computer backup practices. In sum, the findings indicated that:

- Half of SMBs have lost important business data from their computers.
- A third of the companies that lost data suffered lost sales as a result and 20% have lost customers.
- Although hardware failure is the most common cause of data loss, midsize

companies lose data in many different ways, some of them surprising. For example, a quarter of the midsize companies that lost data said they have had incidents in which an employee erased it maliciously.

- About a quarter of SMBs do not back up their servers or PCs.
- Most SMBs are vulnerable to some forms of data loss from their PCs and servers because they store backup files in the same location as the computers backed up.

SpectrumData (Data, 2010) cited the 10 common causes linked to the loss of data.

- Hard disk drive failure
- Component failure (a telltale sign of this is strange noises such as clicking and buzzing emanating from the device).
- Electrical failure such as drive not spinning or starting up
- Accidental or intentional reformatting or overwriting of disks and partitions
- Corrupt or missing critical file system structures and files
- Inaccessible drive partitions
- Media surface contamination
- Accidental or intentional deletion of data
- Virus or worm contamination including adware, spyware, boot sector and file infecting viruses.
- Application or operating system crash or boot problems
- Damage due to power failure or power surge, lightning strikes

- Damage due to water and liquids including floods, rain and accidental spillage
- Damage due to smoke or fire,
- Failure due to wear/tear and age of drive

The lack of adequate backup strategies for security may be addressed through online or cloud backup as a form of alternative backup solution for critical data. Malone of IDG's Custom Solutions Group suggested that some of the key drivers behind cloud computing are regulation, compliance, security, business continuity and disaster recovery of critical data (TechRepublic, 2011). While online or cloud backup has its own security issues, it is a standard recommended industry practice to have backups stored in different locations, including the cloud. However, the risks of online backup must be fully explored before engaging in the practice. Strom (2007) contended in *Online Backup: Worth the Risk?* that "The problem of managing a gigantic amount of data has, in some instances, been compounded by current trends in information technology" (IT).

Strom (2007) raised his concerns with regards to the security risks of cloud backup by suggesting that "This is the promise of online backup services – to automatically backup everything (or everything that is selected) to a secure offsite location. However, is that really a good idea? Are there any issues that should be considered when evaluating whether or not to use automatic online backup? What regulatory frameworks need to be considered if an organization chooses to use an online backup provider? And how does this impact the responsibility to manage corporate data?" Furthermore, TechTarget (2011), concludes that when considering using a cloud storage provider for backing up data, it is critical to first analyze factors such as the

amount of data that must be protected, the amount of available internet bandwidth, and the amount of data that changes on a regular basis. After consideration of the appropriate amount of data to be protected, as well as the available bandwidth, cloud backup may be a viable option for small and medium-sized organizations, which may facilitate the recovery process in the event of a disaster (TechTarget, 2011). This would include K-12 schools.

Technology in the Learning Process

The integration of technology into the learning process has become a priority for many schools. Knezek, the CEO of the International Society for Technology in Education (ISTE) emphasized the importance of technology in education when he asserted "Education without technology compares to the medical profession without technology" (ISTE, 2010). The rapid growth in technology in education is helping teachers to expand beyond linear, text-based learning and to engage students who learn best in a variety of ways (Kessier, 2010). The role of technology in schools has evolved from a contained "computer class" into a versatile learning tool that can change how educators demonstrate concepts, assign projects, and assess progress, such as SmartBoards (Kessier, 2010).

Computer-assisted instruction has been described several ways in the literature (Robyler & Doering, 2009). Robyler and Doering described computer-assisted instruction as the use of a computer to provide course content in the form of drill, practice, tutorial, and simulations. Mahmood (2004) defined computer-assisted instruction as a process by which visual information is presented in a logical sequence to the learner with a computer. The student learns through reading the text presented, or by

observing the information displayed. All the definitions of computer-assisted instruction concur that the computer plays the role of tutor and provides instruction through different modes (Mahmood, 2004; Robyler & Doering, 2009). Computers have also been integrated into the storage and use of all aspects of the educational community, which prompts a concern for protection of the data.

Protecting Data in Schools

Although technology in the classroom has benefits for students, the need for student and staff data to be protected must also be considered a primary application of technology in the educational environment (Gardner, 2000). In schools, technology has the power to make the entire educational process more efficient. Information about students, staff, courses, programs, facilities, and fiscal activities can be collected and maintained so schools can effectively coordinate services offered to students, measure learning progress, assign and monitor staff responsibilities and resource use, and provide other valued services for all stakeholders. Technology in businesses is used to modify the manner in which they operate; thus, its application in schools is an extension of the way administrators conduct the business of education (Gardner, 2000). While computers and networks contribute to the efficiency of educational record-keeping, data access, and use, they have not changed the reasons schools need to maintain, share, and use student and staff information.

The educational community has always required many types of information to carry out the mission to instruct students. Although it may be fitting to discuss analogies between paper files in wooden cabinets, and electronic files on hard drives or 3½-inch diskettes, there are significant differences in the specific processes required to maintain

appropriate security in the age of computer networking. With a flip of a switch, information can be damaged irreparably. With the careless turn of one's head, a pocket-sized disk or thumb drive containing thousands of records can disappear. With the connection of a single wire, sensitive material can be shared with millions of users.

While these scenarios may seem foreboding, they are a small part of the story, because by another keystroke or switch, properly storing disks, and connecting the right wires, information stored on school computers and networks can be secured more safely than any paper file in an office filing cabinet, whether locked by deadbolt or protected by an armed guard. The same technology that can be the source of so much concern when in the hands of untrained users can be used to protect information more securely than before the digital revolution if it is used wisely (National Center for Education Statistics, 2009). A preliminary search of the literature failed to reveal any empirical study of the security measures K-12 schools in Korea have implemented to protect data. This proposed study will fill that gap.

Purpose of the Study

Sensitive school information may require special precautions to protect it from unauthorized disclosure, accidental or intentional modification, destruction or denial of use. Assigning information to a sensitivity category helps to define the security measure that is appropriate for its protection. Categories of information that must be secured are the personal records of students and staff, financial data about the costs associated with operating the school, contracts concerning services, records of incidents of bullying or other problems between students, and operational paradigms.

The purpose of the proposed study is to determine the extent to which such

records are committed to technology-based storage systems, how records are categorized regarding the need for security, and how existing systems are protected. It is the general responsibility of school administrators, and the information technology department's sole responsibility to review electronic information with respect to the Public Records Act (Act, 2003), the Information Practices Act (1997), and other State or Federal statutory or regulatory requirements that may apply in determining the sensitivity category of records that are kept in the educational environment, as well as the security measures reasonable and prudent with respect to the protection of that information (Statistics, 1997). In Korea, Data Protection Laws such as Act on Protection of Personal Information Maintained by Public Agencies (1994), Use and Protection of Credit Information Act (1995), Act on Disclosure of Information by Public Agencies (1996), Act on Real Name Financial Transactions and Guarantee of Secrecy (1997) are in place to protect information. In 1999, the Act on Promotion of Information and Communications Network Utilization and Information Protection aka "the Information Protection Act" was enacted to provide guidelines for personal information protection in the private sector (Korea Law, 1999) which includes international schools in Korea. This Act, which went into effect in 2000, adopted eight principles recommended by the OECD Privacy Guidelines of 1980, including the principles of information protection, the rights of data subjects, the responsibilities of service providers, and possible remedies following personal information infringements. All organizations in the private sector in this country must abide by these laws, hence the need for international schools to know and adopt policies that align with these regulations.

Research Questions

Based on the preceding paragraphs, the primary research questions were:

1. To what extent do K-12 schools in Korea engage in technology-based applications to protect sensitive school data?
2. How are school records categorized regarding the need for secure storage?
3. How are existing security systems protected?

Results of the study were used to (a) identify the different types of data that need to be managed, (b) categorize the types of data by security priority, and link the category and priority to a specific security measure. Results of the proposed study may equip school data guardians with the information they require to employ best practices to safeguard school data through proper backup strategies and data recovery measures.

Definition of Terms

Data

Information that has been translated into a form (binary digital form) that is more convenient to move or process (TechTarget, 2009).

Backup

Making copies of data so that these additional copies may be used to restore the original after a data loss event (Mifflin, 2008).

Security (Information)

Information security means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide integrity, availability and confidentiality (Cornell University Law School: United

States Code, n.d.).

International School

A school that promotes international education, either by adopting an international curriculum such as that of the International Baccalaureate or the Cambridge International Education (CIE) or by following a national curriculum different from that of the country the school is located in (IASL, 2009).

SECTION 2

LITERATURE REVIEW

The purpose of the proposed study is to explore data backup security practices for K-12 schools in South Korea. This study is an effort to examine procedures with which K-12 schools (a) protect data, specifically related to backup strategies, (b) provide protection from physical damage and other attacks, (c) establish an appropriate disaster recovery, and (d) provide plans and recommendations for best practices. In this chapter, literature pertinent to data backup is discussed.

Documentation

Scholarly books, seminal journal articles, and research documents were reviewed through the University of California at Berkeley library and Lewis University library. Additional databases searched included Association of Computing Machinery (ACM) Digital Library, EBSCOhost, ProQuest Digital Dissertations, ATLA Religion Database with ATLASerials, Business Source Complete, Catholic Periodical and Literature Index, MLA Directory of Periodicals, Library Literature & Information Science (H.W. Wilson), Lexis Nexis, JStor, WilsonWeb, ArchiveGrid, Euromonitor International, and FAITS – Faulkner Information Services. The online databases of Google also provided information for the search of the pertinent literature. Bibliographic and reference listings were accessed from appropriate titles discovered within the review process. Approximately 120 current scholarly articles pertaining to backup systems, backup security strategies, crises management, data protection, computer security, data security, information security systems, backup security systems, electronic data processing, data

replication, data warehousing, school data protection, data protection procedures in education were reviewed.

The Need for Data Backup

As previously observed, the integration of technology into the learning process has become a priority for many schools. With the growth in storage, investment in education, the dependence on IT infrastructures for higher productivity, and competitive advantage, the need for data protection in schools is becoming critical for everyday operations, especially during major failures, and natural disasters. This highlights the need for data backup and restoration of operations based on optimal utilization of IT resources. Several companies and organizations today are considering various approaches for protecting their valuable data and mechanisms for quick recovery.

Factors affecting these infrastructure and policy decisions include cost of downtime, backup windows, time-to-recover, frequency of backups, maturity of technological options, and so forth. Such decisions typically result in a combination of online data replication (disk-to-disk) or offline (disk-to-tape) backups, and the implementation of policies required with these operations (Cisco Systems & Network Appliance, 2008).

A number of reasons demand adequate "data availability" (the ability to protect and recover valuable business data when needed) by organizations and companies. The key factor among them is the cost associated with downtime. This includes costs associated with lost productivity, reduced customer satisfaction, and the cost from lost revenues due to inability to access business-critical data. Accidental data deletions and data corruption by an application may lead to irrecoverable losses resulting in significant

effort and time expended to reconstruct the data. Reconstructing all business-critical data and rapidly recovering to full business operation can be extremely difficult, if not impossible. Such data recovery could take days, which could severely affect the functioning and viability of an enterprise. Far-sighted enterprises, including schools, could implement disaster recovery plans to guard against such potential calamity.

Classification and Sensitivity of School Data

Sensitive school information may require special precautions to protect it from unauthorized disclosure, accidental or unintentional modification, destruction or denial of use. Assigning sensitive school information to a sensitivity category helps to define the security measure that is appropriate for its protection. Also, written policies help schools classify data into directory information, transcript information, or supplemental information, and to determine how to maintain and release each piece of information. Each data element to be maintained about an individual student is classified as part of the directory information (subject to public release), a part of the transcript information (will be released in a student's transcript if he or she transfers to another district or applies to a postsecondary education institution), or is supplemental (all the other information collected), e.g., bus route and class schedule. Both confidential and public information can be categorized as sensitive information. Table 1 below refers to the four levels of sensitivity for educational records and the level of protection that is warranted for a specific file of information or data.

This standard (Cheung, Clements, & Pechman, 1997) applies when transmitting S4 and S3 classified information outside of the organization's secure network. Sensitivity categories have been established to insure adequate levels of protection for the

State's informational assets. Sensitivity categories also provide a convenient means of determining how the information is to be handled.

Table 1: *Sensitivity and Protection Levels*

Sensitivity Level	Level of Protection
S1	Information needed for the day-to-day operation of government. Information in this category should not contain data that can be related to the identity of an individual, result in a negative fiscal impact to the State, or adversely impact State's operations. Information typical of this category is accounting information, statistical information, procedures, policies, published regulations, operational directives, and others.
S2	Information which if disclosed, modified or destroyed may have an adverse impact on Department of Education's activities. Information typical of this category would be civil service examinations, scoring keys, or competitive bids, among others.
S3	Information which if disclosed, modified or destroyed would have a serious negative impact on the State operations. Included in this category would be financial or investment information
S4	Information that if accidentally or intentionally disclosed, modified, or destroyed would constitute an invasion of privacy or result in harm to the individual. Information typical of this category may consist of medical, financial, welfare information, or records pertaining to pending litigation. This category also would include operational information or data, such as personal identification numbers, codes, or passwords. The security measure for the transmission of S4 classified information requires encryption such that: • All manipulations or transmissions of data during the exchange are secure. • If intercepted during transmission the data cannot be deciphered. • When necessary, confirmation is received when the intended recipient receives the data. • Agencies must use industry standard algorithms, or cryptographic modules as validated by the section 6 guidelines of the Office of Information Technology-Security and Risk Management

To insure that the proper degree of protection is applied to information, all documents should display the sensitivity category. Categories of information that must be secured and backed up are the personal records of students and staff, financial data about the costs associated with operating the school, contracts concerning services, records of incidents of bullying or other problems between students, and operational paradigms. It is the general responsibility of school administrators, and the Information Technology (IT) department's sole responsibility to review electronic information with respect to the Public Records Act (Act, 2003), the Information Practices Act (Information Practices Act, 1997), and other State or Federal statutory or regulatory requirements that may apply in determining the sensitivity category of records that are kept in the educational environment, as well as the security measures reasonable and prudent with respect to the protection of that information (Statistics, 1997).

Data security components outlined in this section are designed to reduce the risk associated with the unauthorized access, disclosure, or destruction of school data.

Data Classification

Schools must classify data into categories based on the sensitivity of the data. School data classifications must translate to or include the following classification categories as shown in Table 2 below.

Table 2: *Data Classification*

Categories	Description
Category 1: Public Information	This is information that can be or currently is released to the public. It does not need protection from unauthorized disclosure, but does need integrity and availability protection controls.
Category 2: Sensitive Information	This is information that may not be

	specifically protected from disclosure by law and is for official use only. Sensitive information is generally not released to the public unless specifically requested.
Category 3: Confidential Information	This is information that is specifically protected from disclosure by law. It may include but is not limited to: (a) Personal information about individuals, regardless of how that information is obtained; (b) Information concerning student or staff personnel records; (c) Information regarding IT infrastructure and security of computer and telecommunications systems.
Category 4: Confidential Information Requiring Special Handling	This is information that is specifically protected from disclosure by law and for which especially strict handling requirements are dictated, such as by statutes, regulations, or agreements. Serious consequences could arise from unauthorized disclosure, such as threats to health and safety, or legal sanctions.

Security measures for Categories 1 and 2 are general data protection policies required for the protection of public information. As stated by the Information Security Board "when sharing Category 3 and above data outside the organization, an agreement must be in place unless otherwise prescribed by law. The agreement (such as a contract, a service level agreement, or a dedicated data sharing agreement) must address the following:

1. The data that will be shared.
2. The specific authority for sharing the data.
3. The classification of the data shared.
4. Access methods for the shared data.
5. Authorized users and operations permitted.

6. Protection of the data in transport and at rest.

7. Storage and disposal of data no longer required.

8. Backup requirements for the data if applicable.

9. Other applicable data handling requirements (ISB, 2009).

Secure Management and Encryption of Data

The storage of Category 3 and above information requires an organization to select and apply encryption, at the discretion of the school, after completing a school-wide IT Security Risk Assessment. Schools must use industry standard algorithms or cryptographic modules validated by the National Institute of Standards and Technology (NIST, n.d.). Although maintaining backups is a prudent undertaking, it is not enough. Schools must be proactive in ensuring not only that their backups are reliable and that they are secure from unintended uses or exposure. Research conducted on backup security strategies employed by K-12 international schools in Korea failed to identify any schools implementing any strategies.

Research by Center for Education and Research in Information Assurance and Security (CERIAS) indicates that in the State of Indiana and all across the U.S., there is a significant need across public and private sectors for educating and distributing information to the users and administrators of information systems. The public and private sectors, and particularly home users, are isolated from awareness and training opportunities in information security. CERIAS spokespersons contend that the solution to this problem begins by integrating information security topics into the K-12 curriculum and aligning it with state and national standards to help alleviate the shortage by increasing the skills of the entire future workforce. Additionally, CERIAS spokespersons

note that integrating security topics into the curriculum will also help address issues of online safety, critical literacy, and transfer of ethical behavior to the online environment as well as promote cross-curricular studies and real-world problem-solving (CERIAS, n.d.).

However, it was discovered that CERIAS (CERIAS, n.d.) offers a training program for school data guardians on the topics, such as, Introduction to Information Security, Risk Analysis, Legal Issues and Regulations, Creating & Auditing School Security Practices, Building an Awareness and Training Program, Intrusion Detection: An Overview. They do not proactively address the issue of backups in general and backup security in particular. Additionally, according Veeam (2010), many school divisions in Prairie South in Canada use a backup system known as server virtualization to reduce costs, leverage investments in high-capacity servers, and respond to user demands in a timelier manner. This is because they determined that "other solutions were slow, unreliable, and required large amounts of backup storage space" (Veeam, 2010).

Use of Back Strategies

Backup Strategies used by several organizations include tape backups. According to Backup Assist (2011), tape is an ideal medium for backing up data because of its high storage capacities, low cost, and the ability to store cartridges off-site. A number of different tape formats exist. Some common formats are shown in Table 3 below.

Table 3: *Backup Strategies*

Tape format	Data capacity (uncompressed)	Data transfer rate	Applications
Travan	1 - 20Gb	1Mb/sec	Home use, low range servers
DAT / DDS / 4mm (Digital Data Storage on Digital Audio Tape)	2 - 20Gb	2.75Mb/sec	Low range servers, small business
AIT (Advanced Intelligent Tape)	15 - 50Gb	3Mb/sec	Low to mid range servers
LTO (Linear Tape Open)	200 - 1600Gb	40-320Mb/sec	Mid to high range servers and mainframes

The average small business and organization will find that a Travan or 4mm DDS tape will provide an appropriate solution in terms of data capacity and cost. All data will generally fit onto a single tape, meaning that a single stand-alone tape drive can be purchased (instead of more expensive options such as tape autoloaders, and others). Backups should ideally take place outside of business hours, when network traffic is at its minimum. Scheduling the backup at some time during the night (e.g. Midnight) is a suitable tactic for most organizations. Backing up data once a day (after each working day) provides good coverage against data disaster.

Backup Tape Rotation Methods

The backup tape rotation methods can be implemented manually or in software. When software is used, it assists organizations in managing and scheduling backups to provide an easy way of implementing a backup rotation, for example, in a tape rotation strategy easily. In a tape rotation system, multiple tapes are organized into a tape backup pool, or tape backup library to provide you with data recovery capabilities, whilst allowing for selected backup tapes to be stored off-site for added security. Different tapes are used for different days' backups according to a predefined system. Three such tape rotation systems are described here. The simplest tape rotation scheme is to have one tape for each day of the working week. Tapes are labeled Monday, Tuesday, Wednesday, Thursday, and Friday, as shown in Table 4 below.

