2011

Educational Technology: Transitioning from Business Continuity to Mission Continuity

Kelly Broyles Mekdeci
Lehigh University

Educational Technology: Transitioning from Business Continuity to Mission Continuity

by

Kelly Broyles Mekdeci

Presented to Dissertation Committee

of Lehigh University

Dissertation in Candidacy for the Degree of

Doctor of Education

in

Educational Leadership

Advisor: Dr. Roland K. Yoshida

Committee Members: Dr. M.J. Bishop, Dr. Bruce Taggart,

and Dr. Leona Shreve

November 2, 2011

This thesis is accepted and approved in partial fulfillment of the requirements for the degree of Doctor of Education.

_____
November 2, 2011

_____
Roland K. Yoshida, Advisor

_____
M.J. Bishop

_____
Bruce Taggart

_____
Leona Shreve

_____
Chairperson of Department

ACKNOWLEDGMENTS

I doubt it would be possible to single out the hundreds of individuals who have contributed to my growth and journey thus far. Consequently, I will begin by thanking God for having filled my life from the beginning with exceptional people and profound opportunities, including more than one second chance. I have been blessed to the point of indulgence.

The members of my incomparable family provide the love and support that sustain me every day. My parents, Doug and Benita; my sister, Nicki; my husband, Joe; and our three children, Ian, Ben, and Rachel; thank you for believing in me, tolerating my whims, and supporting my adventures. I love you and dedicate this work to you.

Dr. Ron Yoshida, you are also an exceptional person in my journey and I thank you for your devotion to your students' success and your commitment to quality. I value every lesson you have taught me and will always consider you to be the mentor by which to measure all other advisors. I feel privileged to have had you guide me through this most challenging of processes.

Thank you, Dr. Leona Shreve; your educational leadership has inspired me for nearly two decades. Dr. M.J. Bishop and Dr. Bruce Taggart, thank you for your invaluable contributions to my study. Your expertise and willingness to share your time and insight provided immeasurable enhancement to the quality of my study. Thanks also to Dr. Daphne Hobson, Dr. Karen Hendershot, and Cohort 4 for being inspiring sources of encouragement.

To my colleagues at the Georgetown International Academy and my peers at other AASSA schools, thank you for backing me up and cheering me along. I extend particular thanks to Paul Poore, Judi Fenton, Dr. Ronald Marino, and Dr. Bill Scotti. Finally, I wish to give hearty thanks to the precious friends who helped carry me through this journey. Johnette, Shiromanie, Donna, Karen, and many others, but especially Pilar Lisa Starkey.

TABLE OF CONTENTS

LIST OF TABLES

Abstract

United States schools and American Overseas (A/OS) schools depend upon educational technology (ET) to support business operations and student learning experiences. Schools rely upon administrative software, on-line course modules, information databases, digital communications systems, and many other ET processes. However, ET's fragility compared to buildings and other physical resources makes it vulnerable to potential compromise from a variety of threats including natural disasters, human created risks, and environmental dangers. In order to make certain that their ET is adequately protected, schools would benefit from engaging in business continuity planning. This study examined the business continuity planning practices among overseas American schools in South America. The results indicated that nearly every school engaged, to some degree, in business continuity planning for ET. However, many educators did not recognize such planning as being critical to the school's mission. In addition, the primary drivers of business continuity planning for ET were reported to have been derived from external factors that existed outside of the school's governance and organizational structures (e.g. keeping abreast of recommended business practices, threats specific to geographic location, etc.) In contrast, the barriers to effective business continuity planning were reported to have been derived from internal factors such as business or academic units not having defined their business continuity needs, lack of staff expertise, and difficulty developing campus policies and procedures. These results indicate a need for educational leaders to take steps to ensure that members of their school community perceive business continuity in terms of mission continuity. Regardless of size, A/OS status, or previous experiences, much of the capacity to remove barriers to effective continuity planning existed within the participating schools' internal

governance and organizational structures. Accrediting bodies and other organizations that influence the development of school policy should review their standards of good practice and continuous improvement in the areas of business continuity planning and consider requiring schools to protect the administrative, instructional, and technological systems that support their mission. If new mission continuity standards are proposed, then guidelines and training should be made available to help school leaders implement best practices.

Keywords: technology, educational technology, business continuity planning, disaster recovery, American overseas schools, mission, mission continuity, accreditation, standards, IT

Chapter 1

Introduction, Rationale, and Literature Review

United States schools and American Overseas (A/OS) schools depend upon educational technology (ET) as a crucial component of business operations and student learning experiences (Condie & Livingston, 2007; Huett, Moller, Foshay, & Coleman, 2008; Kim & Olaciregui, 2008; Ligon & Mangino, 2005; Solomon, 2006). However, ET's fragility compared to buildings and other physical resources makes it vulnerable to potential compromise from a variety of threats. Threats to ET include natural disasters, such as fires and weather-related events, human created risks such as viruses and sabotage, and environmental dangers including power outages and software errors (Banks, Higgs, Emeagwai, Walters, Guy, 2010; Swanson, Wohl, Pope, Grance, Hash, & Thomas, 2002).

Despite a lack of empirical data regarding disaster preparedness, many business firms are engaging in contingency planning for information technology (IT) (Barbara, 2006; Cerullo & Cerullo, 2004; Nguyen, 2007; Pitt & Goyal, 2004). Historically, IT contingency planning focused on disaster recovery. Disaster recovery planning addresses the reconstruction and retrieving of information after significant damage or destruction (Elrod, 2005; Kirchner, Karande, & Markowski, 2006, slide 2; Pirani & Yanosky, 2007). Disaster recovery plans define the resources, actions, tasks and data required to manage the business recovery process in the event that a crisis-induced disaster has disrupted IT operations (Nwosisi & Nieto, 2007; Pirani & Yanosky). However, disaster recovery planning is now widely considered to be a component of a more encompassing preventative approach called business continuity planning (Agee & Yang, 2009; Elrod, 2005; Yanosky, 2007).

Organizations adopt business continuity plans in order to keep a business operational throughout a disaster (Barbara, 2006; Golden & Oblinger, 2007; Kuzyk, 2007; Nguyen, 2007). A business continuity plan comprises the interdependent objectives of identifying major risks of business interruption, developing a plan to reduce the impact of the risks, and implementing, testing, and maintaining the plan (Cerullo & Cerullo, 2004). These plans often include a redundant IT system and operations at an alternate site (Elrod, 2005; Nguyen, 2007; Swanson, et al., 2002). IT business continuity planning specifically addresses the continuous functioning of IT services during a disaster. Most organizations are dependent upon IT for their day-to-day operations. Therefore, IT business continuity planning is an integral component of overall business continuity planning.

Schools also need to engage in business continuity and disaster recovery planning to ensure that their technology is adequately protected (Carlise, 2005; Dewey, 2006; Ligon & Mangino, 2005; Shroads, 2005; Wilson, 2005; Omar, Udeh & Mantha, 2010). Many United States public school districts engage in business continuity planning for IT (Golden & Oblinger, 2007; Henke, 2008; Ligon & Mangino, 2005; O'Hanlon, 2007; Swanson, et al., 2002). However, most individuals have a limited understanding of the extent of ET business continuity planning that occurs in American independent schools and even less of an understanding of the extent of business continuity planning occurring in A/OS schools. Therefore, the purpose of this study was to investigate ET business continuity practices among schools that belong to the Association of American Schools in South America (AASSA), some of which were A/OS schools. This study also sought to determine whether variables such as a school's size, previous ET disaster experiences, and classification as an A/OS influenced the extent to which the schools engaged in ET business continuity practices.

Current Status of Technology Use in Schools

Databases often perform the functions of yesterday's filing cabinets by storing crucial information such as student transcripts, employee work history and salary data, library catalogues, accounting systems, digital libraries, course and curriculum development, and business transactions (Anderson & Becker, 2001; Glennan & Melmed, 1996; Ithaca City School District Department of Information & Instructional Technology, 2006; Kuzyk, 2007; Ligon & Mangino, 2005). ET has also become fundamental to instruction as a means of presenting lessons, organizing materials, and providing classroom experiences beyond the traditional brick and mortar school house environment (Condie & Livingston, 2007; Huett, et al., 2008; Kim & Olaciregui, 2008; Solomon, 2006).

During the past two decades, the federal government, local boards of education and chief administrators of public school districts and private schools in the United States and other parts of the world have encouraged and supported the widespread adoption of computers as teaching devices (Machin, McNally, Silva, 2007; Peck, Cuban, Kirkpatrick, 2002; Tondeur, van Braak, & Valcek, 2007; Twining, 2001). No Child Left Behind also encouraged widespread technology integration by mandating that each American public school student be technologically literate by Grade 8 (Pitrelli, 2007). Also, in 2004 the U.S. Department of Education released a National Education Technology plan that asserted the need for schools to practice new models of education using technology.

It is not surprising that Rowland (2000) found in a large survey study that American teachers frequently used technology for administrative tasks (e.g. keeping records, communicating with parents and colleagues), instructional tasks (e.g. creating teaching materials, gathering information for lesson planning, presenting multimedia classroom lessons), and

professional tasks (e.g. accessing research, best practices for teaching, and model lesson plans) (Pitrelli, 2007). In addition to the uses listed above ET has supported classroom environments via one-to-one laptop programs and digital classrooms that use the Internet to create online or virtual classrooms (Barbour & Reeves, 2009; Bird, 2008; Huett, et al., 2008; Kimber & Wyatt-Smith, 2006; Lowther, Ross, & Morrison, 2003). Bird (2008) found that approximately 73% of US school districts reported that one-to-one laptop programs are now in operation in at least one of their schools. Similarly, Roblyer (2006) found that 36% of US school districts had students participating in virtual courses in which students learned in a digital, distance-education format (Roblyer, 2006).