Table 4: *Tape Rotation System*

Monday	**Tuesday**	**Wednesday**	**Thursday**	**Friday**
	1 Tuesday	2 Wednesday	3 Thursday	4 Friday
7 **Monday**	8 Tuesday	9 Wednesday	10 Thursday	11 Friday
14 **Monday**	15 Tuesday	16 Wednesday	17 Thursday	18 Friday
21 **Monday**	22 Tuesday	23 Wednesday	24 Thursday	25 Friday
28 **Monday**	29 Tuesday	30 Wednesday		

One can restore data from any one of the tapes in the library, or in this case, any day in the past week. This strategy requires only five tapes, but only provides one week's data backup history.

Grandfather - Father - Son (GFS)

The grandfather - father - son schedule is the most widely used method, and involves backing up data in the following way:

daily - on the "son tapes"

weekly - on the "father tapes"

monthly - on the "grandfather tapes"

This system is far more powerful than the five tape rotation, but requires more tapes. For example, consider the calendar shown in Table 5 below.

Table 5: *Grandfather – Father- Son Tape Rotation System*

Monday	**Tuesday**	**Wednesday**	**Thursday**	**Friday**
	1 Tuesday	2 Wednesday	3 Thursday	4 Friday
7 **Month 1**	8 Tuesday	9 Wednesday	10 Thursday	11 Friday
14 **Week 2**	15 Tuesday	16 Wednesday	17 Thursday	18 Friday
21 **Week 3**	22 Tuesday	23 Wednesday	24 Thursday	25 Friday
28 **Week 4**	29 Tuesday	30 Wednesday		

This strategy provides the ability to restore data from the last week, plus any Monday over the last month, plus any month for as many monthly tapes as you have. Variations on this scheme are available, and provide a trade-off between the number of tapes required, and the number of monthly tapes available.

Tower of Hanoi

The Tower of Hanoi a complex strategy where five tapes are used - called A, B, C, D, E. A is used every other day, B is used every 4th day, C is used every 8th day, and D and E are used every 16th day, alternating. This ensures that data is available from the last day, 2 days ago, and three other times in history. However, the range of history of backup is dependent on where one is in the cycle as shown in Table 6 below.

Table 6: *Range of History Backup*

Monday	Tuesday	Wednesday	Thursday	Friday
	1 A	2 B	3 A	4 C
7 **A**	8 B	9 A	10 D	11 A
14 **B**	15 A	16 E	17 A	18 B
21 **A**	22 C	23 A	24 B	25 A
28 **D**	29 A	30 B		

This method is clearly confusing, but has the advantage of only requiring 5 tapes. Unless aided by software, this method is not recommended because it is prone to human error.

Types of Backups

Different types of backups are available in backup software. Each will back up different amounts of data, and different types of files as shown in Table 7 below.

Table 7: *Types of Backups*

Backup type	Files that are copied over to backup media
Full	All files, system data, etc.
Differential	All files added or changed since the last full backup
Incremental	All files added or changed since the last full, differential or incremental backup
Daily	All files added or changed on the day of the backup

A full backup will copy all files and system data to the backup media. It allows for the complete restore of all data from one single tape.

Differential, Incremental and Daily are partial backups and are designed to reduce amount of data backed-up to the media, resulting in faster backups. To restore data using one of these backups, the last full backup tape will also be required, along with any other partial backups since the last Full backup. For example, if full backups are performed on Mondays, and Incremental backups on the other days, to restore last Thursday's data, 4 tapes would be required (Monday full + Tuesday incremental + Wednesday incremental + Thursday incremental). The problem with partial backups is the requirement for multiple tapes when restoring data. If any of these tapes is faulty, then the restore cannot be guaranteed to proceed correctly. Clearly, if all your data can fit onto a single tape, performing full backups all the time is the safest strategy.

Pitfalls to Avoid in a Tape Backup System

There are several pitfalls that can reduce the effectiveness of any tape backup system:

1. Faulty media: If one runs the same tapes for years, eventually they will wear out. However, the backup software should be able to detect faulty tapes when it verifies the data written to the tape after each backup.

2. Human error: If one places the wrong tape in the tape drive for a backup, it will obviously disrupt the system. There are ways of minimizing human error, which includes using backup software, which will email the administrator/secretary daily, and instruct him/her to place a certain tape in the drive.

3. Insecure storage of tapes: It is critical that tapes are stored in a secure location such as a fireproof safe, and that monthly, quarterly and yearly tapes be stored off site. Please note that if you store all your backup tapes next to your file server, and your building gets robbed or burns down, not even the best tape backup library in the world will get your data back.

4. Test Your Backup: It is important to conduct tests on backups to ensure that these will work when needed for restoration purposes.

Steps to Implement a Tape Backup System

The fastest and most cost effective way of protecting data are described in the following steps.

Step 1: Select and purchase your backup hardware. The data of most small organizations will fit onto a single tape. Work out the amount of data that you need to back up, and select an appropriate tape drive according to these rough guidelines:

Up to 10 Gig Travan cartridge drive

Up to 20 Gig DDS tape backup drive

Up to 40 Gig DDS tape backup drive with hardware data compression

Then purchase the necessary tapes for your backup rotation strategy. A good Grandfather-Father-Child variation will require 10 tapes or 14 tapes.

Step 2: Implement tape backup processes using software. The next step is to select a tape rotation strategy, devise a calendar of tapes, and to set up your tape backup software to schedule tape backups at the end of the working day. This process is time consuming, but fortunately there is software available to simplify the process (BackupAssist, 2011).

Step 3: Continually perform backups. Backups must be done every working day to be effective.

In addition to the above, one should monitor the results of each backup to check for errors. For example, if a tape wears out and data cannot be verified, one needs to take action and replace that tape.

Remote and Cloud Data Backup

According to Search Security (n.d.), remote and Cloud Backup is becoming a popular alternative to portable media, such as tape. There are currently two popular approaches to cloud data backup: Software-as-a-Service (SaaS) and cloud storage services. As an alternative to on-premise software and secondary storage, backup SaaS is a Web-native application hosted and operated at a central location and accessed via a browser-based interface. It is typically characterized as having a multitenant architecture (i.e., a shared, scalable infrastructure that keeps data virtually separated) and a utility pricing model. Lightweight agents residing on the systems to be protected pass data at the primary site to the cloud. Examples include Fortiva's (Toolbox, 2010) email archiving service, Evernote (Schonfeld, 2011) and Dropbox (Deacon, 2011).

Cloud storage services are a hybrid of on- and off-premise components. For backup, the organization has on-premise control of software and, optionally, hardware, coupled with leveraging off-premise services or infrastructure (massive data centers housing powerful computer, network and storage resources). Cloud backup services are charged back to the customer on a consumption basis - based on capacity, bandwidth or seat.

Considerations for Cloud Backup

Every cloud has a silver lining, and in the case of cloud-based backup, there are several benefits (Search Security, n.d.). Both cloud backup technology approaches are convenient because the information can be accessed from any Internet-connected device; information can be more easily shared; it has built-in security; and digital information is easier to manage, search, retrieve and transfer. There may also be some cost and/or

budgeting advantages to outsourcing all or a piece of the backup storage. There are several advantages to using cloud backup (SearchDataBackup, n.d.) as follows:

1. Efficiency and Reliability

Cloud providers utilize state-of-the-art technology, such as disk-based backup, compression, encryption, data reduplication, server virtualization, storage virtualization, application-specific protection, and more in SAS 70-certified data centers. In addition to the security that accompanies their certification, many providers offer 24/7 monitoring management and reporting -- features and capabilities that may not be afforded by many companies. Furthermore, there's no need to worry about upgrades, migrations or technology obsolescence; the burden of the backup infrastructure lies with the service provider.

2. Scalability with Capital Savings

Organizations can leverage the unlimited scalability of a third-party cloud provider without the upfront capital expenditure. In fact, the pay-as-you-go model significantly reduces the procurement and provisioning headaches for backup. This approach allows for predictable management of capacity growth and operational costs. Table 8 below shows a typical example of such costs using New Amazon EC2 Reserved Instances Pricing (HinchCliffe, 2009).

Table 8: *New Amazon EC2 Reserved Instances Pricing**

One Year Term

Instance Type	Instance Price	Hourly Charge	Effective Hourly Rate
M1.xlarge	$1820.00	$0.24	$0.448
M1.large	$910.00	$0.12	$0.224
M1.small	$227.50	$0.03	$0.056
C1.xlarge	$1820.00	$0.24	$0.448
C1.medium	$455.00	$0.06	$0.112

*These rates are as of August 2009

Amazon Elastic Compute Cloud (EC2) provides flexibility to choose from a number of different instance types to meet specific computing needs. Each instance provides a predictable amount of dedicated compute capacity and is charged per instance-hour consumed. The table above describes the instance type and the associated charges (Amazon, 2011).

In addition to Elastic Compute Cloud (EC2), Amazon also operates the Elastic Block Store (EBS) as a regular cloud backup storage system. In this system, volume storage is charged by the amount you allocate until you release it, and is priced at a rate of $0.10 per allocated GB per month. Amazon EBS also charges $0.10 per 1 million I/O requests made to a volume. Programs like IOSTAT can be used to measure the exact I/O usage of a system at any time. However, applications and operating systems often do different levels of caching, therefore it is possible to see a lower number of I/O requests on a bill than is seen by an application unless the I/Os are synced to disk (Amazon, 2010). For example, a medium sized website database might be 100 GB in size and expect to average 100 I/Os per second over the course of a month. This would translate to $10 per month in storage costs (100 GB x $0.10/month), and approximately $26 per

month in request costs (2.6 million seconds/month x 100 I/O per second * $0.10 per million I/O) (Amazon, 2010).

3. Improvement in Recovery Time for Small Data Sets

For a recovery from tape, an operator would need to recall the tape, load it, locate the data and recover the data. Conversely, file recovery from cloud storage is faster; it does not require physical transport from the offsite location, tape handling or seek time. Files to be recovered are located and streamed over the WAN connection, saving time and eliminating the need for a local tape infrastructure.

4. Accessibility

Cloud backup may be attractive to organizations that could not afford the investment and maintenance of a disaster recovery infrastructure -- or for those who can, but recognize the greater efficiency and cost savings to be gained by outsourcing. Offsite data copies -- accessible from any Internet-connected device/location -- provide an added measure of insurance in the event of a regional disaster (SearchDataBackup, n.d.).

There are cloud backup trade-offs as well including the following:

1. Seeding Data and Full Recovery

Depending on the total capacity of data, the first full backup and/or full recovery off-site data could prove to be too time-consuming and impactful on production systems.

2. Size Limitations

Depending on bandwidth availability, every organization will have a threshold for the most reasonable capacity of data that can be transferred daily to the cloud. These limitations will have an impact on backup strategies.

3. Discontinuation of the Service

Understanding the most graceful "exit strategy" for the service is just as important as vetting specific features. Termination or early withdrawal fees, cancellation notification, and data extraction are just a few of the factors to be considered.

4. Nonexistent Service-Level Agreements (SLAs)

The performance of the service and the "guarantees" that backup is completed successfully is not always in the provider's control. For example, availability of sufficient bandwidth, the amount of data that has to be transferred over the network and accessibility to systems to be protected are all scenarios that could contribute to non-compliance with service-level agreements (SearchDataBackup, n.d.). Advancements in cloud computing and backup technology are creating exciting developments in cloud backup. Cloud backup provides indisputable benefits to organizations with limited IT resources and capital budget, including efficiency and reliability, scalability, accessibility, and improvements in recovery of small data sets. The consumption-based pricing, coupled with the ability to fund backup from an operational budget, make the cloud backup approach an attractive alternative to on-premise tape-centric implementations -- especially in tough economic times (SearchDataBackup, n.d.).

Summary

The existing research and literature confirms the importance of data backup security. With the growth in storage, investment in education and the dependence on IT infrastructures for higher productivity, the need for data protection in schools is becoming critical. Thus the cost associated with downtime, including costs associated with lost productivity and reduced customer satisfaction due to inability to access critical business data call for the need to implement effective backup strategies that mitigate such potential calamity.

Also, it has been shown that sensitive school data fall into several categories, which require special precautions to protect it from unauthorized disclosure, accidental or unintentional modification. In addition, it has been shown that several strategies including cloud backup can be used to protect sensitive school data. Data backup security in K-12 schools seems to be an excellent focal point for further research particularly due to the importance of technology in education.

SECTION 3

METHODOLOGY

The purpose of this study was to explore data backup strategies employed by international schools in Korea. Specifically, the goal of the research was to investigate the extent to which sensitive school data are committed to technology-based storage systems, how records are categorized regarding the need for security, and how existing systems are protected. The objective of the study was to uncover specific themes and commonalities from the perspective of IT directors at international schools. The data collection and data analysis is intended to assist international schools in designing interventions to protect sensitive school data. Qualitative studies explore and investigate perception data from the population most affected; therefore, the proposed qualitative phenomenological methodology involved IT directors of 22 international schools.

Quantitative data analysis from participant responses to a survey was analyzed for significance to the problem under study. In contrast to qualitative methods, quantitative methods of research focus on testing and proving a hypothesis by quantifying and statistically measuring interrelationships between independent and dependent variables (Patton, 2002). Researchers using a quantitative methodology adhere to strict, rigorous, and disciplined protocols to test phenomena. For example, quantitative researchers operate on an assumption of realism, and that reality can be studied (Patton, 2002). This concept emulates a positivist paradigm, implying that nature is fundamentally structured and that objective reality exists autonomously of human observation. The combination of

quantitative and qualitative data is an approach that helps to locate the results in a broader context and provides a fuller picture (Silverman, 2006).

Research Design

For this research, a descriptive statistical design was used to identify how international schools in Korea use technology-based storage systems to protect sensitive school data, categorize school records with regards to sensitivity levels and the need for security, and how existing systems are protected. The phenomenological approach was used to identify issues or concerns of IT directors at 22 international schools, and recommendations for improvement were offered. Some of the key information gathered included the number of desktops/laptops, servers, student population, staff size, backup applications, percentage of IT budget committed to data protection budget, importance of backup, and legal issues regarding backup security. The participants were selected from the IT departments of K-12 international schools in Korea numbering 22. A comparison was made between best backup security practices and the current practices employed by the target population to determine whether data backup strategies being used are adequate.

Appropriateness of the Research Design

The research approach for gathering significant data for the capstone project was a mixed method of quantitative and qualitative designs. This seemed to be the most appropriate approach for the project given the limited time available to the researcher. The researcher had originally considered a purely qualitative approach to the research, but the questionnaire designed for the qualitative study would have demanded more time

for the participants to respond to the questions. On the other hand, a purely quantitative approach was also not entirely satisfactory because some of the information needed could not be easily put in a quantitative format. It is for these reasons that a mixed approach was deemed the most appropriate approach for the study. SurveyMonkey website was used to host the survey.

Participants were selected based on convenience of access. The researcher contacted participants (IT Directors) through their designated school's email address with a letter of invitation and consent form containing a direct link to the survey. The letter and consent form summarized the purpose and value of the research and contain guidelines for responding. Participants were informed that they could include their email addresses if they would like to receive information about the findings of the study and/or a copy of the consent for their records. The participants were directed to go to the link for the survey and answer the questions by mostly ticking boxes when selecting responses from multiple-choice option, as well as a few written responses.

Validity and Reliability

An important question in reviewing research literature is discerning if the methodology and findings are valid and reliable. Creswell (2009) contended validity refers to the degree to which the increment of measurement truly measures what it is designed to measure. Reliability refers to infinite duplicability of the data (Creswell, 2009). Babbie (2003) defined reliability as the ability of the research conclusions to be replicated in a different setting. Because the proposed study was mainly qualitative, though it employed quantitative analysis of some parts of the data collected, the purpose

was not to test a hypothesis, but rather to gain a rich understanding of the phenomenon (Farber, 2006). In qualitative studies, themes and patterns are isolated to describe, explore, and understand the phenomenon from the perspectives of the participants. Consequently, this mixed methods study was implemented with other methods such as triangulation to determine the merit of the results.

Internal Validity

Anfara, Brown, and Mangione (2002) referred to five interpretive dimensions that underscore internal validity: credibility, meaning, importance, transferability, and implications of the results. These five areas allow researchers to draw conclusions logically regarding the data collected. From a qualitative perspective, internal validity will yield conclusions about the problems and solutions to data backup strategies used by international schools in Korea.

External Validity

External validity suggests that the conclusions drawn from the study may be generalized to other circumstances (Kitzinger, 1995). Since the participants included IT directors from different international schools at different locations in Korea, results are intended to illuminate or corroborate what is already known in the literature regarding effective data backup strategies and their contribution to the security of sensitive school data.

Research Questions

The need to protect sensitive school data is critical. For this reason effective backup of school data is necessary for the proper functioning of the organization. The direction of this study was explorative and focused on identifying strategies used by international schools to protect sensitive data and to recommend best practices for effective data backup. This study was guided by three research questions:

1. To what extent do K-12 schools in Korea engage in technology-based applications to protect sensitive school data?

2. How are school records categorized regarding the need for secure storage?

3. How are existing security systems protected?

Pilot Study

A pilot study preceded the main observation to correct any problems with the instrumentation or other elements in the data collection technique. A sample population of two IT directors was recruited to comment on the survey in relation to the design and development of the survey instrument, questions, data collection procedures, or any other characteristics of the sample. The pilot study was used to test the effectiveness of the survey and correct any errors or problems identified in any area of the data collection technique. Changes were made in accordance to the reported errors and recommendations. Following this, the actual survey was conducted.

Setting and Participants

The setting for the research was K-12 international schools in South Korea. The participants were IT personnel in internationals schools in Korea who have the ability to comprehend and respond appropriately to the questions posed. Specifically, this involved adults in the IT department of the target schools, particularly those who perform data backup. The research was open to all international schools that fit the above category. This population was chosen for two reasons: first, no research has been done on the international schools in Korea regarding backup security. Second, the researcher has worked among the international schools and as a result has developed a special interest with this group.

Instrumentation

With regards to the methodology for the survey questionnaire, it must be noted that the concepts were developed from the literature review and the questions were framed after the best data backup security practices were identified. The researcher created the instrument used to collect the data. The selection of the questions were based on what the researcher thought would generate the most accurate information regarding data backup strategies employed by K-12 international schools in Korea. The questionnaire was constructed in various parts to capture the information needed to answer the three primary research questions. Two types of questions were generated in the interview protocol: the primary research questions, which were not asked of the participants, and the interview questions designed to reveal the information needed to answer the primary research questions.

Data Collection

The researcher contacted participants through their designated school's email address with a direct link to the survey. The researcher also spoke directly to some participants. The questionnaire was hosted online through SurveyMonkey. The survey questionnaire included a request letter stating the purpose and value of the research and guidelines for completing the survey. Additionally, the questionnaire included a voluntary informed consent for participants, and noted that they were free to withdraw their participation at any time without any consequence. The participants were not required to include their names, email addresses or any personally identifiable information.

The survey was intended to explore participant's perceptions by answering questions mostly ticking boxes when selecting responses from multiple choice options, but also included lines for written responses. The survey took approximately 10 minutes to complete and apart from clicking a mouse and typing, there were no risks identified by the researcher since all the participants hold a college degree or higher in a computer related field and were capable of comprehending the questions fully and responding appropriately. The proposed study was deemed to be one of minimal risk to participants as determined by the U.S. Federal Government Department of Health and Human Services (2009) regulation 45 CFR § 46.10, which states the probability and magnitude of harm or discomfort anticipated in the research should not be greater in and of themselves than any ordinarily encountered in daily life, or during the performance of

routine physical or psychological examinations or tests. The survey was conducted over a period of 3 weeks.

Data Analysis

Descriptive statistics (frequencies, percentages, etc.) was used for the data analysis of the quantitative data. In addition, comparisons across levels of responses by individual schools were implemented to determine differences. Further, theme analysis was employed to analyze the responses from participants in this mixed methods study. Babbie (2003) argued theme or content analysis is effective in answering questions such as why, how, or what. The described methods for the proposed study were chosen because they would yield a more detailed and accurate information regarding data backup strategies employed by international schools in Korea. Though a few of the questions were open-ended, with the majority close-ended, a combination of both theme analysis and descriptive statistical analysis ensured that appropriate interpretation of the data and the development of effective strategies can subsequently be recommended to ensure best practices for the backup of sensitive school data.

Summary

Previous sections in this paper delineated the justification for the combination of a qualitative, phenomenological research method and qualitative research method using a survey questionnaire. Due to the critical role of data backup in schools, it was necessary to perform a qualitative study that collected IT directors' thoughts and opinions regarding data backup strategies used in their respective schools. The review of literature suggested the importance of the protection of sensitive school data. An investigation into strategies

used by international schools for data backup helped to identify issues and prompted the need for effective strategies that may go a long way in improving the overall functioning of the school. Additionally, the study's rationale included the population, data collection methods, validity, reliability, the appropriateness of the methodology and data analysis.

SECTION 4

RESULTS

The purpose of this study was to explore data backup strategies employed by international schools in South Korea. The goal of the research was to investigate the extent to which sensitive school data are committed to technology-based storage systems, how records are categorized regarding the need for security, and how existing systems are protected. The objective of the study was to uncover specific themes and commonalities from the perspective of IT directors at 22 international schools in South Korea.

A combination of qualitative phenomenological methodology and quantitative analysis were employed for the study. This approach assisted in the investigation of IT Directors' perceptions of data backup security strategies used at the respective schools and the issues and vulnerabilities they face. To expand insight and current understanding of data backup security strategies employed by schools, the objective of this study was to (a) develop survey questions, (b) employ a pilot study to ensure the validity and reliability of the survey tool, (c) present the findings to establish the effectiveness of data backup strategies employed by schools, and (d) determine how issues or vulnerabilities identified impact the general functioning of the schools.

Findings

There were 22 schools involved in this study. The demographic data of the participants is presented in Table 9.

Table 9: *Demographic Information of International Schools*

School Information	Number and Percentage (%)
Size of School	
100-249	5 (38.5)
250-499	3 (23.1)
500-999	3 (23.1)
1000-1499	2 (15.4)
Size of Faculty & Staff	
10-49	5 (38.5)
50-149	8 (61.5)
Number of Desktops and Laptops	
Fewer than 50	3 (23.1)
50-149	4 (30.8)
150-299	4 (30.8)
300-499	2 (15.4)
Number of Servers	
1-5	9 (69.2)
6-10	2 (15.4)
11-25	2 (15.4)

Participants for the study were chosen from among the international schools in South Korea. Twenty-two international schools were selected for the study. From this number, 16 representing 72% responded to the survey; responses from 3 schools

representing 14% were not suitable for use. Thirteen completed surveys representing 59% were deemed suitable for the analysis. Due to privacy concerns, schools that participated in the survey could not be identified by name.

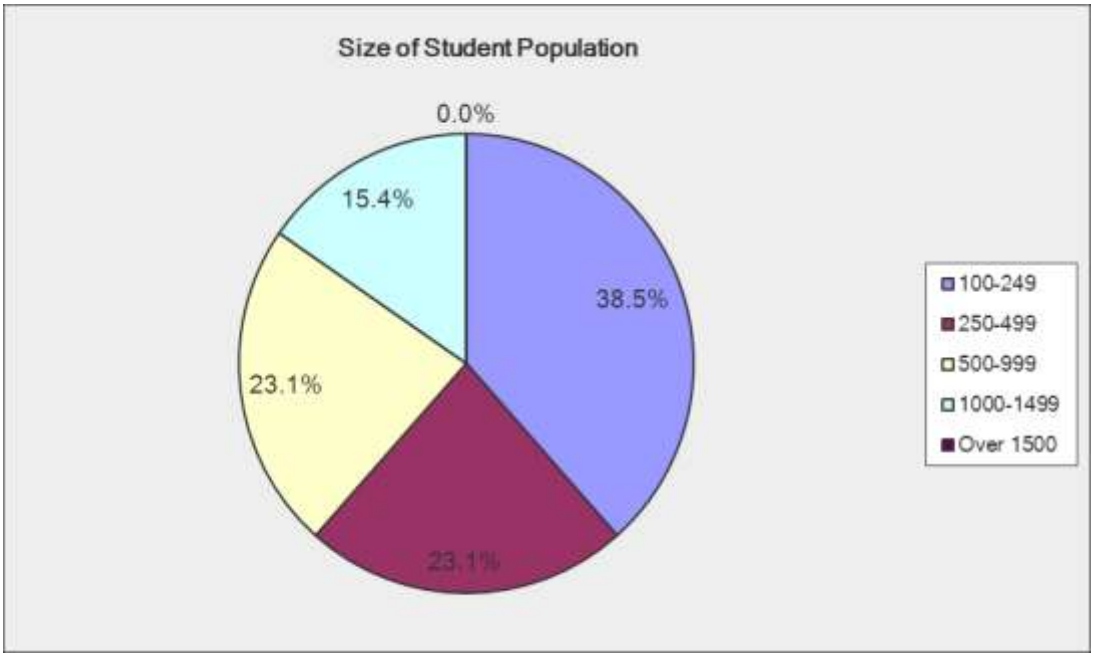

Figure 1. Size of student population.

Table 8 shows the size of the schools in terms of student population. According to the demographic information provided in Figure 1, there were five schools with a population of 100-249, three schools each with a population of 250-499 and 500-999 respectively, and two schools with a population of 1000-1499.

The questionnaire was divided into three sections. The first section sought to answer the question: To what extent do K-12 schools in South Korea engage in technology based applications to protect sensitive school data? The second section asked: How are school records categorized regarding the need for secure storage? The third section asked: How are existing backup systems protected? Significant observations that emerged from the findings were consistent with previous studies by

Forester research (Data, 2007), Wilson (2010) and TechRepublic (2011) suggesting the need for secure data backup in international schools. A report of the findings in relation to the research questions is presented below.

Analysis of Research Question 1

The first research question asked: To what extent do K-12 international schools in South Korea engage in technology based applications to protect sensitive school data? Regarding the availability of intranet-based applications for secure data backup, participants identified six applications: NovaBackup (15.4%), Genie Backup Manager (7.7%), DataBackup (30.8%), Tri-BACKUP (15.4%), Super Duper (7.7%), and Others (61.5%). Among those who chose other applications, two chose BackBlaze, one chose redundant Mirrored RAID sets, two chose Windows Server Backup features, and the rest did not name any specific application for backup (Figure 2).

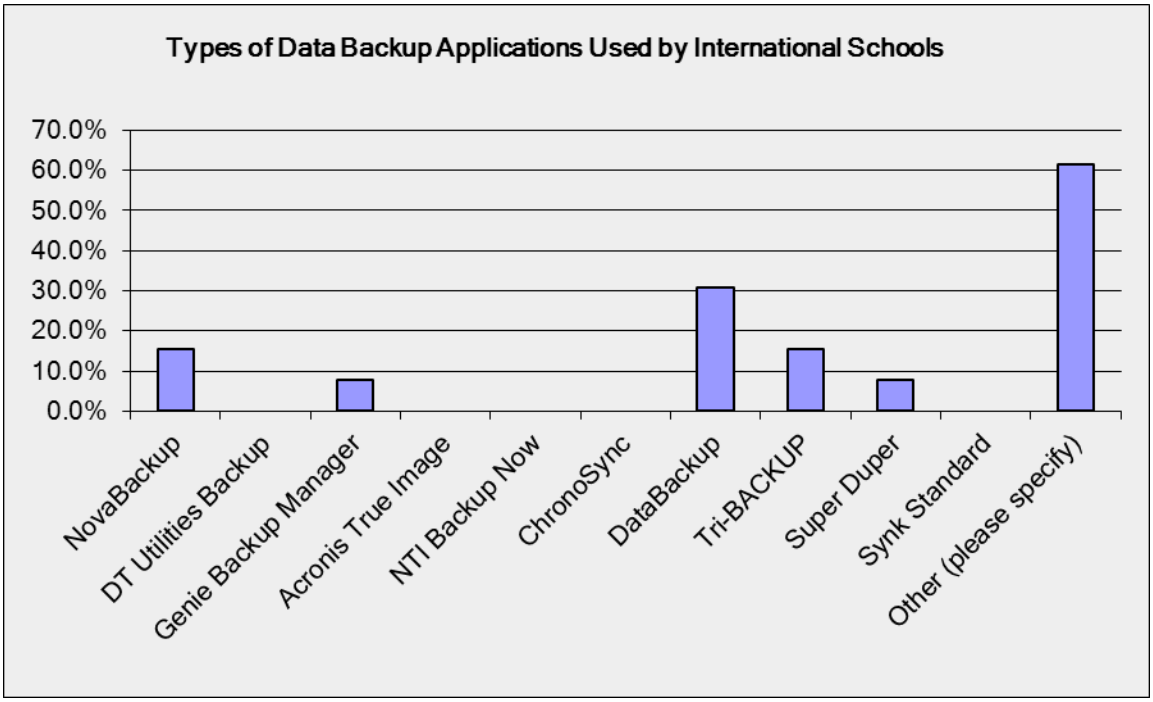

Figure 2. Backup applications used by schools.

On the need for data protection policies, 76.9% of the participants indicated there were no policies in place while only 23.1% indicated the existence of such policies (see figure 3 below).

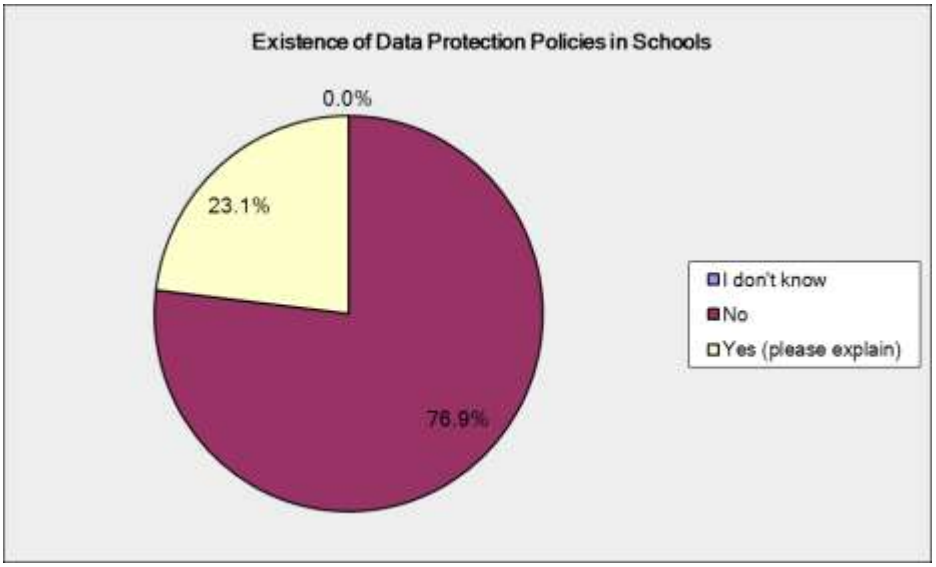

Figure 3. Existence of data protection policies.

Regarding the allocation of funds for data protection and backup, the majority of the respondents (84.6%) indicated that less than 5% of the budget for the IT department is allocated for data backup and security. Only two respondents indicated a budget allocation ranging from 5%-15% for data backup and security (Figure 4).

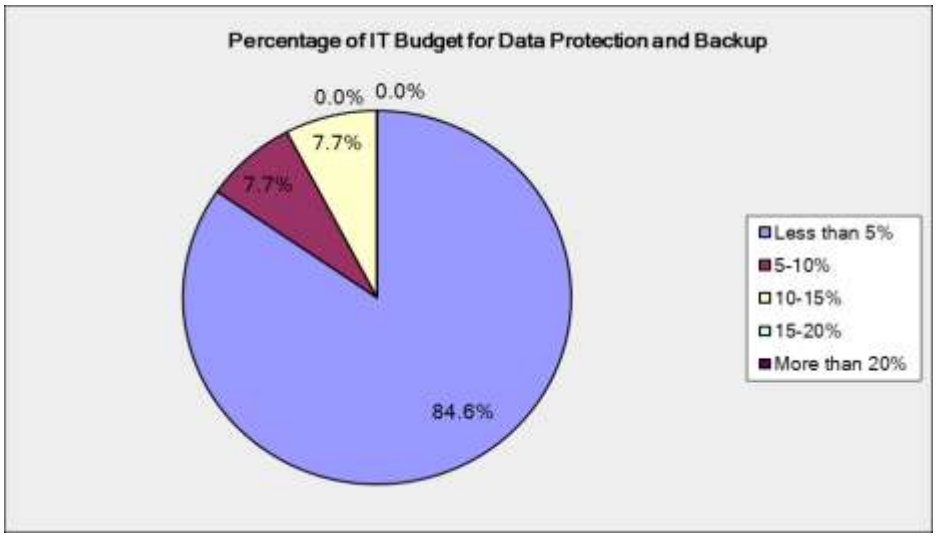

Figure 4. Percentage of IT budget for data protection and backup.

Most participants (92.4%) emphasized the importance of data backup to their schools' operations, while 7.7% indicated data backup was not important to their school. Figure 5 is a breakdown of the responses.

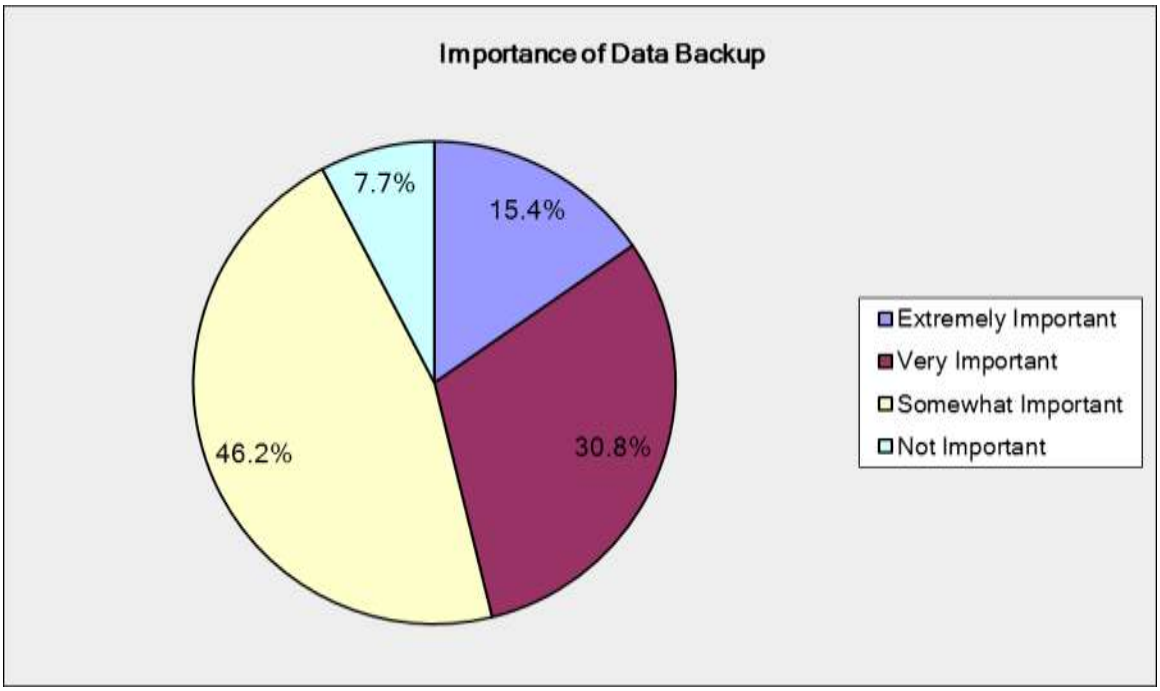

Figure 5. Importance of data backup.

Analysis of Research Question 2

The second research question 2 asked: How are school records categorized regarding the need for secure storage? In this study, school records were classified into two categories: Organizational records – financial records, personnel records, minutes of meetings, contracts and schedules; and Student Records – basic identity information, academic transcript/grades record, attendance record, health record, honours and awards. Participants were asked to rate the records according to the level of security (high, medium and low). The following information represents the rating based on the order of importance and the number of schools.

High security records: financial records (10), personnel records (8), student academic transcripts (8), staff and faculty contracts (7), student health records (7), student attendance records (5), basic student identity information (4), and minutes of meetings (1). Medium security records were identified as follows: basic student identity information (7), schedules (6), staff and faculty contracts (7), student health records (7), honors and awards 5), personnel records (4), minutes of meetings (4), Student attendance records (4), Student Academic Transcript/Grade records (4), and Financial records (3). Low security records identified were: Minutes of meetings (7), Schedules (7), Honors and Awards (7), Student attendance records (4), Basic Student Identity Information (3), Personnel Records (2), Staff and faculty contracts (1), Student Academic Transcripts (1), Student health records (1) (Figure 6).

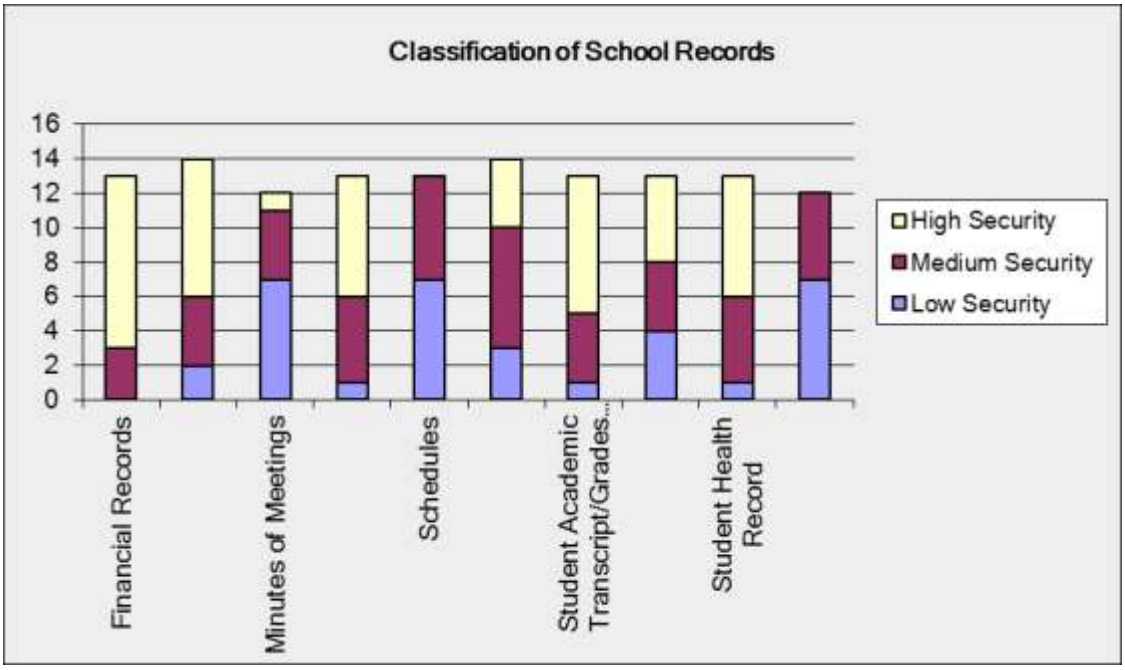

Figure 6. Classification of school records.