In recent years, some schools have also begun to use cloud computing to support both administrative tasks and student learning. The term "the cloud" describes the thousands of servers and computers that power the Internet (Johnson, Smith, Levine, & Haywood, 2010; Knorr, 2008). The term "cloud computing" refers to the practice of accessing and using technology resources such as storage facilities and enterprise applications via the Internet from specialized data centers as opposed to hosting and operating those resources on campus (EDUCAUSE, 2009; Johnson, et al., 2010). The anticipated advantage of cloud computing is that each school shares common hardware and support services rather than investing in individually developed sites and applications. At the administrative level, the use of cloud computing applications is becoming increasingly commonplace. Schools use cloud computing for student and faculty schedules, curriculum development, rosters, grade books, e-communication, and administrative collaboration (Johnson, et al., 2010). Cloud computing is also becoming more commonplace in supporting student learning. Some educational leaders theorize that cloud computing promotes 21st Century skills including collaboration (Siegle, 2010) and the ability to

participate in global discussions (Bull & Garofalo, 2010). Columbia Secondary School in New York uses cloud applications to facilitate student work in engineering, English, and debate (Johnson, et al., 2010). North Carolina State University and IBM are working together to provide cloud applications, additional computing power, and storage space to every public school in the state of North Carolina (Johnson, et al., 2010).

As with its stateside schools, the United States government encourages its American Overseas (A/OS) schools to integrate technology into their teaching practices. The American Overseas Schools Advisory Council (OSAC) of the US Office of Overseas Schools (USOOS) has placed increasing emphasis on educational projects that support and increase the use of technology. The OSAC currently requires that all project proposals requesting program support include a technology component. This policy is intended to encourage A/OS schools to use technology in their educational programs (retrieved September 16, 2008 from http://www.state.gov/m/a/os/c6971.htm). AASSA also encourages its member schools to participate in on-line learning opportunities by endorsing such programs as Walden University's on-line College of Education and Leadership courses for faculty members and K12 Academy's virtual courses for students of AASSA member schools.

As American schools strive to meet current recommendations for using technology integration to promote student achievement, school boards and administrators are becoming aware of the need to protect ET hardware, software and their resulting administrative records. School administrators also recognize the need to protect student curricula and performance data and general communication within and outside of the school building. Although several organizations had authored guidelines for business continuity and disaster recovery pertaining to commercial businesses, Ligon and Mangino (2005) found that no one had authored similar

guidelines for schools. However, the National Institute of Standards and Technology (NIST) did release a contingency planning guide with disaster recovery and business continuity recommendations for government and academic organizations (Swanson, et al., 2002). These recommendations have helped some schools to design individualized ET contingency plans based upon the principles of the NIST guidelines and similar documents.

In 2010, Southern University at New Orleans' College of Business released "Contingency Planning: Disaster Recovery Strategies for Successful Educational Continuity (Omar, Udeh, & Mantha, 2010). This project focused primarily upon universities along the Gulf Coast of the United States. It generated a model for successful educational continuity that can be instituted by most educational institutions that wish to pursue the three interdependent objectives of business continuity planning (i.e. identifying major risks of business interruption, developing a plan to reduce the impact of the risks, and implementing, testing, and maintaining the plan).

The Southern University project's ten cyclical steps for meeting the objectives for successful educational continuity require schools to first identify goals and objectives based upon the school's needs. Further steps involve prioritizing the type of data to be stored and the type of backup needed before selecting an off-site storage location. It also involves educating team members and key employees. After schools implement the plan, the guidelines recommend a repeating cycle of testing, reviewing, monitoring, and updating the components. Other steps entail uploading courses to Blackboard or a similar program and maintaining a solid, current contact list. In order to understand the basis and rationale for these guidelines and recommendations a review of the potential threats to technology systems is presented.

Potential Threats to Organizations

An understanding of the potential risks to technology is an important precursor to effective continuity planning. Disaster recovery and business continuity plans typically attempt to protect a technology system from three classifications of threats: natural disasters, human threats, and environmental dangers (Banks, Higgs, Emeagwai, Walters, Guy, 2010; Swanson, et al., 2002). Natural disasters include hurricanes, fires, floods, earthquakes and other phenomena. Human threats include terrorist attacks, human error, and deliberate sabotage. Environmental dangers include power or telecommunications outage, equipment failure, and software error.

Natural disasters present familiar widespread threats to people, buildings, and technology. Unfortunately, some scientists predict an increase in weather-related disasters. For example, in June 2008 the U.S. Climate Change Science Program, which is sponsored by thirteen government agencies, released a report stating that extreme weather such as heat waves, heavy downpours, and super-powered hurricanes will be more common in the near future (Carlson, 2008). In 2005, Hurricanes Katrina, Rita, and Wilma affected more people over a larger area, and to a more profound extent than any previous North American disaster season (American Red Cross, 2006; Henke, 2008). Hurricanes like Katrina devastated hundreds of area schools and colleges (Kiernan, 2005; Rojas, 2006; Villano, 2010).

In February of 2008, Union University near Jackson, Tennessee experienced an extreme weather event. An unpredicted, out of season tornado ripped through the Union University campus, leveling more than a dozen buildings (Ahmed, Bixler, & Payne, 2008; Carlson, 2008; Wood & Yates, 2008). Fortunately, Union University had a well-rehearsed business continuity plan and was able to restore many ET functions within 48 hours. Union drew national attention and praise for its technology crisis preparedness (Union University, 2008). However, if Union

University had not had a business continuity plan for technology valuable data may not have been recovered.

The Caribbean and South and Central America have also experienced recent natural disasters. Early in 2010 two devastating earthquakes affected AASSA schools within weeks of one another. On January 12 a magnitude 7.0 earthquake devastated Haiti. The following month Chile suffered a magnitude 8.8 quake that displaced 1.5 million people (retrieved September 2, 2010 from http://www.nytimes.com/2010/02/28/world/americas/28chile.html?_r=1). Fortunately, the Nido de Aguilas School in Chile suffered only minor damage (Bergman, 2010). However, Haiti's Union School remained closed for several months until engineers could repair all structural damage (Panther Paws, March 25, 2010). Since the disaster the Union School's governors and administrators have altered their approach to safeguarding ET. According to Union School director, Marie-Jean Baptiste:

> (Prior to the earthquake), we did not have a definite (business continuity) plan in place. Our data is backed up manually on an external drive. We use Rediker's services, but they do not do our backup. Our policy simply states that the backup must be done regularly and stored at one of the local banks. This is going to change (post disaster), as many of the banks had problems during the events of January 12. Fortunately, we did not lose data because we had actually backed up data the morning of the 12th….Our new tech coordinator is looking at putting a plan together in the event we find ourselves in a similar situation (personal communication, October 5, 2010).

Union University's tornado crisis and the Union School's earthquake provided dramatic illustrations of vast damage to infrastructure and ET. However, far less dramatic occurrences can also devastate an organization's ET. So-called "quiet catastrophes" (Jarriel & Shomper, 2005)

pose minimal danger to facilities but can destroy the technology of an unprepared organization (Botha & Von Solms, 2004; Henke, 2008; Jarriel & Shomper, 2005; Ligon & Mangino, 2005; Pirani & Yanosky, 2007). Quiet catastrophes include vandalism, a broken water pipe, power failures, computer viruses, and stolen passwords. They are more likely to occur than are natural disasters. A 2007 survey reported that within the past five years, 35% of United States universities have experienced at least one electrical failure that triggered a central ET emergency response (Yanosky, 2007).

In August 2003 a single quiet catastrophe affected the ET of thousands of schools. The Blaster worm caused instability in the remote procedure call (RPC) service on infected systems running Windows programs in schools that were infected. The threat of the Blaster worm forced hundreds of school districts across the United States to shut down their networks (Sieberling, 2005; Trotter, 2003). Several districts across the country elected to delay the opening of schools by at least a week. The delay caused the suspension of e-mail delivery, the scheduling of fall classes, and other computerized functions pertaining to the start of school (Trotter, 2003).

Another quiet catastrophe occurred in 2003 in the form of a major hydro-electrical blackout in the Northeastern United States and most of Ontario that was the result of human error (Barbara, 2006). While power was restored to most locations within twenty-four hours, we do not know how many schools suffered permanent data loss during the power outage. Computer damage can occur within moments of a blackout because memory loss and data corruption occur when the dynamic random access memory (DRAM) ceases to be constantly refreshed (McGrath, 2003). Power outages such as the one in 2003 can also quickly cause systemic hardware damage. A 2008 study showed that a typical data center running at 5,000 watts per server cabinet would experience an automatic thermal shutdown within three minutes and nine seconds of a power

outage because its cooling system is no longer functional (McGrath, 2003). In short, loss of electrical power is the most frequent cause of ET disasters in the K-12 workplace (Ligon & Mangino, 2005; O'Hanlon, 2007).

Business Continuity and Disaster Recovery Planning

Current business guidelines do not provide a detailed blueprint for IT contingency planning. Instead, they offer principles and strategies for organizations to follow as they design and redesign their individual plans for IT continuity and/or recovery. IT continuity and recovery planning is a continuous, dynamic, ongoing process because new technology and applications are created daily (Barbara, 2006; Cerullo & Cerullo, 2006; Kiernan, 2005; Pritchard, 2007; Sieberling, 2005; Swanson et al., 2002). In addition, business continuity planning for IT must be based on the organization's needs, priorities, staffing, skills, budget, and other available resources (Nguyen, 2007). Like businesses, schools have unique situations and technology needs. Some, but not all, of the business world's IT business continuity planning and disaster recovery practices can be applied to schools. These practices include protecting confidential information and processes that affect their core business, namely programs associated with the curricula.

Evolution from Disaster Recovery Planning to Business Continuity Planning

Many people equate disaster recovery planning with business continuity planning (Gregory & Hover, 2007; Savage, 2002; Wan & Chan, 2008). Some of the current literature uses the terms interchangeably (Barbara, 2006). Although the terms share a basic premise, business continuity is a more inclusive and further evolved concept than disaster recovery (Elliot, Schwartz, & Herbane, 2002; Elrod, 2005). Business continuity planning evolved from simple

reactive disaster recovery planning (Elliott, et al., 2002; Pitt & Goyal, 2004; Wan & Chan, 2008) into a comprehensive process designed to avoid or mitigate the risks associated with crisis (Agee & Yang, 2009; Cerullo & Cerullo, 2004; Pirani & Yanosky, 2007). Both business continuity planning and disaster recovery planning help organizations return to their original states of operation following a disaster. However, business continuity planning includes the concept of continuous functioning during a particular disaster (Barbara, 2006; Golden & Oblinger, 2007; Kuzyk, 2007; Nguyen, 2007, Scott, 2008; Yanosky, 2007). The following overview of business continuity planning begins with an explanation of disaster recovery planning.

Disaster recovery planning addresses the reconstruction and retrieving of information following significant damage or destruction (Elrod, 2005). Disaster recovery plans define the resources, actions, tasks and data required to manage the business recovery process in the event that a crisis-induced disaster has disrupted IT operations (Nwosisi & Nieto, 2007). Disaster recovery approaches emphasize "after the fact actions" (Kirchner, Karande, & Markowski, 2006, slide 2) for resuming IT operations following a significant disruption. The term "disaster recovery" emerged in the 1960s and typically referred to plans instituted by large-scale organizations in order to protect their infrastructure from natural disasters (Barbara, 2006). However, as organizations became increasingly dependent upon technology, disaster recovery planning efforts began to emphasize the protection and recovery of computer-based systems (Pitt & Goyal, 2004). Early IT systems were centralized. However, during the 1980s and 1990s, local and wide area networks (LANs/WANs) became the norm in organizations. Globalization and the Internet further broadened the technological capabilities, dependencies, and vulnerabilities of most organizations thereby expanding the risks associated with business and IT interruptions (Cerullo & Cerullo, 2004) and underscoring the importance of IT contingency planning.

Whereas disaster recovery planning helps organizations expeditiously return to their original states of operation, a business continuity plan's objective is to enable the organization to continue functioning during the disaster (Kuzyk, 2007; Yanosky, 2007). Business continuity planning is designed to avoid or mitigate the risks associated with crisis (Cerullo & Cerullo, 2004). In the 1990s, the term business continuity became a popular replacement for the term disaster recovery because contingency planners sought to mitigate vulnerabilities such as network downtime and communication failures that were common to decentralized IT environments during a crisis (http://www.businessresiliency.com/evolution_history.htm). However, business continuity planning did not eliminate the need for disaster recovery. Rather, disaster recovery became widely considered to be a subset of overall business continuity planning (Agee & Yang, 2009; Barbara, 2006; Kirchner, et al., 2006; Kuzyk, 2007; Nguyen, 2007; Swanson, et al., 2002; Wan & Chan, 2008). Eventually, the term disaster recovery came to be used to describe the technological aspect of business continuity planning including traditional data backup and recovery procedures (http://www.businessresiliency.com/evolution_history.htm; Barbara, 2006; Nwosisi & Nieto, 2007).

A business continuity plan addresses three interdependent objectives: identifying major risks of business interruption, developing a plan to mitigate or reduce the impact of the identified risk, and training employees and testing the plan to ensure that it is effective (Cerullo & Cerullo, 2004). In order to meet those objectives, most business continuity plans include five phases of development: analysis, solution design, implementation, testing, and maintenance (Pitt & Goyal, 2004; Nguyen, 2007; Savage, 2002; Wan & Chan, 2008). Although the Southern University project's researchers did not group their ten steps for successful educational continuity into the

five phases, their cyclical model includes and implies the same principles thus providing a framework that schools can adopt (Omar, et al., 2010).

Phase 1: Risk assessment and business impact analysis. The analysis phase involves assessing the potential impact on technology of all unexpected events or disruptions though a process known as risk assessment and business impact analysis (Pitt & Goyal, 2004; Swanson, et al., 2002; Wan & Chan, 2008). The first step involves identifying threats or potential events that could cause technology or facilities to be unavailable or damaged (Savage, 2002). These threats include natural disasters, human-induced errors, and environmental hazards (Swanson, et al., 2002; Wan & Chan, 2008). In 2007, the Disaster Recovery Journal (DRJ) and Disaster Recovery International (DRI) published guidelines for business continuity practices. In order to identify potential threats and the probability of their occurring, DRJ and DRI recommended that organizations engage in the following practices: research past disasters within their geographical area, research past disasters within their industry and related industries, research past disasters internally within their organization, and identify interdependencies to other organizations, systems, and research past disasters within interdependent organizations (Disaster Recovery Journal and DRI International, 2007).

The next step attempts to characterize the consequences of a disruption (Omar, et al., 2010; Swanson, et al., 2002). This analysis helps an organization understand the degree of potential loss that could result from certain technology disasters. Such losses include direct financial loss, damage to reputation, loss of customer confidence (Savage, 2002), and, in the case of schools, disruption to students' learning processes (Ligon & Mangino, 2005).

Business impact analysis identifies those technology functions that are "mission critical" (Barbara, 2006, p. 34), and the impact on operations if a critical resource were to be disrupted or

damaged (Pitt & Goyal, 2004; Scott, 2008; Swanson, et al., 2002). For example, an organization might determine payroll processing to have a high priority to the mission and thus a correspondingly high recovery priority. Similarly, school administrators might ask themselves which technology functions are currently more important than others such as offering online courses or paying members of staff (Kiernan, 2005). Once IT priorities have been determined, the effects of a technology outage must be analyzed in terms of the maximum allowable time that a resource may be unusable before it prevents or inhibits the performance of an essential function (Barbara, 2006; Nguyen, 2007; Scott, 2008: Swanson et al., 2002).

Phase 2: Solution design. The next task is to identify appropriate procedures for preventing incidents or limiting the effects of an incident (Swanson, et al. 2002). Some common relatively inexpensive preventive measures include the use of uninterruptible power supplies (UPSs), generators for backup power, fire suppression systems, smoke detectors, and water sensors. Also, many organizations use plastic coverings or tarps for technology equipment, and fire, heat, and water resistant containers for records and media. Other economical procedures consist of using emergency master shutdown switches; storing backup media, records, and system documents off-site; utilizing technical security controls (e.g. cryptographic key management, least-privilege access controls); and scheduling frequent backups.

Organizations can engage in preventive measures such as those mentioned above without incurring significant expense. However, many optimal business continuity measures entail considerable financial cost (Nguyen, 2007; Scott, 2008). Business continuity planning for schools involves more than simply providing UPSs and backing up computer files at the end of each day (Consortium for School Networking, 2006; Ligon & Mangino, 2005; Omar, et al., 2010; Swanson, et al., 2002). Technology recovery experts recommend, among other things,

vendor agreements, alternate sites, reciprocal site agreements with similar institutions, various data consolidation strategies, and the storing of data in two distinct locations separated by at least 100 miles (Agee & Yang, 2009; Barbara, 2006; Burton, 2004; Foster, 2005; Kiernan, 2005; Nguyen, 2007; Swoyer, 2003; Wan & Chan, 2008). Additionally, technology experts advise organizations to ensure redundancy at every level of equipment, services, data, and personnel (Consortium for School Networking, 2006) and recommend regular testing of business continuity plans (Banks, et al., 2010; Dewey & DeBlois, 2006; Golden & Oblinger, 2007; Savage, 2002; Scott, 2010; Swanson et al. 2002; Trump & Lavarello, 2003; Voss, 2006). Since most schools work within financial constraints these IT priorities help schools determine which business continuity practices will take precedence within their budgets. After these analyses, an organization will have the necessary data to determine the optimum point to recover a technology system if its operations were to be disrupted. The optimum point can be determined by balancing the cost of system inoperability against the cost of resources required for restoring the system (Barbara, 2006; Nguyen, 2007; Scott, 2008).

At the conclusion of phases 1 and 2, the business or school should have a formal plan that is approved and distributed to all critical members of the organization (Banks, et al., 2010). The resulting document, the business continuity plan, should include an organization chart showing names and positions, especially those with specific authority to act in an emergency situation. Emergency contact information for key members of staff, emergency services, vendors, and alternate sites should be included and kept up to date. The plan should also contain maps and floor plans of the premises, evacuation procedures, and fire, health, and safety procedures. Asset inventories, standard operating and administrative procedures, and specifications of key technology and communications systems are equally important. Finally, the plan should include

insurance information, copies of service lender agreements, and details of off-site storage and system restore process (adapted from Pitt & Goyal, 2004; Pirani & Yanosky, 2007; and Savage, 2002).

Phase 3: Implementation. The IT business continuity plan is but one component of an organization's overall contingency planning process. IT contingency plans must be implemented in a way that is compatible with contingency plans from all areas of the organization (Agee & Yang, 2009; Cerullo & Cerullo, 2004; Pirani & Yanosky, 2007; Swanson, et al., 2002; Wan & Chan, 2008). These plans include security-related plans, facility level plans, business resumption plans, and critical infrastructure protection plans (Yanosky, 2007; Swanson, et al., 2002). For example, a recovery strategy that requires key employees to remain on site during a disaster runs the risk of obstructing organization-wide disaster policies relating to the personal safety of employees. However, a policy of regularly backing up data is a no risk preventive strategy that probably will not collide with any other organization-wide policy. Therefore, business continuity planners must frequently coordinate with representatives from other areas of the school or organization in order to remain aware of new or evolving policies or capabilities.

Policies and protocols from other areas of the organization must also support and enforce the procedures that are designated by the business continuity plan. For example, a school or other organization that uses least-privilege access controls must also have strict rules regarding the storing of passwords and a user's ability to read, modify, or access data. Under a least-privilege access a user may be allowed access to view particular documents, but will not have the ability to modify them or create new documents (Armstrong, 2005). Otherwise, a hacker or student might be able to easily infiltrate the system (Fryer, 2003). Similarly, organizations must ensure that

policies are in place requiring employees to backup data each day, use protective tarps to cover equipment, and use storage facilities to protect technology from dangers such as floods or fire.

Another important aspect of business continuity plan implementation involves the training of key personnel. After a system recovery or continuity strategy has been selected, teams must be trained and be ready to respond to any disaster in order to efficiently and smoothly recover the technology system's capabilities and quickly return the system to normal operations (Banks et al., 2010; Cerullo & Cerullo, 2004; Swanson, et al., 2002). This training requires clear communication and a clear delineation of individuals' responsibilities and procedures for communication during a disaster (Banks, et al., 2010; Barbara, 2006; Cerullo & Cerullo, 2004; Pitt & Goyal, 2004; Swanson, et al., 2002). Ideally, continuity and recovery teams will be staffed with personnel responsible for the same operation under normal conditions. However, a disaster could occur that renders a majority or all personnel unavailable to respond. In this situation organizations are recommended to consider using personnel from vendors or from another geographic area of the same organization (Swanson, et al., 2002). Thus, organizations also need to rehearse the continuity plan alongside any external personnel hired as back-ups (Scott, 2008).