Concerning the mode of data storage, majority (23.1%) chose either using a secure server or in-house location. This is followed by 15.4% of participants choosing tape, outsourced or off-site (cloud computing). Only 7.7% chose a combination of cloud (Google applications and mac server) and in-house (Figure 7).

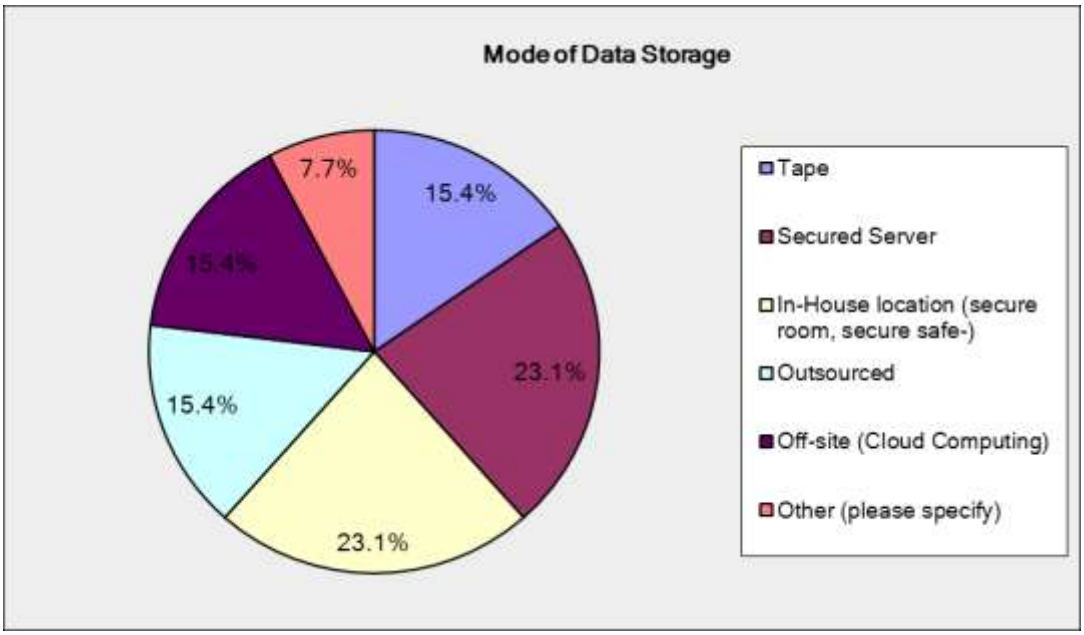

Figure 7. Mode of data storage**.**

Analysis of Research Question 3

Research question three asked: How are existing backup systems protected? Responses from participants are classified into four sections: (1) security measures, (2) security challenges (3) Legal Issues, and (4) Support and Improvement.

(1) ***Security measures.*** Results from participants' responses regarding measures for protecting backup data showed that 23.1% used the services of an off-site provider and lock containers respectively; 38.5% relied on encryption methods, storage drives, desktop storage and outsource respectively; while 15.4% used intrusion detection/prevention systems (Figure 8).

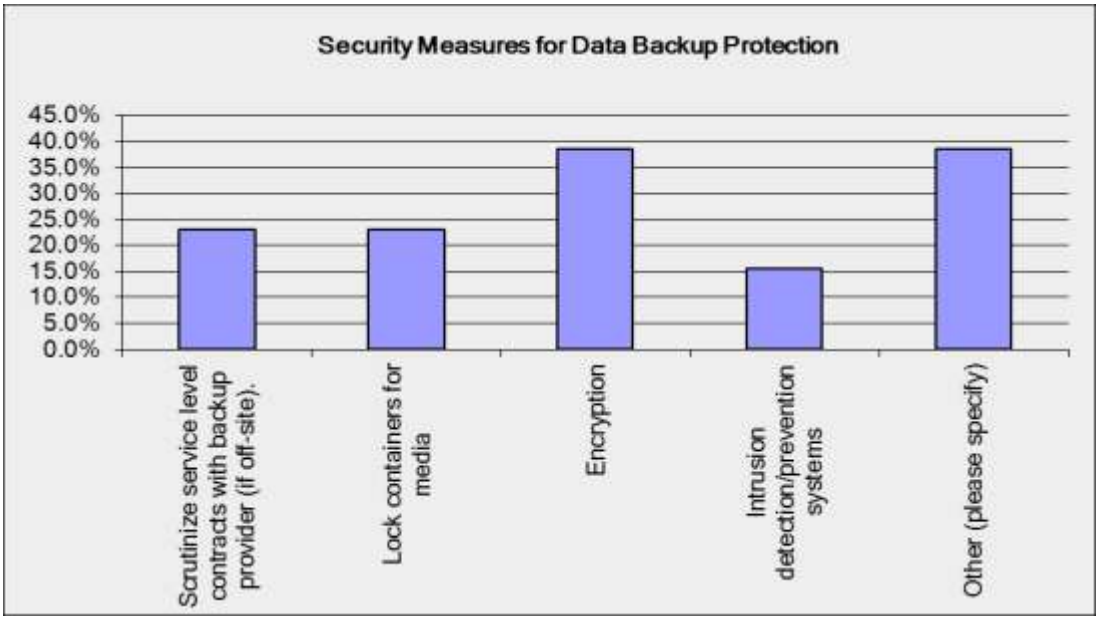

Figure 8. Security measures for data backup protection.

Regarding the general security arrangement of the schools with regards to access to buildings and offices, 38.5% of respondents rated it as secure, while 61.6% rated it as either insecure or somewhat secure (Figure 9).

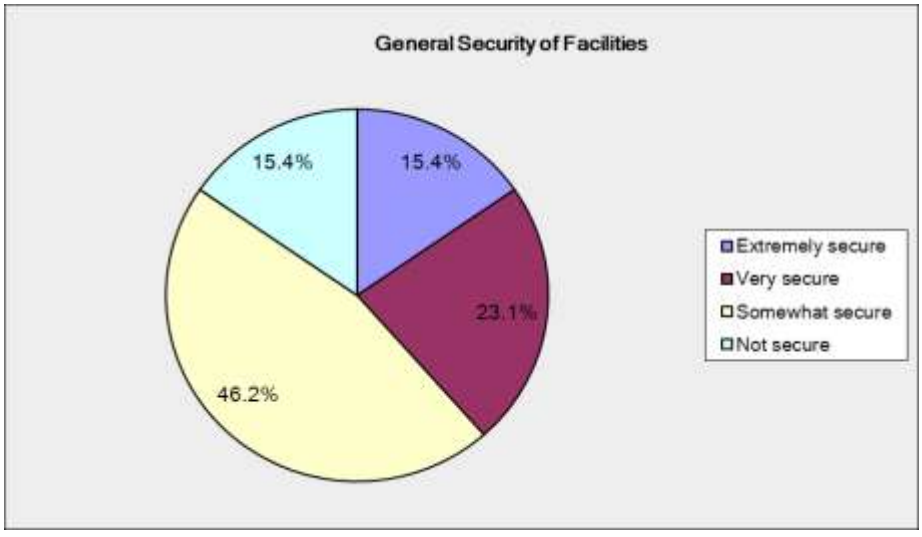

Figure 9. General security of facilities.

On the security of backup systems, 46% rated it as secure while 53.9% rated between somewhat secure and insecure (Figure 10).

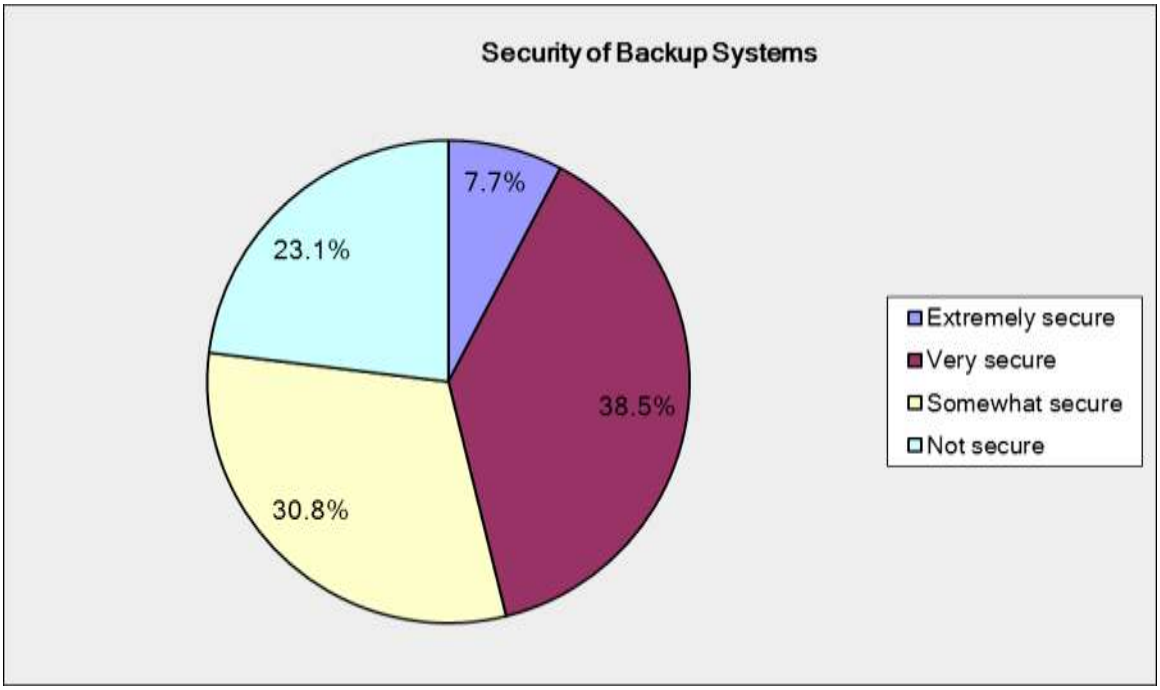

Figure 10. Security of backup systems.

Also, on measures for keeping students and staff from accessing sensitive data, all respondents indicated the use of passwords while only 4 (30.8%) indicated the use of access cards and 1 (7.7%) indicated the use of VPN's, group policies and hidden shares (Figure 11).

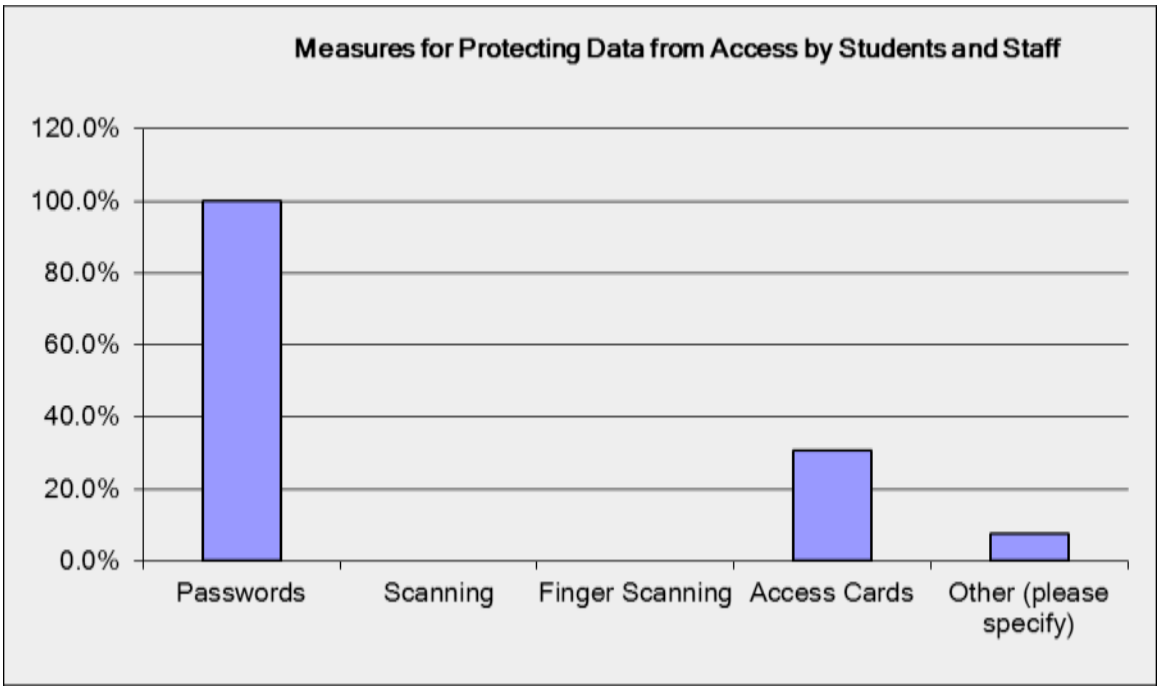

Figure 11. Measures for protecting data from access by students and staff.

Furthermore, 15.4% of respondents indicated that their schools processed confidential information at an off-site location; 61.5% did not process confidential information internally, while 23.1% had no knowledge of where school confidential information was processed.

Regarding the security of data shared between various divisions in a school, 53.8% reported the use of secure networks, 38.5% used Campus networks (CAN), 7.7% used Virtual Private networks (VPN) and 15.4% used either PowerSchool or Google applications (Figure 12).

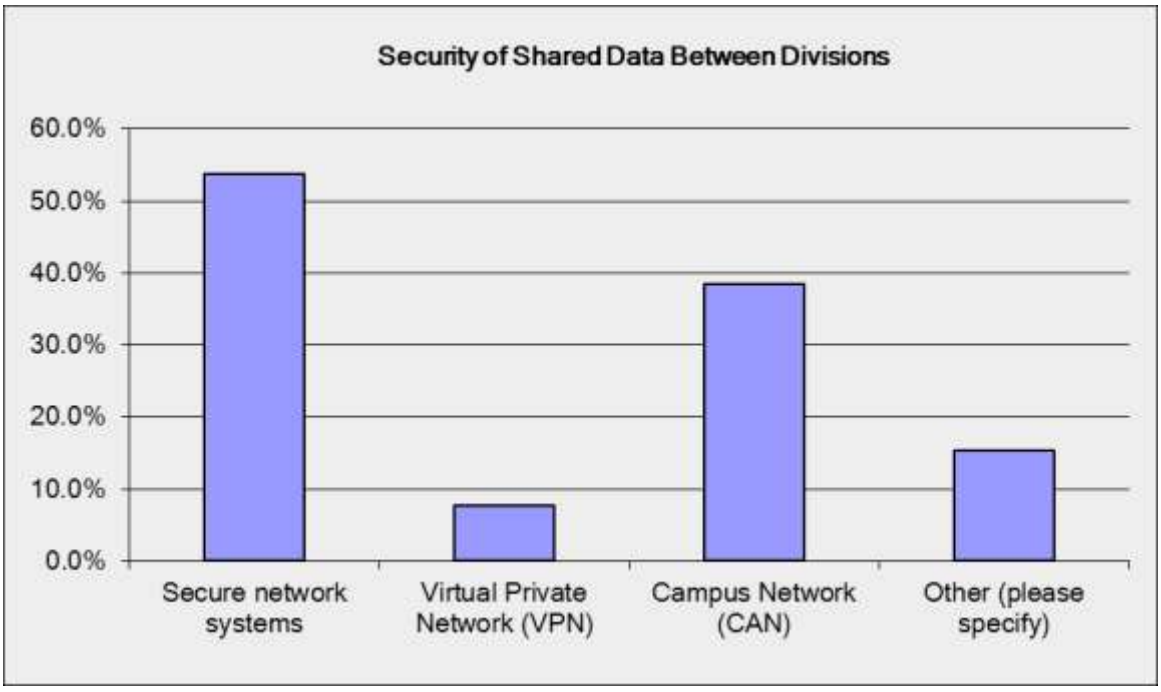

Figure 12. Security of shared data between divisions.

On the importance of information security to schools 15.4% indicated it was extremely important, 30.8% indicated it was very important while 53% rated it as either somewhat important or not important (Figure 13).

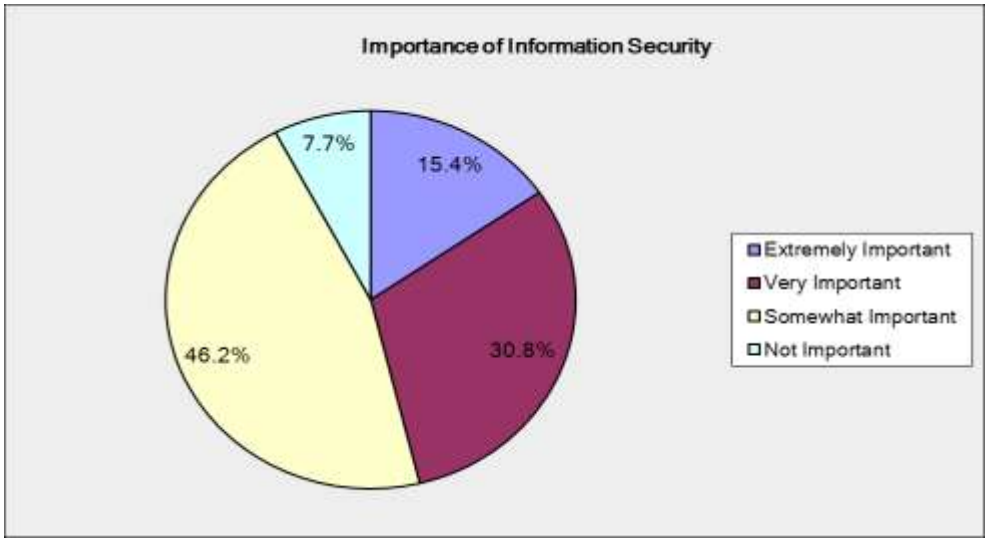

Figure 13. Importance of information security.

Regarding the maintenance of systems and networks, 46.2% indicated it was handled in-house, 38.5% indicated it was outsourced, while 15.4% reported a combination of both (Figure 14).

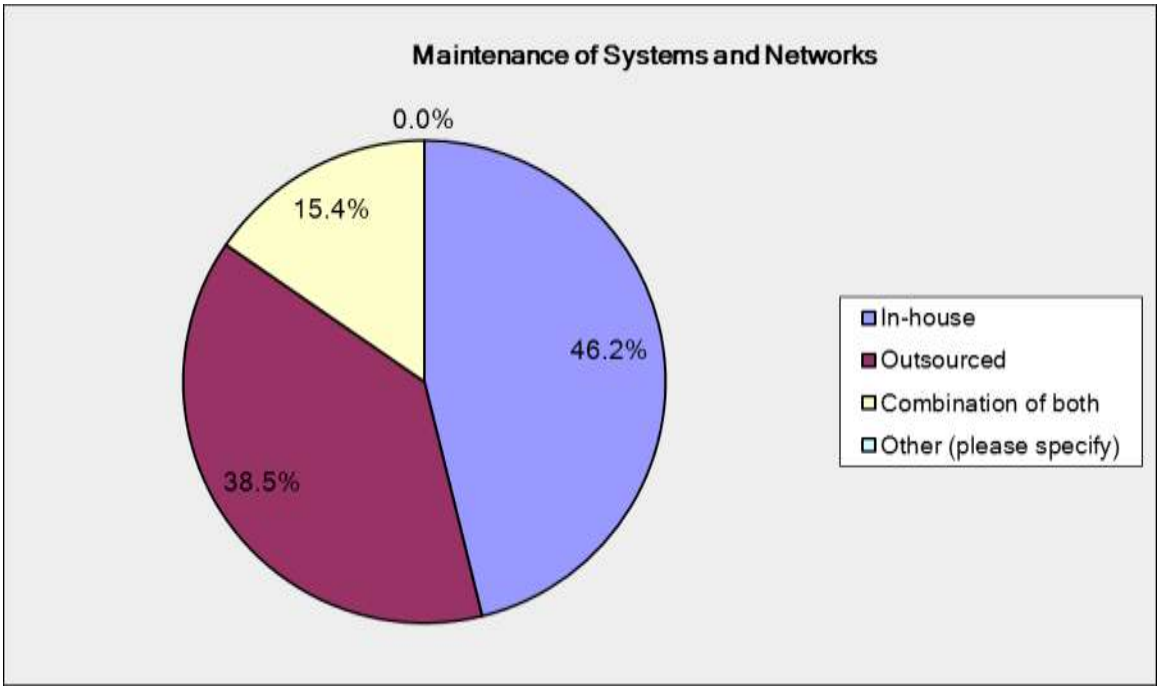

Figure 14. Maintenance of systems and networks.