Phases 4 and 5:Testing and Maintenance. Business continuity plans require frequent testing (Banks, et al., 2010; Barbara, 2006; Golden & Oblinger, 2007; Pirani & Yanosky, 2007; Savage, 2002; Swanson, et al., 2002; Trump & Laverello, 2003). Smith said, "The three golden rules for [disaster planning] success are (1) testing, (2) testing, and (3) testing" (Smith, 1995, p.21). These experts' advice is not limited to continuity planning for technology, but was intended to apply to the wide spectrum of continuity and disaster planning. The testing scenario may be either a worst-case incident or an incident most likely to occur (Barbara, 2006; Swanson,

et al., 2002). The most common types of emergency testing comprise classroom exercises and functional exercises (Savage, 2002; Swanson, et al.). Classroom exercises are the most basic and least costly of the two types of testing. Participants in classroom exercises walk through the procedures without participating in any actual recovery operations. After walking through the steps of the business continuity plan, participants should test the plan via functional exercises. Functional exercises include simulations and often involve interagency and vendor participation. A functional exercise might include actual relocation to the alternate site and system cutover (Savage, 2002; Swanson et al., 2002). Yet, a 2002 Ernst & Young survey found that 21% of companies with a business continuity plan reported having never tested their plans (Cerullo & Cerullo, 2004). Pirani and Yanosky (2007) found a similar trend among US universities. Only 35% reported conducting tests of their IT business continuity procedures and some of these reported carrying out these tests less than once per year.

Lessons learned during the testing phase should be documented and incorporated into the business continuity plan (Pitt & Goyal, 2004; Scott, 2008; Yanosky, 2007). Many organizations purchase commercial toolkits or checklists that are designed to help with business continuity plan maintenance (Savage, 2002). Two examples are The Disaster Recovery Toolkit which is available at http://www.businesscontinuityworld.com and The Business Continuity Plan Generator which is available at http://www.securityauditor.net/bcp-generator. These commercial toolkits were designed for use by businesses. However, schools can borrow from the toolkits' principles, and adapt the maintenance guidelines and checklists to better suit school system needs and priorities.

Finally, technology contingency plans remain effective if the organization maintains them in a ready state that reflects up-to-date system requirements, procedures, organizational

structure, and policies (Swanson, et al., 2002). Systems undergo frequent changes because of technology upgrades, shifting business needs, or new organizational policies. Therefore, a business continuity plan that is not frequently tested and updated is in danger of becoming obsolete (Barbara, 2006).

Approaches to Meeting the Objectives of Business Continuity Planning

The five phases of business continuity planning seem to occur sequentially and discretely. However, in practice the phases might occur sequentially, simultaneously, or out of sequence (Omar, et al., 2010; Pirani & Yanosky, 2007). Although many organizations follow the phases sequentially some engage in phase 2 activities such as backing up data off-site or using UPSs without ever having gone through the phase 1 practice of conducting a business impact analysis. Some organizations also engage in phase 3 practices without having passed through phase 1. A recent Tennessee State University study of business continuity practices among small businesses in Memphis and Nashville revealed that although 50% had not conducted phase one business continuity practices, nearly 70% engaged in the phase 3 practice of maintaining employee emergency contact information on hand (Banks, et al., 2010). Yanosky's 2006 study of ET business continuity practices among US universities reported that whereas only 17 percent had complete central ET business continuity plans nearly all universities engaged in some ET business continuity practices. According to Pirani and Yanosky:

> An incomplete plan does not necessarily imply the absence of [business continuity] procedures. ….[C]oncerning thirteen different central IT procedures related to business continuity that we asked about, 91 percent of respondents said they had documented at least one procedure, and the median number of documented procedures was eight. Some key procedures, such as those for notifying appropriate parties of an

> emergency and recovering IT operations, were reported either in a plan or as a stand-alone procedure by 75 percent or more of our respondents. Thus, institutions lacking a completed plan may nonetheless have substantial documentary coverage at a procedural level (2007, p.15).

Moreover, some organizations either purposefully or inadvertently engage in simultaneous implementation of two or more phases. The interdependency among phases 3 (i.e. implementation), 4 (i.e. testing), and 5 (i.e. maintenance) make them difficult to separate or arrange sequentially (Elliot, et al., 2002; Cerullo & Cerullo, 2004; Scott, 2008). Pricewaterhouse Coopers' Risk and Business Continuity Services recommended that testing and simulations precede implementation (Scott, 2008). Fullick (2010) advised organizations to replace the term "testing" with "exercising" in order to emphasize the interdependencies and ongoing nature of the business continuity planning process. Fullick abdicated embedding assessment exercises throughout the process rather than waiting until phase 4. In acknowledgement of the cyclical, ongoing nature of business continuity planning some business continuity planning experts have also recommended that phases 3, 4, and 5 be integrated (Agee & Yang, 2009). The Southern University projects' ten cyclical steps for meeting the objectives of successful educational continuity did not break the process into the five phases. Instead, it presented the steps as an ongoing, nonlinear process (Omar, et al., 2010).

Regardless of the approach a thorough business continuity plan must aim to meet the aforementioned objectives of identifying major risks of business interruption, developing a plan to mitigate or reduce the impact of the identified risk, and training employees and testing the plan to ensure that it is effective (Cerullo & Cerullo, 2004).

Current Status of Schools' Contingency Planning for ET

Some school districts such as Henderson County Public Schools in North Carolina engage in in-depth business continuity planning for ET. Henderson County's business continuity plan included a vendor agreement with IBM and thorough procedures for minimizing ET data loss. Henderson County's plan also included detailed steps, alternate locations, and individual responsibilities to be implemented in case of ET emergency (Henderson County Public Schools, 2005). However, researchers encountered difficulty when trying to determine how many school districts were engaging in ET continuity planning similar to that of Henderson County. O'Hanlon (2007) found that enterprise business continuity spending for all US businesses totaled $15.1 billion in 2006 and is estimated to reach $23.3 billion in 2012. No such figures are available for K-12 schools (O'Hanlon, unpaginated digital version). However, several school administrative software companies now offer off-site data backup to their client schools. Companies such as Rediker Software, Power School, and Atlas Curriculum Mapping provide both US and overseas schools an opportunity to store data off-site thereby offering a safeguard for ET regardless of the extent of a local disaster.

However, O'Hanlon (2007) reported examples of many school districts that did not adopt formal business continuity plans for ET until after being affected by a disaster. For example, the Nederland Independent School District in Texas had no formal disaster recovery or business continuity plan prior to Hurricane Rita in 2005. After suffering over $10 million in damage to buildings, infrastructure, and ET, the district adopted a business continuity plan that included preventative strategies such as storing mail servers off-site (O'Hanlon, 2007). Many Florida schools had learned similar lessons a year earlier when Hurricane Charley caused $300 million in

damage to Charlotte County schools including the destruction of $2 million worth of ET infrastructure (O'Hanlon, 2007).

Similarly, many universities are unprepared (Kiernan, 2005). For example, a 2004 fire at Eastern Illinois University gutted a structure that housed African-American studies, the Graduate School, grants and research, minority affairs, the School of Adult and Continuing Education, the university's general counsel, and the department of sociology and anthropology (Foster, Hendrickson, & New Freeland, 2006). Prior to the fire the university had neither a remote server nor a policy of requiring faculty and administrators to save backup files at an alternate location. As a result, the university experienced an immeasurable, irreversible loss of intellectual property, faculty data, research agendas, and various collections (Foster, et al., 2006). In 2005, the ET operations of Lynn University in Florida were thwarted for over two weeks following Hurricane Wilma. After their "eye-opening experience" (Boniforti as quoted by Villano, 2009), Lynn administrators made the development of a business continuity plan a priority although it came at a considerable expense (Villano).

Lack of funding is reported as the primary barrier to business continuity planning among colleges (Golden & Oblinger, 2007, p.11; Yanosky, 2007). A 2004 Campus Computing Project survey of American colleges found that while 56% of all colleges have ET disaster recovery plans or business continuity plans, only 40-42% of private colleges are estimated to have such plans (Kiernan, 2005). The survey did not assess how detailed the plans were or whether the colleges had tested them. However, since disaster recovery planning is a component of business-continuity planning this survey indicated that many private colleges probably have no business continuity plan for technology. In 2006, Yanosky's study of business continuity planning practices among US universities yielded similar results. Nearly 70% of the respondents reported

that their universities lacked the necessary funding to provide technology support for business continuity planning.

Yanosky (2007) found that most US tertiary institutions engaged in some business continuity practices for ET with the most prevalent being the backing up of data. However, the practices tended to occur as resources and contingencies permitted rather than as part of formal plan. Those who said that business continuity planning was a work in progress comprised the largest response group. Only one in ten respondents indicated that their institutions had completed a risk assessment or institutional business continuity plan. Nearly all respondents reported that their institutions planned to create an ET business continuity plan.

Yanosky (2007) found that only 16% of respondents had an alternate hot or cold site beyond a five-mile radius of campus. Slightly over half of respondents reported having back up power sources such as generators, however only 20% had redundancy in place. The researchers also determined that most respondent institutions did not regularly communicate business continuity awareness issues to their constituents or test technology readiness to support business operations during a disruption. Nevertheless, half of the respondents indicated that their institutions had experienced at least one disruption within the past five years that had triggered a central IT emergency response, with electrical and hardware failures being the most common triggering events.

Cloud Computing

Cloud computing provides an alternative for the numerous organizations that lack adequate funding to support alternate sites, distant data storage facilities, and other recommended business continuity practices. In recent years, cloud computing has become increasingly an option of choice among educational institutions. Cloud computing encompasses any

subscription-based or pay per use service that, in real time over the Internet, extends IT's existing capabilities (Knorr & Gruman, 2008). Cloud computing provides a means whereby a school or university can increase capacity or add computing capabilities very quickly (Knorr & Gruman, 2008). Some experts believe that cloud computing can provide schools and universities an opportunity to trim costs by eliminating the need to purchase new software, to create new infrastructure, and to train personnel to install and operate the latest programs (Johnson, et al., 2010, Knorr & Gruman, 2008; Siegle, 2010). However, other experts feel that cloud computing will result in additional costs that include "hidden expenses that have not yet become apparent" such as those associated with security, policies, monitoring, and bureaucratic processes (Taggart, 2011).

Cloud computing resources include applications, development platforms, and massive computing resources (i.e. software or storage platforms that are too large and complex for many organizations to support in-house). The first group, applications, uses the cloud for processing power and data storage that increases the efficiency of programs such as word processors, presentation applications, graphics, and collaborative spreadsheets (Bull & Garofalo, 2010; Johnson, et al., 2010; Siegle, 2010). Applications that offer inexpensive online storage include Dropbox and Flickr. The second group, development platforms, provides the infrastructure and computing power necessary to support applications (Johnson, et al., 2010). Google App Engine, Heroku, and Zoho are examples of development platforms that allow users to create and host locally designed programs. The third group, computing resources, functions without a development platform layer. GoGrid and the Elastic Compute Cloud provide reasonably priced processing and storage capacity in order to support intensive and collaborative research tasks (Johnson, et al., 2010).

Although cloud computing's use has increased among schools and universities, many of these institutions are reluctant to embrace it as a means of backing up data and ensuring business continuity. Some educational leaders have expressed concerns about privacy, security, data integrity, and intellectual property management (EDUCAUSE, 2009). On April 21, 2011, Amazon's Elastic Compute Cloud suffered an outage in excess of ten hours that "caused a lot of pain for customers," resulting in a "black eye" for the cloud computing industry (Bajarin as quoted by Johnston, 2011, unpaginated digital version). In addition, some business continuity planners have expressed concerns that using cloud computing resources for word processing, data storage, and other applications might unintentionally violate the terms of local laws or the organization's software agreements. For example, the European Union has laws that strictly regulate the movement of data and access to data bases (Plant, 2011). Thus, many institutions are reluctant to relinquish control of their online security to external sources. However, other institutions argue that cloud services "offer more security than on-campus solutions, given the complexity of mounting an effective IT security effort at the institutional level" (EDUCAUSE, 2009, unpaginated). The US government expressed confidence in the security of cloud computing in February 2011 when the White House issued a document outlining a government-wide strategy to adopt cloud computing within the federal government (Hoover, 2011). The developing best practices for cloud computing include mitigating and distributing the risk by employing multiple clouds rather than a single cloud resource for all of a school's applications (Taggart, 2011).

Challenges for Overseas American Schools

Overseas American schools face many of the same ET business continuity challenges as stateside schools and universities, including threats from natural disasters, hackers, and

unintentional human error. However, overseas American schools must often cope with additional challenges unique to the regions in which they are located. Overseas American schools are often located in countries with substandard electrical and communications infrastructure, unstable governments, heightened security concerns, and the lack of a core set of vendors to maintain IT systems that will limit their recovery options. Within the AASSA region, schools have experienced earthquakes, flooding, and political instability. Many AASSA schools also have limited budgets for business continuity planning because they are private, and tuition driven with no endowments. (Golden & Oblinger, 2007; Kiernan, 2005; Nguyen, 2007). Nevertheless, schools regardless of their budget should be engaged in some form of business continuity or disaster recovery planning.

AASSA-member and other overseas American schools do not belong to a school district or consortium. Instead, they are independent and self-governing (Chojnacki, 2007). American overseas schools are typically governed by a Board whose members are elected by the parent association, appointed, or self-perpetuating. The Board is responsible for hiring the school's director or superintendent, developing broad policies, planning for future development and sustainability, and ensuring financial stability (Ambrose, 2003). The Board is also responsible for developing policies pertaining to business continuity planning. However, the school's director typically bears the responsibility of supplying the board with budgeting and other recommendations including those that pertain to ET and business continuity. In addition, the United States departments of Defense and State operate or assist more than 300 schools in over 100 foreign countries. However, more than 600 private American owned or supported schools exist outside of the Department of Defense (DoD) and Department of State (i.e. A/OS) networks

(retrieved April 25, 20011 from http://www.aoshs.org). The sample for this study includes no DoD schools, however, it includes 29 A/OS schools.

The United States Office of Overseas Schools (USOOS) provided A/OS schools with guidelines and recommendations for creating site-specific emergency handbooks and crisis plans (OSAC-funded Emergency Procedures Handbook, 2006). These recommendations emphasized the physical and emotional safety of students and members of staff. They also recognized the need for safeguarding records and quickly resuming normal school operations. The USOOS' guidelines urged A/OS schools to incorporate the "Threat Assessment and Intervention" sections into their Crisis Response Plans. The guideline's objectives included saving lives, safeguarding school property and records, promoting a fast, effective reaction to coping with emergencies, and restoring conditions back to normal with minimal confusion as promptly as possible (OSAC-funded Emergency Procedures Handbook, 2006, unpaginated digital version).

These guidelines did not provide specific recommendations for how school records should be safeguarded or how normal conditions should be promptly restored. Instead, these recommendations advised that each A/OS school develop a Crisis Response Plan that is "site specific" (OSAC-funded Emergency Procedures Handbook, 2006) and designed for efficient business continuity. Thus, each school that follows these USOOS' guidelines should be analyzing and evaluating its ET assets. The school should be prioritizing those assets, and determining what portion of the school's budget can be devoted to business continuity planning.

Purpose of Study

The purpose of this study was to investigate ET business continuity practices among schools that belong to AASSA. This study also investigated whether variables such as a school's size, previous ET disaster experiences, and classification as an official A/OS school were related

to the extent to which the school engaged in business continuity practices. Finally, this study examined the impetuses and obstacles to effective business continuity planning. Prior to this study, little or no research had been conducted pertaining to the business continuity or disaster recovery practices that occur in overseas American schools. However, Yanosky's 2006 study of business continuity practices among US tertiary institutions and the 2004 Campus Computing Project survey of technology administrators at US colleges and universities (Kiernan, 2005) laid groundwork for studying such practices in an educational setting.

Correlates to Business Continuity Planning for ET

The work of Yanosky (2007), O'Hanlon (2007), and Kiernan (2005) suggested that three variables may relate to a school's engagement in business continuity practices for ET. First, Yanosky's study found an association between an institution's size and its ET business continuity planning status. "Institutions of 4,000 or fewer were only about half as likely to report a completed plan as larger institutions….[Larger institutions] were substantially more likely to report a plan in progress; 63.9% versus 45.7% (Yanosky, 2007, p. 59). Thus, the Business Continuity Planning for IT instrument (BCPIT), which was designed for this study, was used to determine whether a school's size affected its business continuity planning for ET.

Second, Yanosky found that half of the respondent institutions in the study had experienced disruptions in the past five years that triggered ET emergency responses, with the most common being electrical failure. O'Hanlon (2007) reported examples of many school districts that did not adopt formal business continuity plans for ET until after being affected by a disaster. Consequently, this study investigated whether schools that have experienced previous IT catastrophes were more likely to engage in ET business continuity planning.

Third, the 2004 Campus Computing Project survey found that private colleges and universities were less likely than state or government supported universities to engage in business continuity planning for ET (Kiernan, 2005). Although all AASSA schools are private institutions, 28 of them are official A/OS schools. A/OS schools receive United States government support and are encouraged to adhere to specific guidelines, including those for overall disaster recovery or business continuity. Therefore, this study also sought to determine whether those AASSA schools that are also A/OS schools engaged in more ET business continuity planning than non- A/OS schools.

Yanosky's survey also asked respondents to identify the barriers to and drivers of business continuity planning. Respondents reported a lack of adequate funding as the primary barrier to engaging in business continuity planning. The top three drivers of business continuity planning among responding institutions were: keeping current with generally accepted business directions and best practices; audit requirements; and awareness of recent global disasters (p. 36). By using several questions from Yanosky's survey instrument, this study identified the triggers of and barriers to business continuity planning for ET among schools in the target population.

Thus, the research questions for this study were as follows:

1. Which of the recommended ET business continuity practices did AASSA schools engage in?
2. Was the size of a school related to its ET business continuity practices?
3. Was a school's previous disaster experience related to its ET business continuity practices?
4. Was a school's A/OS status related to its ET business continuity practices?

5. What were the impetuses and obstacles to ET business continuity planning among AASSA schools?

Chapter 2

Method

Participants

The target population for this study was all AASSA member schools. As of the 2010-2011 academic year, AASSA's membership comprised 43 full member schools and 15 invitational member schools. These 58 schools ranged in student population from over 2,500 at The American School Foundation, A.C. of Mexico City to only 15 at Freeport Mining Schools in Chile. The AASSA member schools included in this study are located in the following countries: Argentina, 1; Bolivia, 3; Brazil, 13; Chile, 2; Colombia, 7; Costa Rica, 1; Ecuador, 6; Guatemala, 1; Guyana, 1; Haiti, 1; Honduras, 3; Jamaica, 1; Mexico, 1; Netherlands Antilles, 1; Nicaragua, 1; Panama, 2; Paraguay, 1; Peru, 2; Trinidad and Tobago, 1; Uruguay, 1; and Venezuela, 7 (see Appendix A). The US Department of State recognizes 28 AASSA schools as official A/OSs. Thirty-nine out of 58 AASSA member schools participated in the Business Continuity Planning for IT (BCPIT) survey for a response rate of 67%. Of the persons completing the survey, 97% indicated that they were personally involved in decisions pertaining to business continuity planning at their schools. The 39 respondents were heads of school (11), technology directors (8), IT managers (6), technology coordinators (5), a technology consultant, an information systems director, and a quality assurance director. Six respondents declined to state their job titles.

Instrument

The BCPIT was designed specifically for this study. The BCPIT (Appendix B) consisted of 32 questions correlated to the five phases of IT business continuity planning and the three interdependent objectives, i.e. identifying major risks of business interruption, developing a plan

to mitigate or reduce the impact of the identified risk, and training employees and testing the plan to ensure that it is effective (Cerullo & Cerullo, 2004). The BCPIT also posed questions about triggers of and barriers to business continuity planning for IT among AASSA schools.