Concerning the change of credentials for privileged accounts, 15.4% of participants indicated the change occurred every 3 months; 30.8% - every 6 months; 46.2% more than 6 months and 7.7% indicated it depended on the person using the account. Further, concerning the change of credentials and privileged accounts after the termination of personnel with privileged access, 30.8% participants indicated it was done the same day; 23.1% within one week; 15.4% within one month; and 30.8% more than one month (Figure 15).

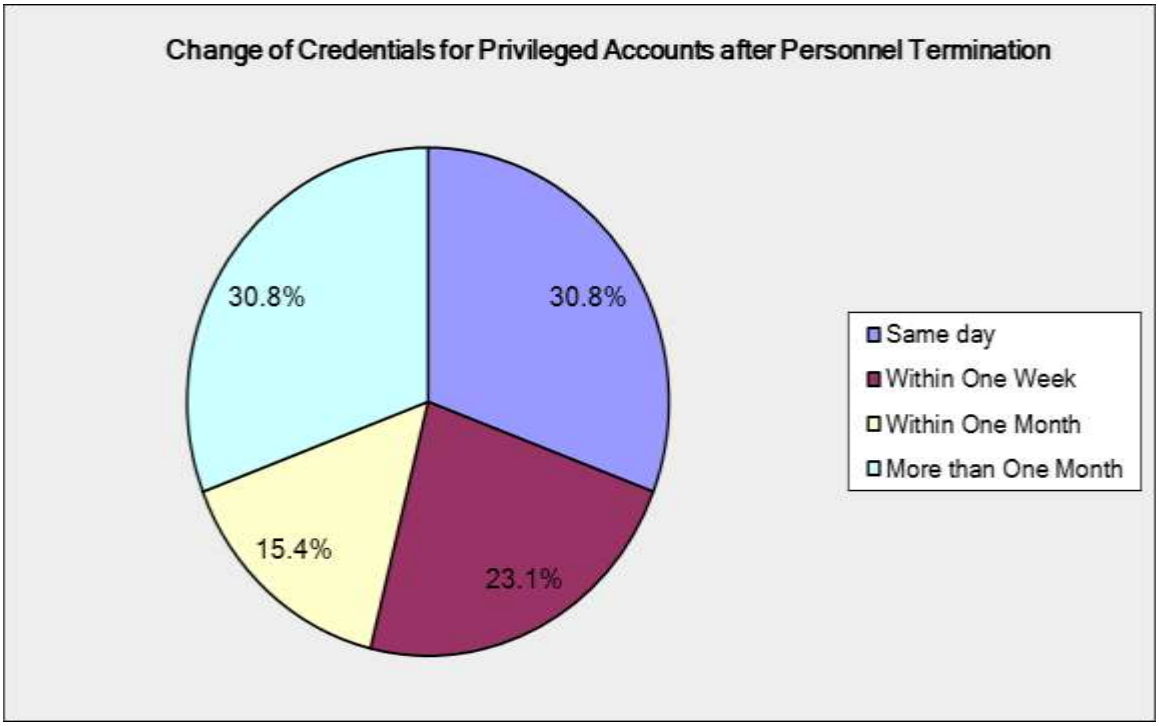

Figure 15. Change of credentials for privileged accounts after personnel termination.

(2) Security challenges. Regarding challenges associated with the security of backup data, participants were given an open-ended question and a close ended question. The following responses were obtained from the open-ended question:

1. "How to maintain data in two locations: in-house and off-site"
2. "Maintaining synchronized records both at in-house and cloud locations"
3. "Deciding between data that needs to be encrypted and ones that does not need encryption"
4. "Unauthorized personnel were able to gain access a secure server. The incident was reported and tighter access controls are now in place for the secure server room"
5. "Scheduling a backup system off-site"

6. “Students accessing teacher’s unattended computer account. Student was expelled and teacher was given a verbal warning”
7. “Tapes cannot backup all data due to large size of files and we are forced to do incremental backups”

In addition to the above, participants also reported dealing with other challenges such as virus attack (53.8%), misuse (30.8%) and other issues such as bottleneck network bandwidths and theft (46.2%) (Figure 16).

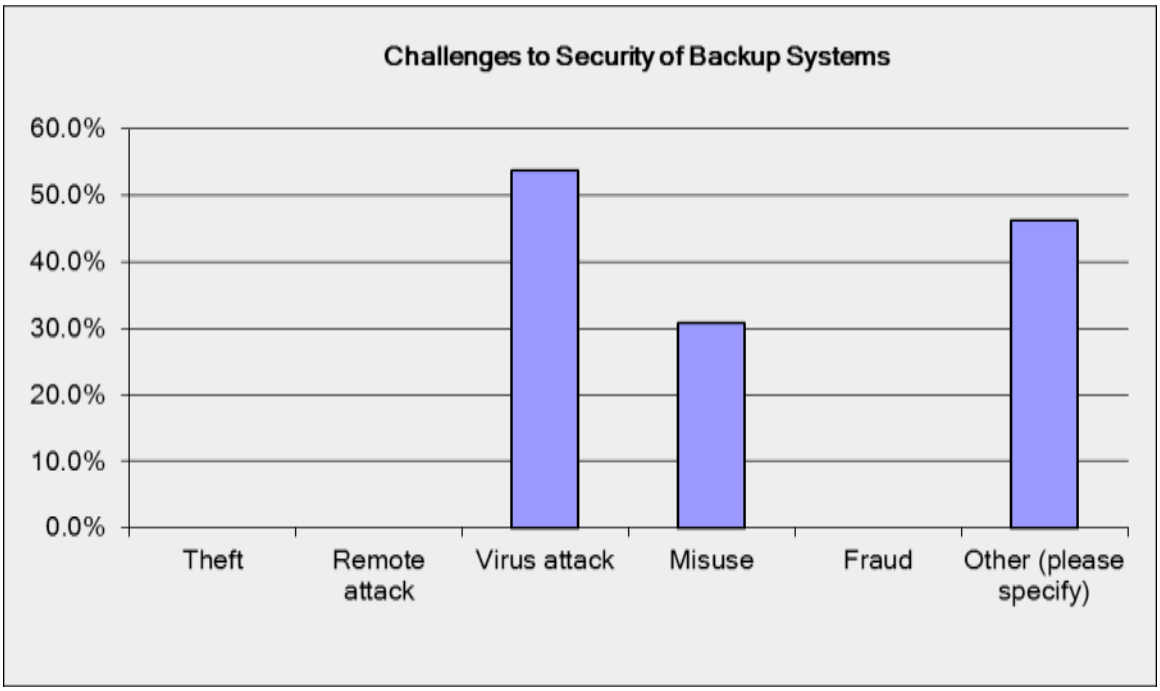

Figure 16. Challenges to security of backup systems.

(3) Legal issues. Participants reported dealing with several legal issues associated with the security of backup data. These issues are violation of copyright/federal law (7.7%), Sabotage (7.7%), Piracy (23.1%), Compromise of Data Integrity (15.4%), Breach of Confidentiality (30.8%), and Children’s Online Privacy Protection Act

(COPPA) and compromise of private information of students under 13 (46.2%) (Figure 17).

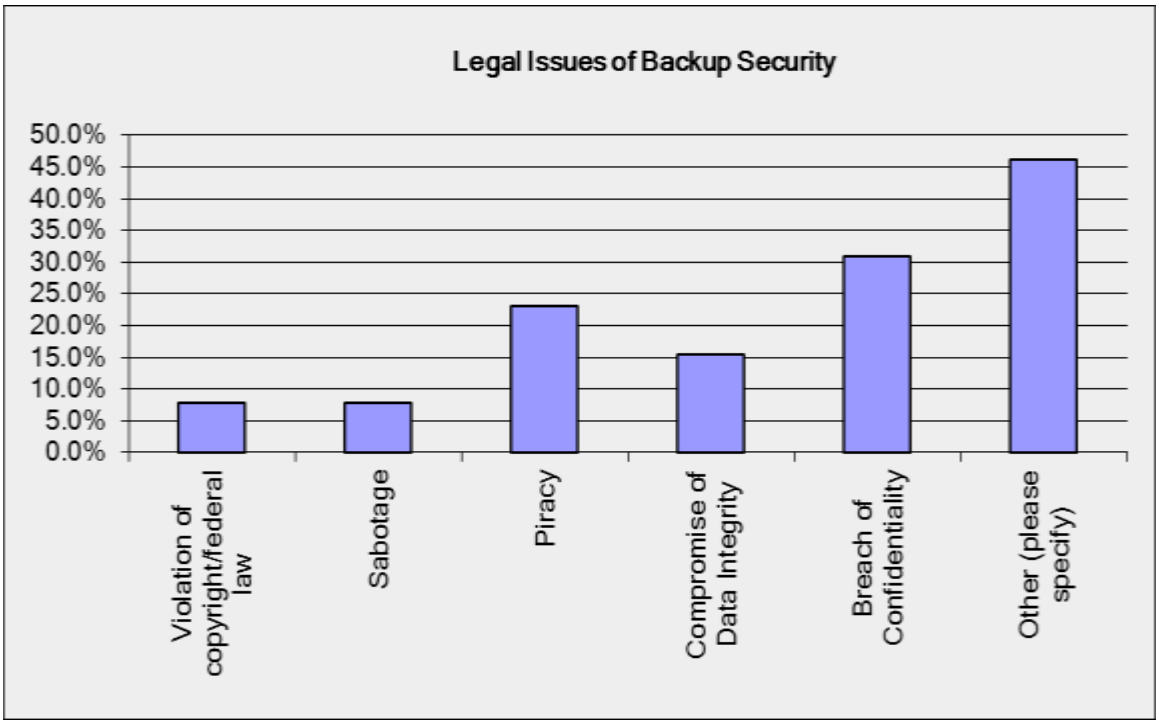

Figure 17. Legal issues of backup security.

Regarding familiarity with the laws in South Korea regarding data protection, 15.4% of participants indicated they were familiar, 23.1% reported they were somewhat familiar, and 61.5% reported they were not familiar (Figure 18).

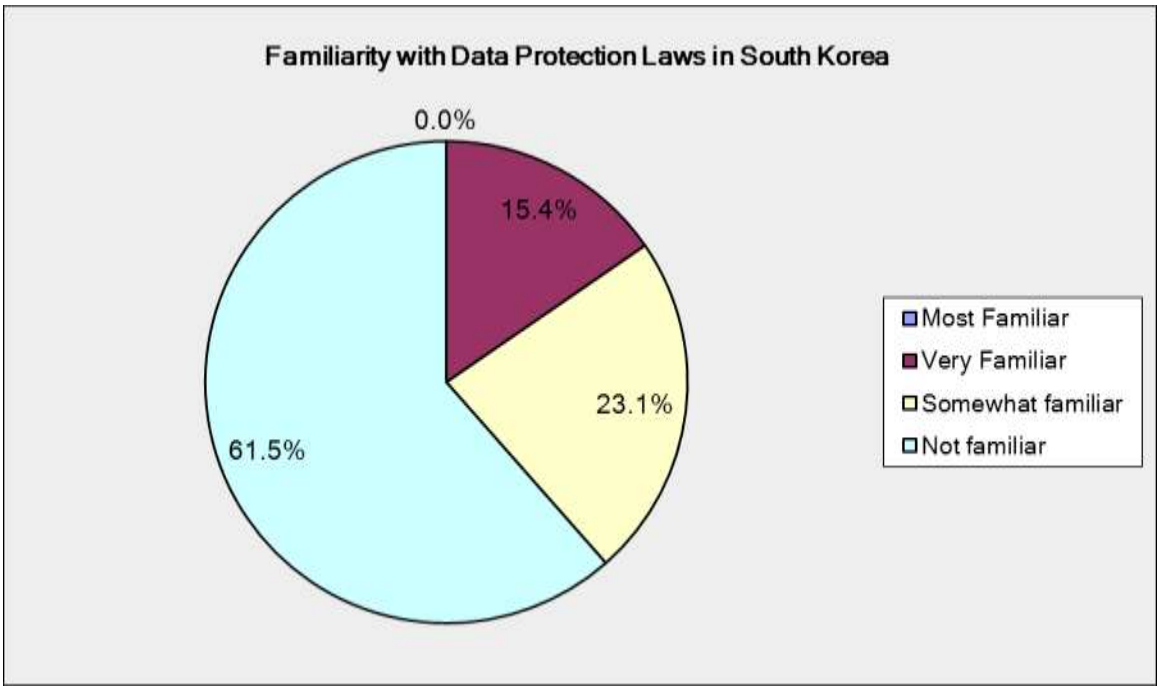

Figure 18. Familiarity with data protection laws in South Korea.

Concerning the extent to which the requirements of the law on data protection have been addressed by schools, 7.7% of participants reported full compliance, 38.5% reported moderate compliance, 23.1% reported fair compliance and 30.8% reported minimal compliance (Figure 19).

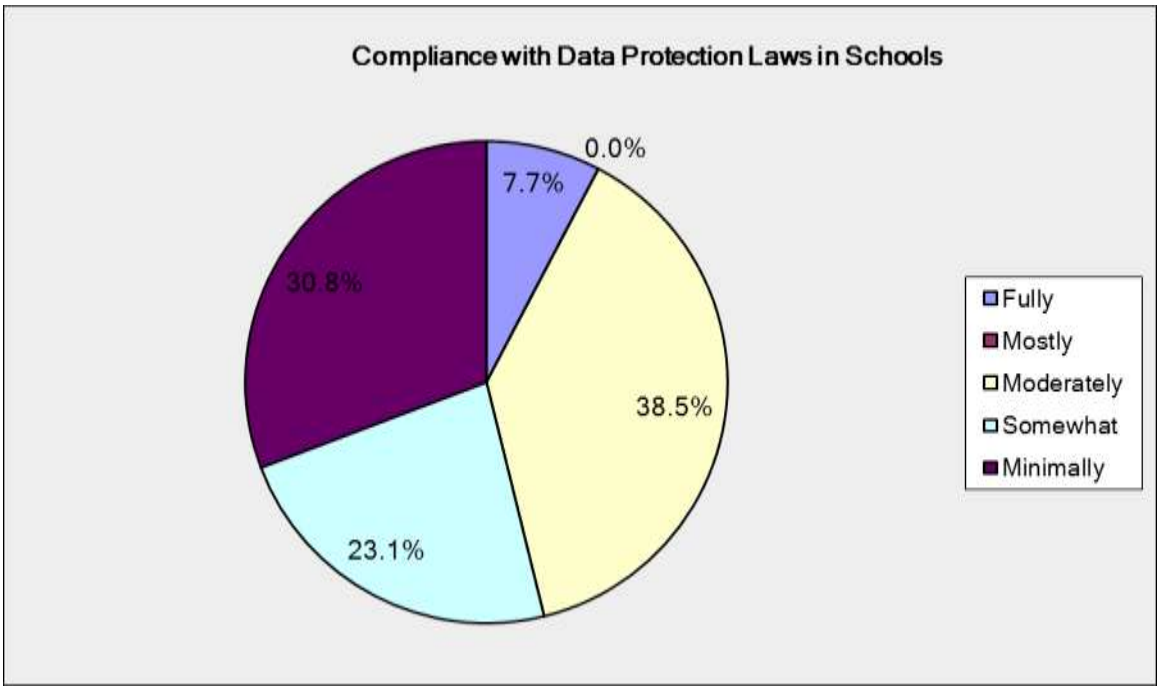

Figure 19. Compliance with data protection laws.

(4) Support and improvement. On the question of availability of support from school administration for the security of school data, 46.2% of participants reported the availability of management level support, 53.8% reported support from IT Policy Administrator, 23.1% reported support from an outside security consultant, and 15.4% reported lack of support (Figure 20).

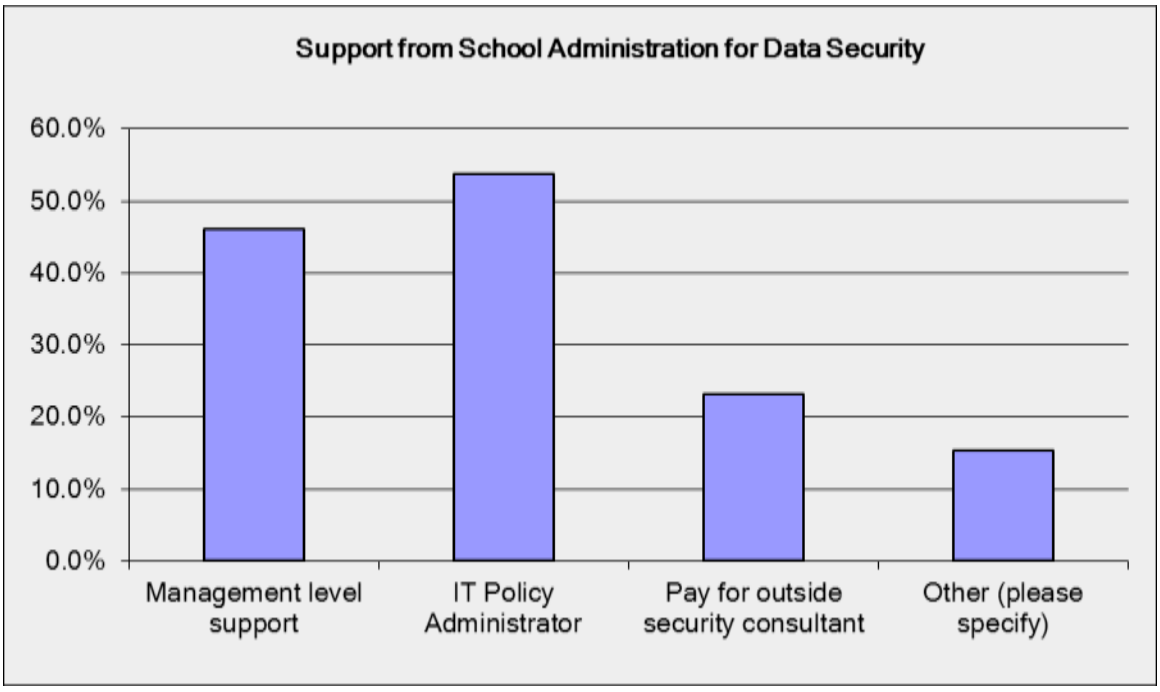

Figure 20. Support from school administration for data security.

Also regarding what is needed to improve the security of data backup systems, 61.5% of the participants suggested data security awareness education, 53.8% suggested training of IT personnel in backup security, 23.1% suggested allocation of more funds for backup security, and 15.4% suggested encryption or educating teachers about copyright laws (Figure 21).