The BCPIT's items were derived from Yanosky's "IT Readiness for Business Continuity" survey instrument (2006) (Appendix C). Yanosky conducted his survey as part of an EDUCAUSE Center for Applied Research (ECAR) initiative and in response to the disastrous hurricane season of 2005. He designed the study to inform university and college administrators about the ways in which institutions approached business continuity issues. Yanosky developed his survey instrument in consultation with "a select group of [Chief Information Officers] and business continuity experts" (2007, p.12). Yanosky and his team "reviewed the relevant standards, interviewed [business continuity] consultants and [Chief Information Officers] who had an interest in the subject, and read through both practitioner and academic research" in order to identify pertinent questions for their instrument (R. Yanosky, personal communication, February 28, 2011).

Yanosky's instrument comprised 11 sections and took 30 to 40 minutes to complete. The sections were entitled: About You and Your Institution; Institutional Perspectives on Business Continuity Planning; IT Perspectives on Business Continuity Planning; Recovery Objectives; Awareness and Training; Business Continuity Testing; Business Continuity Infrastructure and Technologies; Incident Management; Incident Experience and Effects; Funding; and Outcomes. The items included multiple choice and open-ended questions. Although the BCPIT collected some of the same data as Yanosky's "IT Readiness for Business Continuity Survey," it was modified to achieve the purposes of this study. Yanosky surveyed Chief Information Officers at colleges and universities within the United States. For this reason many of the items did not

necessarily apply to AASSA schools. Adjustments were made to the wording to make the BCPIT suitable for the context of K-12 or K-8 international schools. The BCPIT did not include those items that pertained exclusively to colleges and universities nor did it contain those items that were not relevant to this study's research questions. However, the format and style of the questions were not altered. In addition, the BCPIT included four items that referred to cloud computing, an alternative that was rarely used by universities and schools in 2006 when Yanosky conducted his study (Johnson, et al., 2010).

The items in the BCPIT followed approximately the same sequence as that of the "IT Readiness for Business Continuity" survey. However, the BCPIT is a considerably shorter instrument and required approximately 12 minutes to complete. Appendix D presents a table that shows the BCPIT item number that corresponds with each IT Readiness for Business Continuity item. This table also indicates which items were excluded from the BCPIT or modified from the original. Table 1 presents the 32 survey items presented in seven sections along with a brief description of each section.

The validity of the BCPIT paralleled that of Yanosky's instrument since the structure of the questions was not altered. When developing the IT Readiness for Business Continuity Survey instrument Yanosky "reviewed the relevant standards, interviewed business continuity consultants and Chief Information Officers who had an interest in the subject, and read through both practitioner and academic research looking for hypotheses and points to ask about" (R. Yanosky, personal communication, February 28, 2011). In addition, Yanosky presented drafts of his instrument to university chief information officers and corporate business continuity consultants for review. As an extra measure, a pilot study was conducted using the BCPIT. Participants consisted of five heads of A/OS schools outside of the AASSA region. The

Table 1
The Seven Sections of the BCPIT

Section	Title	Description
One	School's Approach to Business Continuity	Pertains to school's attitudes and approaches toward business continuity planning in general; the items follow a multiple choice format
Two	Risk Assessment	Pertains to school's formal and informal risk assessment activities, processes, and plans; items 3-6 follow a multiple choice format; item 7 comprises three questions that are presented in a yes/no format
Three	Formal Written Plans for Business Continuity	Pertains to the business continuity practices that occur formally and informally; items 8 through 10 are yes/no response questions; item 11 comprises thirteen questions that are presented in a yes/no format;; item 12 follows a multiple choice format;
Four	Testing, Training, and Maintenance	Pertains to the types of business continuity tests that occur and the catalysts to testing; items 13 and 14 are presented in a yes/no response format; items 15 and 16 are presented in a Matrix of Choices* format and comprise ten questions
Five	Alternate Sites	Pertains to hot sites, cold sites, cloud computing, and approaches to central IT data storage and recovery procedures; items 17 through 22 and 24 through 26 are presented in a multiple choice format; item 23 comprises six items presented in a Matrix of Choices* format
Six	Incident Exposure	Pertains to IT disruptions that have occurred within the past five years; item 27 is presented in a yes/no response format; item 28 comprises 16 items presented in a Matrix of Choices* format; items 29 and 30 are presented in a multiple choice format
Seven	Demographic data	Three short answer questions

Note. A Matrix of Choices format is similar to a rating scale, however it does not calculate a rating average.

participants provided feedback about the clarity of the BCPIT's instructions, the relevance of its questions, and the amount of time required to complete it.

Scores for business continuity planning. Question 11 of the survey instrument asked respondents to state "yes," "no," or "I don't know," concerning whether 13 activities associated with business continuity were being performed in their schools. For each activity, a "yes" response was assigned a value of 1 whereas "no" and "I don't know" responses were assigned a value of 0. The values from the 13 activities were summed to yield an overall score of business continuity ranging from 0 to 13.

Categories of previous disaster experience. For the variable, "previous disaster experience," each respondent school was placed in one of four categories based upon the responses to items in the Incident Exposure section of the BCPIT (i.e. section 7). Section 7 required respondents to identify any disruptions to IT that had occurred at their schools within the past five years. Respondents had fifteen categories of responses to select from (e.g. flood, electrical failure, cyber attack, etc.). The sixteenth selection allowed the respondent to provide a description of a disaster that might not have been included in the list. This section also required respondents to rank the impact of those IT disruptions that they identified. The final item in section 7 consisted of an open response item that requested respondents to briefly describe the disruption that had the most serious impact and to explain the school's response to it. The respondents provided data about the degree of disruption that occurred by placing the disaster in one of four categories based upon its impact. The four categories were: impact on a few processes; impact on many processes; campus-wide impact; campus-wide and regional impact. These four categories were coded from 1 to 4 respectively; 0 indicated that the school had experienced no disruptions to IT within the past five years. Only the disaster that the respondent

identified as having had the most serious impact on IT processes was considered when determining the school's placement among categories 0-4 of previous disaster experience.

Procedure

AASSA's executive director Poore announced the upcoming study via email to all heads of AASSA schools and asked for their voluntary participation in the BCPIT. Afterward, an invitation and the link to the BCPIT were forwarded to each head of school. The head of school had the choice of completing the survey or designating someone with extensive knowledge of the school's IT to respond on his or her behalf. Only one response per school was used.

Data Analysis

For the variable "size of school," the approximate student population for each school was determined based upon school demographic information provided by AASSA. AASSA's demographic data presented each school's student population rounded to the nearest 50 (see Appendix A). A t-test and Pearson correlation were calculated to assess the relationship between the school's size and its business continuity score. A Levene's test was conducted to ensure that the variances for the three groups of previous disaster experience (i.e. no impact/minor impact, moderate impact, and severe). After the Levene's test confirmed that the variances for the three groups were not different, a Tukey's HSD test was calculated between the schools' assignment to one of the categories of disruption and the business continuity scores, thereby providing data about the relationship between schools' IT disruption history and the number of business continuity planning for IT procedures that occurred. For the variable "A/OS status," each respondent school was categorized as either an A/OS school or non-A/OS school. An independent samples t-test tested the mean differences between A/OS and non-A/OS schools and

their business continuity scores. An alpha level of .05 was set for all statistical procedures. For the final research question, summary descriptive statistics provided data about the impetuses and obstacles to business continuity planning among respondent schools. Both relative and absolute frequency distributions provided data pertaining to the rate of occurrence of each practice.

Chapter 3

Findings

Question 1: Which of the recommended IT business continuity practices do AASSA schools engage in?

Of the 39 schools that responded, 32 (82%) agreed or strongly agreed that business continuity planning for IT was a priority at their school whereas 7 (18%) disagreed or strongly disagreed. Sixteen (41%) of the respondent schools reported having a formal, documented plan for business continuity of which only five had a formal process in place for updating the plan. However, 17 (44%) respondents stated that their schools did not have a formal business continuity plan nor did they intend to create one.

Most schools, including those that lacked a formal business continuity plan, reported engaging in at least some of the recommended business continuity practices. Table 2 lists the frequencies, from the highest to the lowest, for thirteen business continuity procedures that respondent schools reported conducting. The most frequently mentioned procedure was notifying appropriate parties of emergencies (59%). Twenty-one schools (54%) had procedures for the recovery of IT operations following a disruption. A majority of schools also had procedures for prioritizing systems for purposes of recovery (n = 19; 49%) and notifying constituents of system status (n = 18; 46%). The least frequently mentioned business continuity practice was providing transportation for logistical support staff at alternate sites.

In preparing for an emergency, seven schools (18%) reported having conducted a risk assessment; however, only three of these schools reported that their risk assessments were kept up to date. Of the remaining 32 schools, ten indicated that risk assessments were in progress and nine stated that risk assessments were planned. Twelve schools reported that no risk assessment

Table 2
Frequency and % of Responses to the Question: Has Your Central IT Unit Documented Procedures for the Following? (*n = 39)*

	Yes		No		Not certain	
	f	*%*	*f*	*%*	*f*	*%*
Notifying parties of emergency	23	59	12	31	4	10
Recovery of IT operations	21	54	13	33	5	13
Prioritizing systems for recovery	19	49	14	36	6	15
Notifying constituents	18	46	17	44	4	10
Declaring return to normal	16	41	19	48	4	10
Activating/escalating response	15	38	19	49	5	13
Declaring an IT emergency	14	36	21	54	4	10
Performing damage assessments	13	33	19	49	7	18
Evaluating post-recovery environment	10	26	24	62	5	13
Moving activities/equipment to alternate sites	9	26	25	74	5	13
De-escalation of emergency response	9	26	26	74	4	10
Return activities/equipment to primary locations	7	20	27	77	6	15
Transportation for logistical support at alt. site	5	13	30	77	4	10

was anticipated. Among the schools with risk assessments in progress or planned, the following actions were taken: five, a completion date assigned; seven, staff members assigned to the task; one, funds allocated to the project; and one, the school's business units were participating. Furthermore, 22 schools had plans or processes for identifying the probability of disruptive events or threats, 15 had procedures to assess the potential impact of disruptive events on business and academic processes, and 12 had prioritized their risks to IT.

In terms of protecting their software and databases, four respondent schools had fully operational hot sites and five had fully operational cold sites. However, all respondents reported engaging in the recommended practice of storing data. Table 3 presents the data storage procedures that are used, typically some form of backup on or off campus.

Table 3
Frequency and % of Responses to the Item: Describe Your School's Current Approaches to Central IT Data Storage and Recovery. (*n = 39)*

	Not used		Used for some systems		Used for many systems		Used for all systems	
	f	*%*	*f*	*%*	*f*	*%*	*f*	*%*
Backup to media on campus	1	2.5	4	10.0	12	30.7	14	35.8
Backup to media off campus	13	33.3	4	10.2	10	25.6	3	7.6
Continuous data mirroring	19	48.7	5	12.8	3	7.6	2	5.1
Redundant systems with failover	19	48.7	4	10.2	5	12.8	2	5.1
Backup to a cloud	17	43.5	9	23.0	1	2.6	1	2.6
Batch electronic vaulting	22	56.4	3	7.6	2	5.1	1	2.6

Beyond planning and having options for backups, only three (8%) reported engaging in rehearsals and tests of IT readiness for supporting business continuity. Only one school reported that such tests and rehearsals occur on a regular basis. Twenty-five (64%) reported that their schools have no process for training IT staff about overall business continuity plans and procedures.

Question 2: Is the size of a school related to its IT business continuity practices?

BCP scores ranged from a possible minimum of 0 to a possible maximum of 13 (M = 5.0, sd = 4.1); (population < 600, M = 4.1, sd = 4.0); (population > 600, M = 6.0, sd = 4.1). The Pearson correlation between school size (enrollment) and BCP scores was .001 (*ns*). Similarly, the t-test between school size (enrollment) and BCP scores was t = 1.80 (*ns*).

Question 3: Is a school's previous disaster experience related to its IT business continuity practices?

No respondent schools reported having had a severe disruption to IT and operations within the past five years. However, schools reported disruptions having an impact of differing magnitudes as follows: 32% minor impact or no IT disruptions within the past five years; 37% moderate impact; 32%, substantial impact. Twenty-five schools experienced more than one disaster. Table 4 presents the frequency of each type of disruptive event and the severity of the event's impact on school operations. Electrical failure (n = 20; 51%) and hardware failure (n = 19; 49%) were the most frequently mentioned causes of IT disruption among respondent schools. No respondent selected events such as hurricane, tornado, fire, hazardous material spill, or terrorism. Although events having a regional impact were infrequent, respondents mentioned nine such occurrences.

Separate one-way ANOVAs were calculated between the schools' assignment to one of the categories of disruption (none/minor, moderate, and severe) and their business continuity scores. Table 5 presents the mean BCP scores by category of previous disaster experience. No significant differences were found between the means for the BCP scores (F = 0.2, *ns*).

Question 4: Is a school's A/OS status related to its IT business continuity practices?

Eighteen A/OSs and 12 non-A/OSs responded to the BCPIT. Nine respondents did not provide their school's A/OS status. No significant differences were found on the BCP scores (t = .58, *ns*) between A/OS (M=5.3, sd= 4.1) and non A/OS (M= 4.5, SD= 4.4).

Table 4

Number of Schools Reporting Specific Disruptive Events and the Extent of Impact of the Disruptive Events. (*n = 39)*

Type of Event	Few Processes	Many Processes	Campus-wide Impact	Regional Impact
Hardware failure	12	5	2	1
Electrical failure	7	1	7	4
Severe weather	1	2	4	1
Disease outbreak	8	0	0	0
Cyber attack	7	1	0	0
Cable cut	1	4	2	0
IT environmental failure	4	2	1	0
Flood	2	0	2	1
Seismic event	2	0	0	1
Theft	2	0	0	1

Note. Twenty-five respondents reported having experienced more than one disruptive event.

Table 5
Mean BCP Scores by Category of Previous Disaster Experience and F-test Results (*n = 38)*

Severity of Disaster	*n*	*Mean*	*sd*
No disaster/Minor impact	12	4.7	4.4
Moderate impact	14	4.9	3.7
Substantial/Severe impact	12	4.6	4.6
Total	39	4.7	4.0

Question 5: What are the barriers and impetuses to IT business continuity planning among AASSA schools?

Twelve respondents indicated that their schools had no plans to engage in risk assessment activities. Of these twelve, seven stated that the threats to their school's business continuity do

not justify the effort of conducting a risk assessment. Three respondents cited each of the following barriers to conducting a risk assessment: lack of institutional leadership support; undefined needs; lack of staff expertise; and difficulty developing campus policies and procedures. Two reported that the benefits of a risk assessment did not justify the investment and/or that their schools preferred an ad hoc approach to business continuity planning. Only one school reported that inadequate funding was a barrier to conducting a risk assessment.

Table 6 shows that 35.9% of respondents indicated that the primary barrier to business continuity planning was that business or academic units had not defined their business continuity needs. The next most common barrier was a lack of staff expertise (33.3%) followed by difficulty developing campus policies and procedures (28.2%). Inadequate leadership or funding presented business continuity barriers to only 15.3% and 17.9% of responding schools respectively.

Two participants reported having a fully functional hot site and four reported having a cold site capable of assuming key IT operations if the primary site were compromised. Of the remaining respondents, 50% reported that their schools had no plans to develop a hot site. Nearly 56% reported that their schools had no plans to develop a cold site. The primary barrier to schools' developing a hot site was the belief that the benefit would not justify the expense. The same reason was one of the two most frequently cited barriers to schools' developing a cold site.

Two-thirds of respondents reported that keeping current with best practices was a driver of business continuity planning. Approximately one-third stated that demand from constituents, threats specific to the geographic location, and/or school leadership mandates as drivers.

Table 6
Barriers and Impetuses to Business Continuity Planning

	f	*%**
Barriers to school wide business continuity planning (*n* = 39)		
Business/academic units have not defined BC needs	14	35.9
Lack of staff expertise	13	33.3
Difficulty developing campus policies/procedures	11	28.2
Lack of acceptable return on investment	9	23.0
Technology issues	8	20.5
Lack of adequate funding	7	17.9
Lack of leadership support	6	15.3
Barriers to developing hot sites (*n* = 16)		
Do not believe benefit justifies expense	9	56.3
Do not believe a hot site is necessary	7	43.8
School is not far enough along in BC planning	6	37.5
Lack of adequate funding	4	25.0
Lack of leadership support	3	18.8
Lack of staff resources	2	12.5
Lack of staff expertise	1	6.3
Barriers to developing cold sites (*n* = 17)		
Do not believe benefit justifies expense	9	52.9
School is not far enough along in BC planning	9	52.9
Do not believe a cold site is necessary	5	29.4
Lack of adequate funding	4	23.5
Impetuses to school wide business continuity planning (*n* = 39)		
Keeping current with best practices	26	66.6
Demand from constituents	14	35.8
Threats specific to geographic location	12	30.7
School leadership mandate	12	30.7
Recent global natural disasters	11	28.2
Audit requirements	9	23.1
Hazards arising from school's operations	7	17.9
Recent incident at school	5	12.8
Terrorism/security concerns	4	10.3
Regulatory compliance	2	5.1
Other	2	5.1

Note. Column total does not add up to 100% because respondents could select up to three responses

Chapter 4

Discussion

External Drivers and Internal Impediments

International schools are vulnerable to ET threats, yet research on technology-related educational leadership issues is "nearly nonexistent" (McLeod, 2011 p. 3.) This study serves as an initial step to describe the business continuity practices of American international schools. The results indicated that in regard to business continuity planning for ET, AASSA schools encountered similar impetuses and obstacles regardless of their size, A/OS status, or previous disaster history. If these three factors did not influence business continuity planning among AASSA schools, what factors were said to make a difference? The primary drivers of business continuity planning were derived from external factors, i.e. sources that existed outside of the school's governance and organizational structures. Respondents (n = 39) reported that the four top drivers of business continuity planning were: keeping abreast of recommended business practices (n = 26; 67%); demands from constituents (n = 14; 41%); threats specific to geographic location (n = 12; 35%); and school leadership mandates (n = 12; 35%). Thus three of the four primary drivers of business continuity planning were rooted in sources external to school operations.

In contrast, the barriers to effective business continuity planning were derived from internal factors; sources within the school's governance and organizational structures. The top three barriers were: business or academic units had not defined their business continuity needs (n =14; 41%); lack of staff expertise (n =13; 38%); and difficulty developing campus policies and procedures (n = 11; 32%). Thus, the primary barriers to effective business continuity planning encompassed impediments that school leaders have the capacity to address.

Two important understandings emerged from the realization that business continuity planning tended to be driven by external factors and impeded by internal ones. The first is that, as a collective body, school stakeholders did not feel impelled to engage in business continuity planning or recognize business continuity as being essential to a school's growth or sustainability. In other words, business continuity planning was not perceived as being mission-critical. The second implication is that regardless of size, A/OS status, or previous experiences, much of the capacity to remove barriers to effective continuity planning existed within the school's leadership, internal governance, and organizational structures. Given the findings of this study, educational leaders should become aware of several critical concepts in order to promote schools' optimal engagement in effective continuity practices.

Business Continuity as Mission Continuity

ET has become integral to all aspects of a school's successful operation including administrative and instructional functions. Without a fully functioning ET system, schools lose vital communications networks, access to educational resources such as textbooks and supplementary instructional materials, and records that include student test scores, budgets, and Board minutes. Yet many educators continue to subscribe to the misconception that ET and business continuity are peripheral to a school's mission and solely the responsibility of technology and office personnel (Sieberling, 2005; Trecek, Trobec, Pavesic, & Tasic, 2007; Williams & Krueger, 2005). In contrast, experts in the field of business continuity planning have strongly advocated that educational leaders take an active, purposeful role in embedding business continuity practices into a school's culture, mission, and organizational structure (Association of Governing Boards of Universities and Colleges, 2009; Business Continuity Institute, 2008; Fischman, Carlson, & Young, 2009; Hartman, 2008; Ligon, 2006; Williams & Krueger, 2005).

Accordingly, leaders must take steps to ensure that school stakeholders perceive business continuity as being integral to protecting and sustaining the school's mission.

Fulfilling the school's mission is a shared responsibility that spans all members of the community. According to Fayad, most authors have defined mission as, "'what we, as an organization are all about,' 'why we exist,' and 'what we do'" (2011, p. 3). Schools have long recognized that a mission statement can be a powerful instrument for giving the entire community a sense of shared purpose, direction, and accountability. When business continuity becomes interconnected with a school's mission, teachers and other stakeholders will be more likely to acknowledge their collective responsibility for protecting the data and ET systems that support the mission (Hartman, 2008). A school cannot sustain its mission without the ET that supports it.