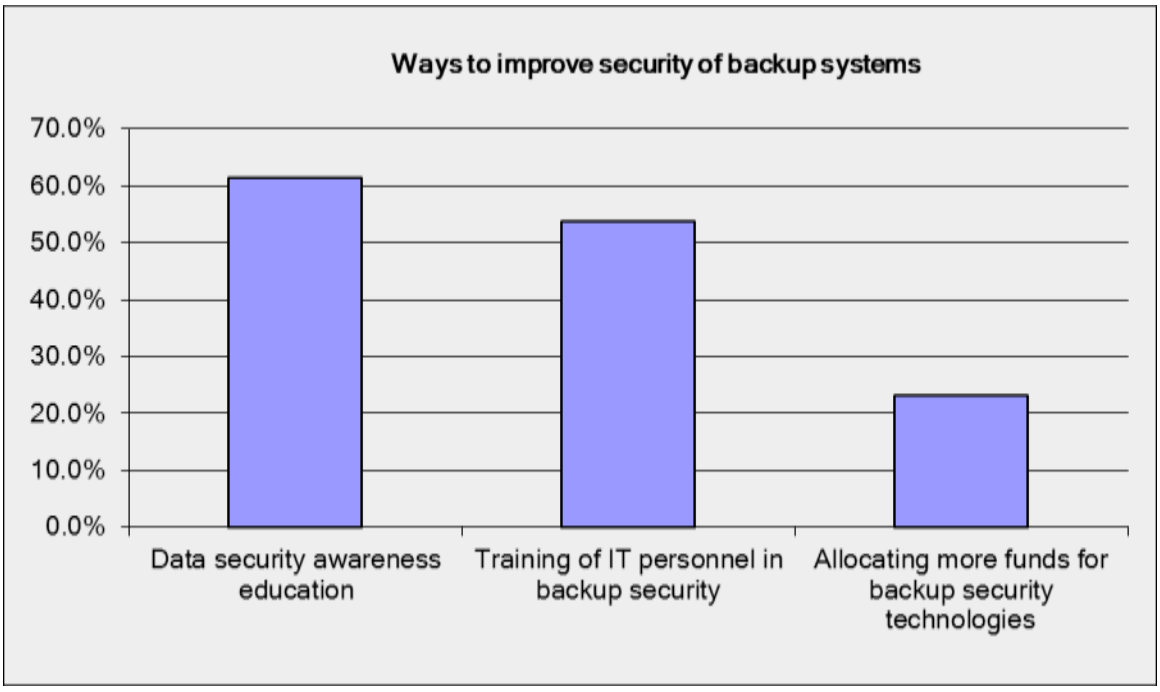

Figure 21. Ways to improve security of backup systems.

Summary

The purpose of this study was to explore data backup systems employed by international schools in South Korea. The objective of the study was to uncover specific themes and commonalities from the perspective of IT directors at international schools in South Korea. A mixed method of quantitative and qualitative research designs was the most appropriate method because the objective was to classify, learn, explain and identify issues of concern to IT directors. Participants in the study had the chance to provide insight into how existing systems in their respective schools are protected, the vulnerabilities involved and recommendations for improvement. Three investigative questions shaped the foundation for the study:

1. To what extent do K-12 schools in South Korea engage in technology based applications to protect sensitive school data?

2. How are school records categorized regarding the need for secure storage?

3. How are existing security systems protected?

Data collected from participants reflected the need improve the overall security of backup systems in international schools in South Korea. According to the participants in the study, several expressed a lack of secure systems, lack of administrative level support, lack of sufficient funding, and a lack of training in data security. With the growth in technological advancement in education and the urgent need for securing data systems, allowing these conditions to continue could undermine the operation of schools.

Conclusion

Chapter 4 presented the data collected in the study. On the basis of the perceptions of IT directors, the findings suggest the need for securing backup data and systems in schools. Most participants recommended the need for data security awareness education, training of IT personnel in backup security and allocation of more funds for backup security technologies. Chapter 5 presents a discussion of the results, implications, significance and recommendations based on the findings of the research.

SECTION 5

DISCUSSION

This study examined data backup strategies employed by international schools in South Korea. The goal of this research was to investigate the extent to which sensitive school data are committed to technology based systems, how records are categorized regarding the need for security, and how existing systems are protected. A sample of IT directors from 22 international schools was chosen for the study for two reasons: first, no research has been done on data backup security for international schools in South Korea; and secondly, the researcher has worked in an international school and therefore has developed a special interest for this group. The questionnaire utilized for this study consisted of two types of questions: the primary research questions, which were not asked of the participants, and the interview questions designed to elicit the information needed to answer the primary research questions. The questionnaires were made available online through www.surveymonkey.com.

Chapter 4 provided a comprehensive examination of the IT directors' perception regarding data backup security strategies used at the respective schools and the issues and vulnerabilities they face. Themes and commonalities were identified to gain a clear and accurate representation regarding the IT directors' perception of data backup security strategies used in the respective schools. The data used by schools is critical to their daily operations and therefore needs to be securely backed up regularly and reliably. Thus, IT directors and school administrators have the professional and ethical responsibility to ensure that secure sensitive data backup strategies are used in their

respective schools (Act, 2003; Information Practices Act, 1997). It must be pointed out that due to the dearth of research specifically examining data backup security strategies used by K-12 international schools in South Korea, this study must be seen as an exploratory effort that serves to highlight relevant themes and patterns to be explored in future studies.

Overview of Research Questions and Findings in the Context of Relevant Literature

Research Question 1: Applications for Backup Security

Research question one examined the extent to which K-12 international schools in South Korea engage in technology based applications to protect sensitive school data. The findings from the perspective of the IT directors revealed that most of the schools surveyed used some form of application for secure data backup. In fact, most participants (92.4%) indicated the importance of data backup to the operations of their schools. However, majority (76.9%) of those surveyed also indicated that there were no policies in place for data protection in their respective schools. Furthermore, 84.6% of the participants pointed out that less than 5% of their total budget was geared toward securing backup data.

These findings indicate that though IT directors are aware of the need for backup security, their efforts are hampered by a lack of adequate funds and specific policies and guidelines for data protection in their schools. This view is supported by Data (2007) that the rapid development and use of technology in the classroom has not necessarily resulted in the growth and understanding of the management of school data. Similarly,

TechRepublic (2011) also confirmed that many mid-size companies (including schools) do not adequately backup their data. Thus, with the investment in education, the dependence on IT infrastructures for higher productivity and competitive advantage, coupled with the growing interest in the integration of technology in education, it is surprising to note that interest shown by schools do not match the resources available for ensuring adequate backup security. The lack of adequate funding and policies may be explained by the following: (1) the position of IT directors in many of the international schools are mid-level positions and therefore not senior-level administrative positions and therefore they do not have equal authority to make policies and/or decisions for the allocation of adequate funding; (2) also, it is possible that school administrators and policy makers are not aware of the need for backup security and the cost associated with the loss of data; (3) or that the lack of adequate funds may be explained by the lack of policies and guidelines; and that perhaps there are no policies in place because policy makers in the school simply have no interest for backup security; (4) it is also possible that school policy makers and stakeholders may place more value on equipment (buildings, computers, etc.) than data. The findings suggest that policies for data security and allocation of adequate funds would go a long way to ensure effective data security in schools.

Research Question 2: Categorization of Records and the Security of Backup Data

The second research question examined the categorization of school records with respect to secure storage. School data was categorized according to high, medium and low level of security. The findings showed mixed responses indicating a lack of

uniformity with regards to the categorization of records. For instance, while some schools rated financial and personnel records, staff contracts, and student transcripts as high security records, others viewed them as either medium or low security records.

Also concerning the mode of data storage, several participants identified using a secure server, or in-house location, with a few choosing off-site or cloud computing. This result also confirms the finding from a recent study (Data, 2007) about the "precarious position" of small business backups where 30% lack formal data backup and storage procedures, 39% review storage procedures only after a problem occurs, 34% admit to only fair or poor performance in storing backup data offsite."

This finding from this research is consistent with Cheung, Clements and Pechman's (1997) view that sensitive school information must be classified by sensitivity category to help define appropriate security measures for its protection. Thus sensitivity categories also provide a convenient means of determining how the information is to be handled.

It may be conjectured that the approach with which K-12 international categorize and store school information reveals a pattern that falls short of the Information Practices Act (1997) that states "Categories of information that must be secured and backed up are the personal records of students and staff, financial data about the costs associated with operating the school, contracts concerning services, records of incidents of bullying or other problems between students, and operational paradigms."

The lack of uniformity in the categorization of school records indicated by the finding of this research may be explained by the lack of written *policies* for data security in international schools in Korea. National Center for Educational Statistics (NCES)

defined *security policies* as "*clear, comprehensive, and well-defined plans, rules and practices that regulate access to an organization's system and the information included in it* (NCES, 2009)." The availability of written policies help schools to classify data into various categories according to the level of importance and determine how to protect and/or release each piece of data. Good policy protects not only information and systems, but also individual employees and the organization as a whole. It also serves as a prominent statement to the outside world about the organization's commitment to security. The significance of this finding suggests the need for policies regarding sensitive classification and security of school data.

Research Question 3: Protection of Backup Systems

The third research question addressed protection measures in place for existing backup systems in relation to *security measures*, *security challenges*, *legal issues*, including *support* and *areas for improvement*.

Security measures. The findings indicated that while some measures were in place for protecting backup data, these were woefully inadequate. For instance, though 53% of participants emphasized the importance of information security in their schools, results from participants' responses regarding security measures for protecting backup data showed the following: 23.1% used the services of an off-site provider and lock containers respectively, while 38.5% relied on encryption methods, storage drives and desktop storage systems respectively; 61.6% rated access to building and offices as insecure; 53.9% rated the security of existing backup systems in their schools as insecure; almost all the schools indicated reliance on passwords for access to sensitive data; 61.5%

processed confidential information externally; 38.5% outsourced the maintenance of systems and networks; 46% changed credentials for privileged accounts after more than six months; and 30.8% changed credentials of privileged accounts after more than one month after termination of personnel with privileged access.

These findings point to the fact that, the need for secure backup data is critical if schools are to operate efficiently and meet their goals. This view is supported by NCES (2009) that, although maintaining backups is a prudent undertaking, it is not enough. Schools must be proactive in ensuring not only that their backups are reliable but, that they are secure from unintended uses or exposure. Additionally, Gardner (2000) provides support for the finding of this research by emphasizing that the primary application of technology for secure data protection in schools must be given priority for the efficient running of the educational process.

It must be pointed out that secure data protection in schools also include access to physical facilities as indicated by the findings of this research. NCES (2009) reiterates that *physical security* is a vital part of any security plan and is fundamental to all security efforts--without it, information, software, user access, and network security will be considerably more difficult, if not impossible, to initiate. *Physical security* refers to the protection of building sites and equipment (and all **information** and **software** contained therein) from theft, vandalism, natural disaster, manmade catastrophes, and accidental damage (e.g., from electrical surges, extreme temperatures, and spilled coffee). It requires solid building construction, suitable emergency preparedness, reliable power supplies, adequate climate control, and appropriate protection from intruders. Thus,

given the finding from this research, it is critical for schools to develop effective measures for data security.

***Security challenges*.** Regarding challenges associated with the security of backup data, the results of the participants' responses revealed issues such as difficulty maintaining synchronized records both at in-house and cloud locations, difficulty in determining which data needs to be encrypted and ones that do not need encryption, unauthorized physical and user access, problems with scheduling off-site backups, limitations of tape backup systems, viruses, network bandwidth bottlenecks and theft of data.

This finding is supported by Rubicon (2008), which observed some of the pitfalls of poorly implemented backup strategies and the consequences of data loss. The report of their study indicated a high level of concern among small and medium-sized businesses about potential data loss. The report also revealed that companies rated backup security as their #2 computing priority, after defense against viruses and other malware, and ahead of cost reduction and the deployment of new computers (Rubicon, 2008). Some of the key findings in the study of Rubicon (2008) identified issues such as malicious attack by employees, hardware failure, accidental data loss, failure to backup data, lack of proper discretion in the storage of sensitive data, etc., as the causes for data loss. Similarly, SpectrumData (Data, 2007) also identified challenges associated with data security such as component failure, electrical failure, accidental or intentional formatting, missing critical files systems, accidental deletion of data, virus or worm contamination, etc., as some of the challenges facing data security.

These challenges suggest the need for the exploration of alternative options for mitigating these challenges. It may be observed that an alternative option could be addressed through the use of an alternative backup solution for critical data such as online or cloud backup. However, the risks associated with online backup must be fully explored before engaging in the practice.

***Legal issues*.** The results of the research showed that participants dealt with several legal issues associated with the security of backup data such as copyright/federal law, sabotage, and piracy, compromise of data integrity, breach of confidentiality and compromise of private information of students under 13. Furthermore, the finding revealed that over 61.5% of participants were not familiar with data protection laws in South Korea and the lack of compliance thereof.

This finding suggests the need for schools to become familiar with laws regarding data security. This view is supported by Statistics (1997), which maintain that it is the responsibility of school administrators and information technology officers to review electronic information with respect to Public Records Act (Act, 2003), the Information Practices Act (Information Practices Act, 1997) and other statutory regulatory requirements that may apply in determining the sensitivity category of records that are kept in the educational environment, as well as the security measures reasonable and prudent with respect to the protection of that information. Overall, the results of this study show that schools have been lax in the knowledge and compliance of data protection laws in South Korea. This situation points to the need for schools to become familiar with data protection laws, particularly in South Korea and commit to complying with these laws.

Support and improvement. The finding of this study showed that while some schools reported management level support, majority (61.5%) indicated the need for data security awareness and the training of IT personnel in backup security. This finding is supported by NCES (2009) that information security managers need to be given the authority and budget necessary for training staff appropriately and subsequently enforcing information security procedures at all levels of the organization hierarchy. Additionally, responsibility for both meeting the public's demands for accountability and securing sensitive information is inescapable for an education institution's chief administrative officer. Like it or not, it comes with the job. Because top educational administrators are ultimately responsible for information security, they must develop a sufficient understanding of sound security strategies and how they can be realized through organizational policy. Thus, the finding provides support for information security awareness training for all staff as a means of improving the overall security structure in international schools.

Implications of the Findings

The aforementioned findings possess significant relevance for IT directors, school administrators, School Boards, Policy makers and faculty.

Data Backup Security Policies

An important finding from this study is that many international schools in South Korea do not have policies in place for data backup security. It is the responsibility of senior administrators to ensure that appropriate and effective security policy is developed

and put into practice throughout the school. Though policies themselves do not solve problems, clearly written policies do define the ideal direction toward which all the schools efforts should point to. Policy making decisions must begin with the identification of an IT Security Policy Administrator. This person must have the skill and concern about protecting sensitive information and critical systems.

Risk assessment. According to NCES (2009), developing a security policy in a school must begin with risk assessment, *a process*, which involves identification of assets, potential threats to the assets, vulnerabilities to the threats, the probability of threats affecting the vulnerabilities, and the cost estimates of losses should a potential threat be realized. The risk assessment process should also aim at eliciting information such as threats, vulnerabilities, penetrations and countermeasures pertinent to backup data. By evaluating *risk*, the school or organization is able to determine its needs so that valuable resources are not spent on unnecessary safeguards and the school is not exposed to unprotected loss. In fact, a properly executed risk assessment provides decision-makers with a methodical approach to determining security strategies based on the findings of cost/benefit analysis. Though top-level administrators must initiate risk assessment, the process must be a team effort involving feedback from all levels of the school. NCES (2009) provides the following guidelines for implementing a risk assessment:

Table 10: *Guidelines for Risk Assessment*

The Players: Team Effort
Timing: Take Stock in What You Have and What It's Worth Step 1 – Identify Sensitive Information and Critical Systems Step 2 – Estimate the Value of System Components
Identify Potential Threats and Vulnerabilities Step 3 – Identify Threats

Step 4 – Identify Vulnerabilities
Step 5 – Estimate the Likelihood of a Potential Penetration Becoming an Actual Penetration

Think Through Your Defensive Options
Step 6 – Identify Countermeasures Against Perceived Threats and Vulnerabilities
Step 7 – Estimate Costs of Implementing Countermeasures

Make Informed Decisions
Step 8 – Select Suitable Countermeasures for Implementation

Adapted from Computer Security Guidelines, p.9 (as cited in NCES, 2009)

Policy development. Findings from the risk assessment process provide policy makers with an accurate picture of the security needs specific to the school. In this way, legal and regulatory concerns, organizational characteristics, contractual stipulations, environmental issues, and use input can all be incorporated into policy development (NCES, 2009). Effective policy synthesizes these and other considerations into a clear-set of goals and objectives that direct staff as they perform their required tasks.

Although finalizing organizational policy is usually a task reserved for top-level decision-makers, contributing to the development of policy should be an organization-wide activity. While every employee does not necessarily need to attend each security policy planning session, top-level administrators should include representatives from all job levels and types in the information-gathering phase (just as in the case of brainstorming during risk assessment). Non-administrative staff have unique perspective to share with policy-makers that simply cannot be acquired by any other means. Meeting with staff on a frequent basis to learn about significant issues that affect their work is a big step toward ensuring that there is buy-in at all levels of the organization (NCES, 2009).

While it makes sense to get as much input from potential users as is possible, it is also essential that voices from outside the organization be heard during the information gathering stages of policy development. This is because decision-makers need to be informed of security arrangements that other organizations are making that potentially impact them and the policies they will be developing. If, for example, every school but one in a district commits to *encryption software* to protect messages sent over the Internet, the lone school that does not have the encryption key is going to have a very difficult time communicating with its partners. The point is that just as security planning demands coordination internally, it often requires it externally as well—a recommendation that should not be overlooked, especially by those organizations that practice site-based management.

Regardless of the findings of the risk assessment, the following general questions should be addressed in security policy (adapted from *Network Security Secrets*, p. 890; cited by NCES, 2009):

- What is the reason for the policy?
- Who developed the policy?
- Who approved the policy?
- Whose authority sustains the policy?
- Which laws or regulations, if any, are the policy based on?
- Who will enforce the policy?
- How will the policy be enforced?
- Whom does the policy affect?
- What information assets must be protected?

- What are users actually required to do?
- How should security breaches and violations be reported?
- What is the effective date and expiration date of the policy?

Policy should be written in such a way that it is concise focusing on expectations and consequences, while explaining the underlying rationale when appropriate. In addition, difficult terminologies that could create potential confusion must be clearly defined. The final document must be distilled into meaningful and manageable set of employee regulations that fits a particular school. These rules serve as the mechanisms for operationalizing policy goals and objectives throughout the school.

To help make policy implementation more realistic, the guidelines must be concise and understandable, making it easy for staff to fulfill. Specific actions that might be helpful in the implementation of policy are: (1) specifically assigning an empowered and committed administrator to be accountable for security; (2) instituting staff training that is specifically tailored to meet the requirements of security policy and the needs of the staff; (3) communicating organizational needs and expectations to staff in both initial and ongoing ways; and (4) enforcing regulations equally at all levels of the organization.

It must be noted that a successful security policy must also eliminate the need for complete trust in the system so that all suspicious behavior of systems or people are reported for action, as this serves to protect both the schools' employees and the school itself. However, before the benefits of security can be realized, staff must be properly informed of their roles, expectations and organizational expectations. For instance, employees could be asked to sign a security agreement to acknowledge their

responsibilities and verify that they comply with security policy. In addition, employees could be informed that security would be part of their performance review.

Finally, the pace of technological innovation requires that all security policies be reviewed frequently depending on the needs of the school or organization. Generally speaking, each new technological change has the potential to necessitate a corresponding policy change. For this reason, it is a good rule to review all organizational policies annually (NCES, 2009).

Funding

Another important factor for policy makers to consider is adequate funding for data security in schools. Funding provides the necessary resources and activities to protect systems and data against unauthorized access or modification of information as well as ensuring data availability. Some of the specific activities include threat assessments, risk management, configuration management, training, network monitoring, certification/accreditation, and so on. The risks associated with data loss far outweigh the cost of data protection. Therefore, it is important for policy-makers to consider allocating adequate funds for data protection in schools.

Secure Data Categorization

Another significant milestone of the finding of this study is the need for secure categorization of school data. Secure data categorization are based on the potential impact on a school should certain events occur which jeopardize the information and information systems needed to accomplish its assigned mission, protect its assets, fulfill its legal responsibilities, maintain its day-to-day functions, and protect individuals.

Security categories are to be used in conjunction with vulnerability and threat information in assessing the risk to schools, hence the need to protect sensitive school data (NIST, 2004). This approach facilitates "*Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information…*" [44 U.S.C., Sec. 3542]. Protecting sensitive data addresses the three security objectives of any information and information systems, which are:

i. C*onfidentiality:* Preventing unauthorized disclosure of information and use of information.

ii. I*ntegrity:* Preventing unauthorized creation, modification or deletion of information. Integrity guards against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity.

iii. *Availability*: Preventing unauthorized delay or denial of information.

These three objectives define the levels of potential impact on the organizations including schools should there be a breach of security (i.e., a loss of confidentiality, integrity, or availability). Therefore, the application of data categorization must take place within the context of each school and the overall security interest of the school. FERPA (1974) states:

> In addition to the everyday use of student information by teachers and administrators, education records are a source of basic data used for administrative purposes and policymaking. Statistical information summarized from education records can be an important resource for monitoring programs and for evaluating the success or failure of education policies. Administrative use of

computerized records means that education records are used increasingly farther from their point of origin. As a result, it has become more complicated but no less essential for school officials to be vigilant about protecting the confidentiality of records. Those who work with education records have legal and ethical obligations to observe rigorous procedures for protecting the privacy of the original information and the individuals whose records are involved.

As NCES (2009) rightly observed:

Education information is often considered to be confidential by its very nature- that is, certain types of sensitive information (in particular individually identifiable student and staff records) must, by law, be protected from all parties who do not have a verifiable need-to-know i.e. a legitimate educational reason for accessing confidential school data. In addition to numerous state and local laws designed to preserve the confidentiality of education records, the Family Education Rights and Privacy Act of 1974 (FERPA) is a federal law designed specifically to protect the privacy of a student's education record.

Another document published by the National Forum on Education Statistics, Protecting the Privacy of Student Records: Guidelines for Education Agencies, describes what and why specific types of information about students and their families are considered to be confidential and clarifies relevant laws governing proper and improper release of such records. Since the institution is ultimately responsible for the integrity and security of its data, the organization and its management need to take active steps to ensure that valuable equipment and, more importantly, information (such as private student and staff records) are being adequately protected. If an education organization

fails to protect its confidential information in a manner that satisfies "standards of due care" and "reasonable safeguards," it opens itself to a host of potential problems from allegations of negligence and incompetence, to law suits charging "computer malpractice," and forfeiture of insurance claims due to "preventable losses." In addition to the legal ramifications of privacy violations, the potentially priceless asset of public confidence is also at risk (Cheung, Clements, & Pechman, 1997)

Information Security

Additionally, the finding on general security measures speaks to the importance of information security, which involves three components such as confidentiality, integrity, and availability. While confidentiality is sometimes mandated by law, common sense and good practice suggest that even non-confidential information in a system should be protected as well, not necessarily from unauthorized release but from unauthorized modification and unacceptable influences on accessibility (*Information Security Modules*, p. 77, as cited in NCES, 2009).

Perhaps more than any other aspect of system security, protecting information requires specific procedural and behavioral activities. Information security requires that data files be properly created, labeled, stored, and backed up. Policy-makers can positively affect this effort by providing organizational support to the security manager as he or she implements and monitors security regulations. The security manager must be given the authority and budget necessary for training staff appropriately and subsequently enforcing information security procedures at all levels of the organizational hierarchy. A final consideration for policy-makers is information retention and disposal. All

information has a finite life cycle, and policy-makers should make sure that mechanisms are in place to ensure that information that is no longer of use is disposed of properly.

Backups. Information security is impossible without a good backup strategy. System backups not only protect the organization in the event of hardware failure or accidental deletions, but they also protect staff against unauthorized or accidental changes made to file contents. If an error is ever made, having the option of accessing an unaltered backup can be very appealing. But reaching into those archives is a viable strategy only when backup files have been made properly- a backup of a file that contains the errors and/or viruses you are trying to eliminate usually is not very helpful. Similarly, backup files need to be created at appropriate intervals and themselves must be well protected from damage and destruction.

Knowing the type of backup that best fits a particular school/organization depends on the types and number of files in the system, the level of technical expertise within the organization/school, and the organization/schools' commitment to security. Certain overarching issues need to be considered before establishing backup plans. These are (1) the amount of exposure to data loss that can comfortably be tolerated by the school/organization, (2) the age and reliability of the equipment, and (3) the nature of the workplace and whether new data is processed everyday.

To further evaluate the type of backup strategy that will best meet a school's needs, the following factors need to be weighed carefully: (1) the time and effort required to make changes to files; (2) the time and effort required to backup files; (3) the value of the data, and (4) the rate of file change (NCSA Guide to PC and LAN Security, p. 323, as cited in NCES, 2009).

In general there are two types of backup strategies that could be implemented:

1. A *full* backup - backing up an *entire* hard drive. The advantage of this strategy is its completeness since it provides a snapshot of the content of a hard disk.
2. A *partial* backup - backing up *selected* directories. This is useful and efficient if the work is concentrated in a specific area of the hard disk. Other types of partial backup are *incremental* backup (backing up files that are changed since last backup), *differential* backup (adding files since last full backup), and *daily* backup (files added or changed on the day of the backup).

It may be suggested that one may choose a combination of complete and partial backup routines. However, when initiating any system, a complete backup should first be done to serve as a reference point. Above all, it is important to devise a backup strategy that is realistic for one's school/organization.

Remote and cloud data backup. Another important area of focus for data backup security in relation to the finding of this study is remote and cloud data backup. Two popular approaches to cloud data backup are Software-as-a-Service (SaaS) and cloud storage services. As an alternative to on-premise software and secondary storage, backup SaaS is a Web-native application hosted and operated at a central location and accessed via a browser-based interface.

According to NextVault (2011)) report on "*How to Measure ROI for Online Backup and Recovery"* remote and cloud backup have the following benefits:

1. It has the potential of making data protection more viable.
2. It allows the IT department to focus on managing information and keeping staff productive rather than managing distributed infrastructure.

3. It can increase coverage and frequency of automatic backups with minor impact on IT capital expenditures and operating expenses.
4. It can address Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO) within a business contingency plan.

However, despite these benefits remote and cloud Newman (2011) points out in the Information Security Magazine on the topic *Cloud Security: Are You Ready?* that one needs to be aware of the potential security nightmares associated with cloud backup such as perimeter disappearance, instability of clients and servers. Cloud computing fundamentally changes long-standing best practices in network design, encryption and data loss prevention, access control, authentication, and auditing and regulatory compliance. While all these challenges can be mitigated, migration to cloud requires that organizations plan carefully by taking stock of their existing infrastructure and adjusting their practices and process accordingly (Newman, 2011). Newman (2011) offers the following recommendations to organizations considering cloud migration:

1. ***Increased bandwith requirements***. Cloud computing involves increased Internet connectivity for every site in the enterprise. Given that applications now reside in the cloud, there is no clearly defined perimeter. Furthermore, the traffic characteristics of every site's Internet connection may affect application performance. Beyond basic network characteristics, there is also the question of what kind of traffic leaves the enterprise as it moves to cloud computing. For this reason, it is important for organizations (schools) to understand the kind of traffic they have and consider the deployment of network-flow analysis (flow-reporting tools in routers) to provide an in-depth view of application traffic.

2. ***Impact on security devices***. Increased Internet connectivity implies a heavier workload for security devices. Depending on the security policy in place, a move to the cloud may require enabling additional IDS/IPS signatures, which may also have a negative performance impact. Other policy issues to consider is interoperability and changes to existing firewall rule sets. While testing can help validate a move to the cloud, a better practice is to model the particular mix of applications that will reside in the cloud, paying particular attention to transaction sizes, transaction durations, concurrent connection counts, overall bandwith utilization and network characteristics such as latency, jitter, and packet loss. These metrics could help organizations craft a synthetic workload that will yield meaningful predictions about security device performance.
3. ***Encryption and data loss prevention (DLP) implications***. Cloud computing require three sets of encryption endpoints: from customer to Internet, within the cloud, and from cloud to enterprise. For this reason encryption within the cloud may be necessary for regulatory compliance. However, encrypting everything from end to end also comes with unintended consequence of "blinding" key security and network management tools such as application-aware firewalls and deep-packet inspection devices. Therefore it is important to review policy for the purpose of redesigning encryption and data loss prevention (DLP) for the cloud. At a minimum, a cloud-aware security policy should specify that traffic never leaves the enterprise unencrypted. Security policies should be revised to add requirements for detection of any breach of the encryption policy, including within the cloud provider's network. Similarly, a cloud migration is an ideal

time to review policy as to permitted protocols. A revised policy should banish, once and for all, insecure protocols such as FTP that allow cleartext transmission of passwords and other sensitive data. At the same time, policy also should specify which users can employ protocols that might leak data over encrypted protocols such as Secure Shell (SSH) and Secure Copy (SCP).

4. ***Access control***. Cloud computing changes access control from an IP-based to a user-based model. Essentially, cloud computing adopts the network access control (NAC) credo that who you are governs what resources you can reach. Because both clients and servers can be mobile in cloud computing, a dynamic approach to security policy is needed. Access control in the cloud should follow the NAC model of applying rules dynamically, in real time, as endpoints appear on the network. This approach is equally valid for clients and servers.
5. ***Authentication requirements***. Cloud computing stretches authentication requirements, both figuratively and literally. Anywhere, anytime client connectivity may require new and stronger forms of authentication. At the same time, the move to place services in the cloud extends the trust domain enterprises need to protect. For both clients and services, strong control over password and key management is a must, as is better break-in detection. With cloud computing, clients no longer cross a single, well-defined security perimeter before being granted access to enterprise resources. Clients also may connect to these resources from shared public networks such as Wi-Fi hotspots, increasing the risk of password interception. A move to two-factor authentication, for example tokens plus some biometric mechanism, makes sense to ensure clients

are properly authenticated. Some well-known public cloud services such as Google Apps also support passwords plus tokens for authentication.

6. ***Compliance complications***. There are bound to be regulatory considerations when it comes to moving sensitive data to and from the cloud. Logging and monitoring is critical in the cloud, but also more complicated, with large cloud providers' networks spanning multiple continents. While this has the advantage of moving content closer to users, it complicates timestamp synchronization between server logs. Without rigorous time synchronization among servers, troubleshooting becomes very difficult. Setting all system clocks in a single time zone, such as coordinated universal time (UTC), also is essential for taking the guesswork out of distributed log analysis. A move to the cloud may increase the number of servers involved, especially where virtualization's cloning features are used, and this in turn increases the volume of logs to be analyzed. Network managers may want to consider implementing a unified log analysis system to collect and synthesize data from all the new sources.
7. ***Contracts with backup providers***. While the selection of a provider may often be based on cost and availability of service in a particular area, the fact that this provider will have physical possession of a school's most valuable assets warrants extra diligence. As with any outsourced IT service provider, schools should seek audit rights, assurance that the service provider's hiring procedures include criminal and credit background checks on all employees and indemnification of losses. Sadly, the largest service providers may resist these commitments, leaving a school to bear all of the risk resulting from mistakes made by the school or the

> service provider. While the benefits of cloud computing are real: a lower IT profile, faster provisioning, and global availability of new services. At the same time, network managers need to think carefully before making the transition (Newman, 2011).

Passwords. Another important finding in this study has to do with the use of passwords. It may be opined that just because **password** systems are the most prevalent **authentication** strategy currently being practiced does not mean that they have become any less effective. In fact, the reason for their popularity is precisely because they can be so useful in restricting system access. However, the major concern about password systems is not their technical integrity, but the degree to which (like many strategies) they rely upon proper implementation by users. While there are certainly more expensive and even effective ways of restricting user access, if risk analysis determines that a password system meets organizational needs and is the most cost-effective, one can feel confident about password protection as long as users are implementing the system properly--which, in turn, demands appropriate staff training.

Physical Security

Physical security is a vital part of any security plan and is fundamental to all security efforts--without it, information security, software security, user access security, and network security are considerably more difficult, if not impossible, to initiate. Physical security refers to the protection of building sites and equipment (and all information and software contained therein) from theft, vandalism, natural disaster, manmade catastrophes, and accidental damage (e.g., from electrical surges, extreme

temperatures, and spilled coffee). It requires solid building construction, suitable emergency preparedness, reliable power supplies, adequate climate control, and appropriate protection from intruders. Physical security requires that building site(s) be safeguarded in a way that minimizes the risk of resource theft and destruction. To accomplish this, decision-makers must be concerned about building construction, room assignments, emergency procedures, regulations governing equipment placement and use, power supplies, product handling, and relationships with outside contractors and agencies.

The physical plant must be satisfactorily secured to prevent those people who are not authorized to enter the site and use equipment from doing so. A building does not need to feel like a fort to be safe. Well-conceived plans to secure a building can be initiated without adding undue burden on the staff. After all, if they require access, they will receive it--as long as they are aware of, and abide by, the organization's stated security policies and guidelines. The only way to ensure this is to demand that before any person is given access to your system, they have first signed and returned a valid Security Agreement. This necessary security policy is too important to permit exceptions.

Legal and Ethical Issues

Concerning legal and ethical issues, it must be noted that data protection laws such as Act on Protection of Personal Information Maintained by Public Agencies (1994), Use and Protection of Credit Information Act (1995), Act on Disclosure of Information by Public Agencies (1996) are in place to protect information. In 1999, the Act on Promotion of Information and Communications Network Utilization and

Information Protection aka "the Information Protection Act" was enacted to provide guidelines for personal information protection in the private sector (Korea Law, 1999), which includes international schools in Korea. This Act, which went into effect in 2000, adopted eight principles recommended by the OECD Privacy Guidelines of 1980, including the principles of information protection, the rights of data subjects, the responsibilities of service providers, and possible remedies following personal information infringements. All organizations in the private sector in this country must abide by these laws, hence the need for international schools to know and adopt policies that align with these regulations.

Support and Improvement

Most staff in education organizations could probably offer a fairly accurate description of the term computer virus if asked. Viruses are big news. They are reported in the major media quite regularly, and, on occasion, are even headline stories. But ask those same staff members what encryption software is, or to suggest effective disk backup procedures and they will most likely find themselves without much to say. While threats and catastrophes are newsworthy, day-to-day activities that protect information systems are often considered mundane. When an organization allows television, magazines, and newspapers to be solely responsible for educating its staff, there is no logical reason for it to expect its employees to know how to implement even the most clearly stated of information technology security procedures. After all, while staff may have heard a thirty-second newsflash about the latest megavirus, they will not

have been exposed to proper ways of using computer equipment and protecting information.

All of the technological and procedural precautions in the world will be ineffective if they are not executed properly. But through well-conceived and committed security training programs, staff will be better prepared to avoid problems in the first place, minimize the damage of those problems that do arise, and maximize their contributions to system and information recovery when necessary. Without appropriate training (and associated reference tools), staff will instead be more likely to actually *contribute* to security risk through accidental but not necessarily malicious behavior. After all, most security problems are the result of unintentional human error. These mistakes will be less likely to occur when a well-intentioned employee has been properly trained.

According to NCES (2009), training in information security must have the following goals:

Goal 1: Raise staff awareness of information technology security issues in general.

Goal 2: Ensure that the staff is aware of local, state, and federal laws and regulations governing confidentiality and security.

Goal 3: Explain organizational security policies and procedures.

Goal 4: Ensure that the staff understands that security is a team effort and that each person has an important role to play in meeting security goals and objectives.

Goal 5: Train staff to meet the specific security responsibilities of their positions.

Goal 6: Inform staff that security activities will be monitored.

Goal 7: Remind staff that breaches in security carry consequences.

Goal 8: Assure staff that reporting potential and realized security breakdowns and vulnerabilities is responsible and necessary behavior (and not trouble-making).

Goal 9: Communicate to staff that the goal of creating a **"trusted system"** is achievable.

NCES (2009) offers the following training outline for information security training session:

Table 11: *Training Outline*

I. Security overview A. What is information security? B. Why does it matter? II. Federal laws A. FERPA overview B. FERPA relevance and application (include specific examples that relate to audience duties) III. State and local laws, regulations, and standards A. Statute, regulation, and standard overview B. Statute, regulation, and standard relevance and application (include specific examples that relate to audience duties) IV. The organization's security plan A. Risk assessment findings 1. Assets 2. Threats 3. Vulnerabilities B. Organizational security policies, procedures, and regulations (focus on those related to audience duties) 1. Physical security regulations 2. Information security regulations 3. Software security regulations 4. User access security regulations

5. Network security regulations

C. Security administration
   1. Expectations
   2. Monitoring activities
   3. Authority
   4. Enforcement and consequences
   5. Avenues of communication

V. On-the-job training (i.e., "Here's what you really need to do...")

A. Explanations
   1. Turning the computer on and off
   2. Logging in and out
   3. Changing passwords
   4. And so on

B. Demonstrations
   1. Turning the computer on and off
   2. Logging in and out
   3. Changing passwords
   4. And so on

C. Testing
   1. Turning the computer on and off
   2. Logging in and out
   3. Changing passwords
   4. And so on

D. Monitoring
   1. Turning the computer on and off
   2. Logging in and out
   3. Changing passwords
   4. And so on

Sample Security Training Plan, (NCES, 2009)

By describing how security protects users as well as the system and organization, security training can become an effective way of garnering staff support and ensuring that policies and regulations are implemented. How often staff should be trained (and when) is an issue that requires significant consideration. A good rule is that all newly hired employees should undergo general organizational security training as a part of their orientation before they actually assume their duties. Similarly, job-alike or comparable training should be required of all staff (new or old) at the onset of initiating a security program.

Methodological Issues and Limitations

There are several methodological limitations that dictate caution when interpreting and generalizing results from the current study. The study faced the same kinds of limitations and challenges that many such studies face when using a convenience sample. First, accessibility of IT directors willing to complete and turn in the surveys in a timely fashion was a challenge.

Second, the study was limited by the measurement tool used to assess data backup security. The questions asked were mostly multiple-choice questions. It is the opinion of the researcher that an open-ended questionnaire could have enabled participants to provide more information about their perspective of data backup security in their respective schools. Third, in terms of generalizability, the findings could not be generalized beyond K-12 international schools, nor could they apply to public schools. Furthermore, all participants were residents of South Korea, therefore the results may not generalize to countries other than South Korea.

Directions for Future Research

Risk Assessment

Based on the current literature and the findings of the present study, the need for data backup security in K-12 schools is critical. Implementing a truly secure yet a financially viable data backup security plans requires a thorough understanding of the associated trade-offs of various backup strategies and costs. Further studies on risk assessment plans for K-12 schools would be helpful in determining the value of system components, needs and safeguards necessary for implementing a viable data backup security plan.

Measurement Issues

Despite the importance of data backup security in education, there is no standard measuring instrument available for assessing security protocol in K-12 schools. For this reason, the development of a suitable instrument to assess data backup security specifically for K-12 International schools would be a desirable undertaking.

Security Policies

An important finding in this study is the lack of data backup security policies in K-12 schools. Future research aimed at policy development process for K-12 international schools is needed to expand our knowledge about information security in education.

Data Protection Contractual Language

Future research needs to be directed toward data protection contractual language. K-12 schools often function within a policy and regulatory context that are unique to them. While regulatory frameworks such as health insurance and other frameworks are common language, few among third party providers of information services to K-12 schools are aware of FERPA or the rich tapestry of internal policies governing data access and distribution. Furthermore, the innocuous nature of many contemporary services (such as social networking) has allowed companies to prosper merely by asserting rather than demonstrating strong security practices. Conveying the appropriate information security requirements, eliciting meaningful and specific responses to those requirements, assessing potential risks, and, utilizing the appropriate contractual clauses assist in framing the contracting party's role within the institution's regulatory context. For example, by including a section that calls attention to FERPA and to the fact that

some of the data the contracting party will be handling qualifies as part of a student's educational record, the organization can ensure that the vendor acknowledges that they will be operating within an environment where FERPA considerations will inform their obligations. This last point is made to underscore the need for an institution to fully understand the nature and scope of the data it is protecting in any contract. Ultimately, this will be the determining factor in choosing to include any particular proposal requirement or contract language.

Summary and Conclusions

Since there were no known studies on data security backup for K-12 International schools, this study sought to investigate the extent to which sensitive school data are committed to technology based systems, how records are categorized regarding the need for security, and how existing systems are protected. The results indicate a lack of secure systems, lack of security policies, lack of administrative level support, insufficient funding and lack of training in data security. Thus the findings suggest that securing data backup in K-12 international schools is critical. The implementation of secure data backup policies in K-12 international schools seems to be vital in protecting valuable information assets in schools. This study is beginning to highlight these realities, point the way for future efforts to explore the data security practices in K-12 international schools.

References

Act, P. R. (2003, December 3). *Public Records Act.* Retrieved February 3, 2011, from The First Amendment Organization: http://www.thefirstamendment.org/publicrecordsact.pdf

Amazon. (2010). Retrieved May 1, 2011, from Amazon Website: http://aws.amazon.com/ebs/

Amazon. (2011). Retrieved May 1, 2011, from Amazon Web site: http://aws.amazon.com/ec2/instance-types/

Anfara, V., Brown, K., & Mangione, T. (2002). Qualitative analysis on stage: Making the research process more public. *Educational Researcher, 31*(7), 28-38. Retrieved March 20, 2011 from EBSCO database.

Babbie, E. (2003). The practice of social research (10th ed.). Belmont, CA: Wadsworth Thomson Publishing.

BackupAssist. (2011). *BackupAssisit.* Retrieved March 1, 2011, from BackupAssist: http://www.backupassist.com/education/bsg3.html

Board, I. S. (2009, August 13). *Information Technology Security Standards.* Retrieved February 13, 2010, from

Center, E. P. (2005, January 3). *Privacy Act of 1974*. Retrieved January 12, 2011, from http://epic.org/privacy/laws/privacy_act.html

Cheung, O. (1997). National Forum on Education Statistics. In Protecting the Privacy of Students: Guidelines for Education Agencies. .

Cornell University Law School: United States Code. (n.d.). *Definition*. Retrieved April 8, 2011, from http://www.law.cornell.edu/uscode/44/3542.html

CERIAS. (n.d.). *CERIAS.* Retrieved March 2, 2011, from CERIAS: http://www.cerias.purdue.edu/assets/pdf/k-12/k12_program_packet.pdf

Cisco Systems and Network Appliance. (2008). Data protection strategies and options for network- storage (NAS) in both distributed and centralized topologies based on Ethernet /IP network infrastructure. Cisco Systems.

Creswell, J. W. (2009). Educational research: Planning, conducting, and evaluating quantitative and qualitative research (2nd ed.). Upper Saddle River, NJ: Pearson.

Data, S. (2010). *Common causes of data loss.* Retrieved February 3, 2011, from Spectrum Data: http://www.spectrumdatarecovery.com.au/content.aspx?cid=176

Data, T. (2007). *Tandberg data corporation.* Retrieved February 1, 2011, from Tandberg Data:http://www.exabyte.com/support/online/documentation/whitepapers/basicbackup.pdf

Deacon, A. (2011, April 14). *Anthony's Blog.* Retrieved May 2, 2011, from Anthony's Blog: http://anthonydeacon.wordpress.com/2011/04/14/dropbox-the-perfect-example-of-software-above-the-level-of-a-single-device/

eHow. (2011). *EHow.* Retrieved March 2, 2011, from Ehow.com: http://www.ehow.com/facts_7261815_importance-data-files-school-computers.html

Farber, N. (2006). Conducting qualitative research: A practical guide for school counselors. *Professional School Counseling, 9*(5), 367-375. Retrieved on March 20, 2011 from EBSCO database.

Gardner, H. (2000). Technology remakes the schools. *Futurist, 34,* 30-34.

Information Practices Act. (1997). Retrieved February 1, 2011, from Information Practices Act: http://www.dhcs.ca.gov/formsandpubs/laws/priv/Pages/StateInformationPractices Act.aspx

IASL. (2009). *International Association of School Librarians*. Retrieved April 8, 2011, from IASL Meeting Place Web site: http://iaslonline.ning.com/group/regioninternationalschools/forum/topics/how-to-define-an-international

ISTE. (2010). Retrieved February 2, 2010, from International Society for Technology in Education: http://www.iste.org/about-iste/advocacy/top-ten-in-10.aspx

Kant, C. (2011, January). *Top considerations for implementing secure backup and recovery*. Retrieved January 11, 2011, from Zmanda: http://www.zmanda.com/backup-security.html

Toolbox, I. (2010, October 14). *IT Toolbox.* Retrieved May 3, 2011, from IT Toolbox: http://it.toolbox.com/wiki/index.php/SaaS

Kessier, S. (2010, November). *Mashable.* Retrieved February 2, 2011, from Mashable Web site: http://mashable.com/2010/11/22/technology-in-education/

Kitziner, J. (1995). Qualitative research: Introducing focus groups. *BMJ*, 311, 299-302. Retrieved March 20, 2011 from http://www.bmj.com/cgi/content/full/311/7000/299

Korea Law. (n.d.). *Law on Information Technology and E-Commerce in Korea*. Retrieved March 13, 2011, from Korea-Law.org Web site: http://www.korea-law.org

Laws, S. (2009). Retrieved March 2, 2011, from http://www.spamlaws.com/why-computer-backup-important.html

Logix, V. (2010, December 3). *Vault logix*. Retrieved February 3, 2010, from Vault Logix: http://www.dataprotection.com/online-backup-news/online-backup/most-small-businesses-do-not-use-cloud-based-backup-study-finds-29538

Mahmood, M. K (2004). A comparison of traditional method and computer-assisted instruction on student achievement in general science. PhD thesis (unpublished), University of the Punjab, Lahore, India.

Mifflin, H. (2008). *American Heritage Dictionary*. Retrieved April 8, 2011, from American Heritage Dictionary Web site: http://dictionary.reference.com/browse/security (information)

Moustakas, C. (1994). Phenomenological research methods. Thousand Oaks, CA: Sage Publications Ltd. National Center for Education Statistics. (2009). Retrieved February 1, 2011, from National Center for Education Statistics: http://nces.ed.gov/pubs98/safetech/chapter1.asp

NCES. (2009). In NCES (Ed.), *National Center for Education Statistics*. Retrieved April 20, 2011, from National Center for Education Statistics Web site: http://nces.ed.gov/pubs98/safetech/chapter3.asp.

Newman, D. (2011, April 11). Cloud Security: Are You Ready? *Information Security Magazine*, pp. 22-30.

NextVault. (2011). How to Measure ROI on Online Backup and Recovery. *Nextvault*.

Patton, M. Q. (2002). Qualitative research and evaluation methods (3rd ed.). Newbury Park, CA: Sage.

Raffo, D. (2010, January 29). *Tech target*. Retrieved January 12, 2011, from http://searchdatabackup.techtarget.com/generic/0,295582,sid187_gci1379943,00.html

Republic, T. (2011). *Tech republic.* Retrieved February 4, 2011, from Small Business Backup: http://www.techrepublic.com/whitepapers/small-business-backup-your-data-may-not-be-as-protected-as-you-think/951689/post?tag=mantle_skin;content

Roblyer, M. D., & Doering, A. (2009). *Integrating education technology into teaching.* Allyn & Bacon.

Rubicon. (2008, November 12). *InformationWeek.* Retrieved February 15, 2011, from InformationWeek:http://www.informationweek.com/whitepaper/download/showPDF.jhtml?id=60900003&site_id=300001&cid=nl_wp_DENWSL021109&profileCreated=true

Schonfeld, E. (2011, February 22). *TechCrunch.* Retrieved May 1, 2011, from TechCrunch: http://techcrunch.com/tag/evernote/

SearchDataBackup. (n.d.). *SearchDataBackup.* Retrieved March 12, 2011, from SearchDataBackup: http://www.searchdatabackup.com

Silverman, D. (2010). Doing qualitative research (3rd ed.). Newbury Park, CA: Sage Publications Ltd.

Statistics, N. C. (n.d.). *nces.* Retrieved March 1, 2011, from National Center for Education Statistics Website: http://nces.ed.gov/pubs98/safetech/chapter1.asp

Statistics, N. C. (1997). *Protecting the privacy of student records: Guidelines for education agencies.* Retrieved February 2, 2011, from http://nces.ed.gov/pubs97/97527.p

Strom, S. (2010, May 7). *Sans InfoSec Reading Room.* Retrieved February 13, 2011, from Sans InfoSec Reading Room: http://www.sans.org/reading_room/whitepapers/backup/online-backup-worth-risk_33363

Target, T. (2009, March 9). *Tech target*. Retrieved Jauary 11, 2011, from http://searchdatabackup.techtarget.com/generic/0,295582,sid187_gci1350058_mem1,00.html#q6

Tube, O. (2010, January 27). *Open tube*. Retrieved January 13, 2011, from http://open-tube.com/what-is-cloud-backup-a-beginners-guide-to-cloud-backuphttp://docs.google.com/viewer?a=v&q=cache:6aqTsnIycysJ:isb.wa.gov/policies/401s.doc+standard+security+measures+for+sensitive+data+S1+to+S4&hl=en&pid=bl&srcid=ADGEESi5WLAoFknVbfeAGXrvU83EBYGm_zdoq8k5iAU6vvoJHbB4P85g8DhuVP1cThkCI5z2aVjV4t8Nv9Txuat2mshTQV17i

TechTarget. (2010, November 3). *Search Storage.* Retrieved March 3, 2011, from Search Storage: http://searchstorage.techtarget.com/sDefinition/0,,sid5_gci211633,00.html

TechMedia Network.com. (2011). *Data Backup Software Review 2011*. Tech March 3, 2011, Media Network.com Top Ten Reviews Web site: http://data-backu-software-review.toptenreviews.com/

TechTarget. (2009). *TechTarget.* Retrieved April 08, 2011, from TechTarget: http://searchdatamanagement.techtarget.com/definition/data

TechTarget. (2011). *TechTarget.* Retrieved February 14, 2011, from TechTarget: http://searchdatabackup.techtarget.com/tutorial/Cloud-backup-tutorial-How-to-leverage-cloud-backup-services#q5

TechRepublic. (2011, January). TechRepublic. Retrieved February 15, 2011, from TechRepublic: http://www.techrepublic.com/whitepapers/online-server-backup-checklist-for-your-small-business/2408563

U.S. Department of Health and Human Services Code of Federal Regulations, 45 CFR § 46.102(2009).

Veeam. (2010). Retrieved March 2, 2011, from Veeam: http://www.veeam.com/success_story_backup_prarie%20south_ss.pdf

Wilson, J. (2010, December 2). Lenovo-AMD study reveals that SMBs are overworked, using insecure computing methods. *Pc Magazine*. Retrieved March 1, 2011, from PC Magazine Web site: http://www.pcmag.com/business/article/resource-and cash-strapped-sma#more

Appendix A

Letter of Invitation and Consent Form

LETTER OF CONSENT

Date: February 22, 2011

Project Title: Data Backup Security: Best Practices for K-12 International Schools in South Korea

Researcher: Monica L. Oteng-Boateng

Email: pecimob@gmail.com

Tel: 010-3142-5694

Dear Participant,

You are being requested to participate in a research study about Data Backup Security for International Schools in Korea. The purpose of the study is to investigate data backup security strategies employed by K-12 international schools in Korea.

Participation in the study is voluntary. However, if you agree to participate in the study you will be required to check or tick a box below to register your consent to participate in the study. You can withdraw your consent at any time without any consequence.

Each participant will answer the questions based on your experiences and observations based on the subject above. Each questionnaire has been randomly assigned a number for research purposes. This number will not jeopardize your

anonymity, and that all information provided will be treated with the strictest confidence. The information will be analyzed and reported in aggregate form. In addition, all completed questionnaire will be shredded on completion of the study.

Most of the questions require short answers with a few written responses. Please answer all questions to the best of your ability. Please feel free to write any additional information that you consider necessary. It takes approximately 10 minutes to complete the questionnaire.

There are no risks associated with your participation in the survey. While there is no financial compensation for participating in the study, participants and international schools (including students and parents) will **benefit** from the outcome of the study. For example, the lessons drawn from the study may help schools' backup strategies used for protecting sensitive school data, which in turn may help them develop effective strategies to secure school data.

The study has been approved by the Institutional Review Board and the Department of Mathematics and Computer Science at Lewis University. It is under the supervision of Dr. Ray Klump, a Professor of Information Security, whose particulars appear below:

Dr. Ray Klump, Professor,

Department Mathematics and Computer Science

College of Arts & Sciences (MSc in Information Security Program)

Lewis University

Main Campus, Romeoville, IL

E-mail: klumpra@lewisu.edu

If you wish further information regarding your rights as a research participant, you may contact the Lewis University Institutional Review Board Administrator, Dr. Stephany Schlachter, Office of the Provost (schlacst@lewisu.edu, 815-836-5639).

Furthermore, if you would like to receive a copy of the findings of the study and/or a copy of the consent for your records, please submit your address in the space provided at the end of the questionnaire. If you have any questions, please do not hesitate to contact the researcher by email or by telephone.

Thank you.

Consent Statement:

I have read the information provided above, and I have had an opportunity to ask any question I have about the study. I am at least 18 years old and therefore agree to participate in the study at my will and not under any duress from the researcher by checking or ticking the box below.

☐ I agree to participate in the study.

Appendix B

Quantitative Survey

PRIMARY QUESTION 1:

To what extent do K-12 international schools in Korea engage in technology-based applications to protect sensitive school data?

Interview Questions

1. Number of Desktops and Laptops:
    a. Fewer than 50
    b. 50-149
    c. 150-299
    d. 300-499
    e. More than 500
2. Number of servers in use at your school:
    a. 1-5
    b. 6-10
    c. 11-25
    d. More than 25
3. What is the size (student population) of your school?
    a. 100-249
    b. 250-499
    c. 500-999
    d. 1000-1499

e. Over 1500

4. What is the size of your staff and faculty?

   a. 10-49

   b. 50-149

   c. 150-299

   d. 300-399

Interview/Survey Questions

5. What intranet-based applications are available in your school for backup of sensitive employee and student data? Please check all that apply.

   a. NovaBackup

   b. DT Utilities Backup

   c. Genie Backup Manager

   d. Acronis True Image

   e. NTI Backup Now

   f. ChronoSync

   g. DataBackup

   h. Tri-BACKUP

   i. Super Duper

   j. Synk Standard

   k. Other _____ (please specify)

6. Does your school have any policy in place for protecting sensitive data?

   a. Yes (if yes, please explain)……..

   b. No

c. I don't know

7. What percentage of your IT department budget is geared toward data protection and backup?

   a. Less than 5%

   b. 5-10%

   c. 10-15%

   d. 15-20%

   e. More than 20%

8. How important is data backup to your school?

   a. Extremely important

   b. Very important

   c. Somewhat important

   d. Not important

PRIMARY QUESTION 2

How are school records categorized regarding the need for secure storage?

Interview/Survey Questions

9. How are school records categorized in terms of their level of security? Please check (√) one according to the level of security.

Organizational Records	**High Security**	**Medium Security**	**Low Security**
Financial Records			
Personnel Records			
Minutes of Meetings			

Contracts			
Schedules			
Student Records			
Basic Identity Info			
Academic Transcript/ Grades Record			
Attendance Record			
Health Record			
Honors & Awards			

10. How is sensitive or critical data stored in your school?

    a. Tape

    b. Secured Server

    c. In-House location (secure room, secure safe-)

    d. Outsourced

    e. Off-site (Cloud Computing)

    f. Other (please explain) _____

PRIMARY QUESTION 3

How are existing backup systems protected?

Interview/Survey Questions

11. What security measures are undertaken to protect backup data? (Select all that apply)

    a. Scrutinize service level contracts with backup provider (if off-site).

    b. Lock containers for media

    c. Encryption

d. Intrusion detection/prevention systems

e. Other (please give details) _____

12. Describe two challenges you have faced in securing backup data and how did you deal with them?
13. How would you rate the general security arrangement (access to offices, buildings, etc.) of your school?

    a. Extremely secure

    b. Very secure

    c. Somewhat secure

    d. Not secure

14. Which of the following issues have you had to deal with regarding the security of your backup systems? (Select all that apply)

    a. Theft

    b. Remote attack

    c. Virus attack

    d. Misuse

    e. Fraud

    f. Others (please specify)_____

15. What legal issues have you had to deal with regarding the security of backup systems? (Select all that apply)

    a. Violation of copyright/federal law

    b. Sabotage

    c. Piracy

d. Compromise of Data Integrity

e. Breach of Confidentiality

f. Others (please specify)_____

16. How familiar are you with the laws regarding data protection in Korea?

a. Most Familiar

b. Very Familiar

c. Somewhat familiar

d. Not familiar

17. To what extent has the requirement of the law regarding data protection been addressed by your school?

a. Fully

b. Mostly

c. Moderately

d. Somewhat

e. Minimally

18. How secure are your school's data backup systems?

a. Extremely secure

b. Very secure

c. Somewhat secure

d. Not secure

19. Which of the following is the most important thing to do to improve the security of your backup system?

a. Data security awareness education

b. Training of IT personnel in backup security

c. Allocating more funds for backup security technologies

20. What support is available from the school administration for securing sensitive school data? (Select all that apply)

    a. Management level support

    b. IT Policy Administrator

    c. Pay for outside security consultant

    d. Other (please explain) _____

21. What measures are in place to keep students and staff from accessing sensitive data? (Select all that apply)

    a. Passwords

    b. Scanning

    c. Finger printing

    d. Access Cards

    e. Other (please specify) _____

22. Aside from backup media, does your school allow confidential data off-site for processing?

    a. Yes (if yes, explain)

    b. No

    c. I don't know

23. What recovery plans are in place in the event of a disaster?

24. How do you ensure the security of data shared between the various divisions in your school?
    a. Secure network systems
    b. Virtual Private Network (VPN)
    c. Campus Network (CAN)
    d. Other (please specify) _____
25. To what extent is information security important for your school?
    a. Extremely Important
    b. Very Important
    c. Somewhat Important
    d. Not Important
26. How are systems and networks maintained?
    a. In-house
    b. Outsourced
    c. Combination of both
    d. Other (please specify)
27. How often are credentials for privileged accounts changed?
    a. Every 3 months
    b. Every 6 months
    c. More than 6 months
28. When does your school change credentials for privileged accounts after termination of personnel with privileged access?
    a. Same day

b. Within One Week

c. Within One Month

d. More than One Month

29. What types of backup schedule is your school using?

Please check all that apply

a. Weekly Off-Site Full Backup

b. Daily Differential Backup

c. Daily Incremental Backup

d. Other (please specify)_____