In his books and articles regarding preparing for threats to operations at universities, Qayoumi used the term mission continuity rather than business continuity. Schools should consider adopting Qayoumi's terminology as way of emphasizing both the "mission criticality" (Decker & Thamer, 2008) of continuity planning and the importance of the participation of all school departments, not just those associated with business or ET. Institutions such as the University of Pennsylvania and California State University are already doing so. The simple shift in terminology may pique the interest of those educators who typically dismiss discussions regarding business continuity or ET. A mission continuity plan, by its very name, implies a construct of centrality and shared responsibility throughout the school community. If a community begins to recognize that continuity planning is essential to the viability and vitality of the school's mission, continuity planning will move from the periphery to the center stage of strategic planning initiatives. If educators shift their thinking from "business continuity" to

"mission continuity," they will recognize the distributed responsibility and accountability that all school stakeholders share for ensuring that data are well-protected.

School leaders are key to the successful process of reviewing, articulating, and promoting the vision and mission statements in their schools (Fayad, 2011). Thus a school community's adoption of effective BCP depends upon the foresight and perspective of its leaders. However, even those leaders who place value on business continuity planning and the safeguarding of ET sometimes lack awareness or understanding of the recommended practices.

Means to Achieving Best Practices

This study showed that most school leaders demonstrated some awareness of the need to engage in business continuity planning. Schools that lacked formal plans still engaged in some business continuity practices. For example, although only 14 of the 39 respondents (36%) had a "formal, documented plan for overall institutional business continuity," 31 respondents (79%) reported that they regularly and systematically backed up data. Also, 35 schools (90%) had procedures to assess the potential impact of disruptive events on business and academic processes and to prioritize risks from disruptive events. However, the substantial variation among participant schools' mean BCP scores suggested that wide disparity existed between the degree to which school policy makers recognized the nature and scope of ET risks or understood effective business continuity practices. Thus, no schools were entirely unprepared but many were under-prepared.

Even among those schools in which leaders recognized business continuity as being mission-critical, procedures and policies sometimes omitted important practices. For example, thirty-one respondents reported that their schools regularly and systematically backed up data. Yet eight of those schools had no off-campus backup locations. Similarly, of the 15 schools that

reported having a cold site, seven stated that the cold site was located on the same campus or within the same building as the central ET unit. Also, among the seven schools that reported having conducted a risk assessment, four indicated that their risk assessments were out of date. Finally, only one school reported engaging in regular tests and rehearsals of ET readiness to support business continuity. Perhaps school leaders are unaware of the prevalence of quiet catastrophes (e.g. hardware failure, computer viruses, power outages, etc.) and therefore underestimate the need for frequent updates and rehearsals of basic ET readiness procedures.

The events of September 11, 2001 and the more recent instances of severe weather in the United States and throughout the world focused policy makers' attention on preparing campuses for dramatic disasters rather than those threats that occur more frequently yet appear routine by comparison (Golden & Oblinger, 2007; Kano & Bourque, 2009; O'Hanlon, 2007; Trump & Lavarello, 2003). The BCPIT's respondents reported that hardware (n = 20; 51%) or electrical (n = 19; 49%) failure had disrupted normal business and academic operations within the past five years, but no respondents reported having experienced terrorism, hurricanes, tornados, or significant fires. However, Board of Trustees or Directors' training manuals, accreditation standards, and other regulatory guidelines typically recognize the need for fire and intruder drills but overlook the importance of drills for ET emergencies, particularly those that result from quiet catastrophes (Advance Education, 2011, Jarriel & Schomper, 2005; Trecek, et al., 2007; Williams & Krueger, 2005). Thus, business continuity drills are seldom mandatory and the individual school's preparedness for ET compromise depends largely upon the foresight of its leaders. The presence of an on-site coordinator is one means to increase a school's awareness of and engagement in best continuity practices (Kano & Bourque, 2009).

Kano and Bourque (2009) studied California public schools' overall preparedness for emergencies and disasters. Though their study was not limited to preparedness for ET continuity, Kano and Bourque also found that contrary to their expectations but consistent with the results of this study, school size and prior disaster experience explained little of the variance in the measures of preparedness for emergency. Their study did find that the presence of an on-campus emergency preparedness coordinator was strongly associated with heightened preparedness in its broadest scope. Kano and Bourque concluded that a coordinator is a "key to improving school preparedness" (p. 58). Perhaps large American international schools would benefit from designating a Mission Continuity Coordinator to serve as a liaison among stakeholder groups while also providing guidance. Such a person could help to keep mission continuity current and in the mainstream of the school community. In addition, a Mission Continuity Coordinator could ensure that faculty and school board members have opportunities to learn the information and skills that will enable them to be informed participants.

Large American international schools typically have a funding base that may be able to support a Mission Continuity Coordinator. Furthermore, they are more likely to have departments of technology that are well-funded and able to run efficiently without direct involvement from the head of school. Schools with these specialized technology departments tend to have structures that include multiple department heads and several principals. In contrast, heads of smaller American international schools given more limited funds and lesser needs for specialization are often more personally involved with all departments within the school, including technology. This personal involvement typically increases the school head's awareness of ET concerns including those pertaining to business continuity. Within small schools, policy and procedure changes have fewer tiers through which to travel and can take effect more quickly.

However, this more manageable structure makes it imperative that heads of school become familiar with the best practices in a wide range of areas including ET because they cannot assign teachers and other staff to do them given their primary responsibilities.

The lack of association between previous disaster experience and engagement in business continuity practices might be explained by some of the same factors that explain the lack of association between school size and engagement in business continuity practices. For example, if the processes for making changes to school policy are lengthy and complex as is the case in some large schools, the sense of urgency might have faded by the time the policy is ready for review and adoption by those with the most authority to effect change. The sense of exigency might lessen if more time passes between a disaster and the review of policy. Perhaps many schools engage in business continuity practices on an ad hoc basis and adhere to those tasks that comprise obvious things to do (e.g. backing up data) as they wait for policies to be developed and adopted. These discrepancies might further underscore the need for schools, particularly large ones, to employ a Mission Continuity Coordinator who would be responsible, among other things, for making sure that the continuity procedures reflect up-to-date practices. Also, inconsistencies between school leaders' desire to engage in effective business continuity planning and their ability to effectively do so further underscores the need for regional associations and accrediting organizations to develop resources, guidelines, and training opportunities about best practices.

Cloud computing represents one area of pressing need for training opportunities. The results of this study indicated that schools are increasingly turning to cloud computing resources as one means of meeting business continuity needs. Twenty-nine respondents (74%) agreed that cloud computing provides "a secure, cost effective, reliable means of storing data" and stated

that their school's use of cloud computing resources will increase over the next twelve months. Indeed, cloud computing addresses a school's need to back up data off-campus. However, cloud computing presents a new set of challenges for school leaders that include risks to security, privacy, and other vulnerabilities (EDUCAUSE, 2009; Gartner, 2011; Knorr, 2008; Plant, 2011). If schools begin to use cloud computing resources without fully understanding the risks to security or the possible hidden expenses, the results could be devastating to mission continuity.

Contributions to Research and Practice

This study provides the first snapshot of the business continuity practices of American international schools in a particular region thus providing a set of questions that can be posed to a wider sample of schools from other regions such as those served by EARCOS, NESA, AISA, and ERSA. Also, results from future studies can be compared to the results reported here. This study suggests a need for further research to explore the degree to which schools integrate business continuity within their mission statements. This study also indicates a need for research that examines the benefits and drawbacks to international schools of using cloud computing resources to support business continuity.

However, the sample for this study was limited to international schools within the AASSA region which comprise a small population. Future researchers should test these questions again with a larger sample. Also, the governance and organizational structures of international schools differ somewhat from United States independent schools and markedly from United States public schools. Furthermore, schools within the AASSA region address many issues that do not occur in all regions. For example, political instability, poor regional infrastructure, and poor local economies are less prevalent in regions such as Europe or parts of

Asia. As such, other regions might have more time and resources available for addressing business continuity issues. In addition, the results comprise self-reported data. Ideally, another study should be conducted to verify the self-report responses. Thus, the findings of this study must be cautiously interpreted when applied to schools or school systems outside of the AASSA region. However, this study served as an initial study in the area of continuity practices among schools and was conducted in order to increase awareness of these issues and provoke discussion.

Nevertheless, these results should compel educational leaders to ask themselves whether members of their school community perceive business continuity in terms of mission continuity. Do stakeholders recognize the role that business continuity planning plays in safeguarding the data that supports the school's shared mission? The fact that drivers of business continuity planning tended to be rooted in sources external to the school's internal governance structure adds weight to their obligation. However, regardless of their size, A/OS status, or previous disaster experience, schools should acknowledge their responsibility to address and remove internal barriers to effective business continuity planning. In addition, accrediting bodies and other organizations that influence the development of school policy should review their standards of good practice and continuous improvement in the areas of business continuity planning and consider requiring schools to protect the administrative, instructional, and technological systems that support their mission. If new mission continuity standards are proposed, then guidelines and training should be made available to help school leaders implement best practices. For maximum effectiveness, the guidelines and training opportunities must extend to members of faculty and school boards and other stakeholder groups.

Buildings and computers can be replaced, but lost data are irretrievable. The story of Haiti's Union School serves as a fitting and compelling illustration of this reality. Union had used an off-site data storage facility and backed up data frequently prior to the 2010 earthquake that damaged all campus buildings. As a result, Union was able to restore academic and business operations within weeks of the disaster, and was able to quickly provide transcripts and other data for those students who transferred to schools in other countries. Even in the aftermath of a devastating seismic catastrophe, Union's students, whether they stayed with the school or transferred elsewhere, were able to complete their school year and the school's mission was preserved. By contrast, the students of an unprepared school could have had their academic records erased by a simple hardware or electrical failure. Union's story underscores the message that business continuity planning is mission critical, and effective practices are imperative.

Afterword

On October 28, 2011 a series of unseasonable snowstorms occurred in several states in the northeastern United States. Widespread power outages affected five states and 1.7 million customers (CNN Wire Staff, 2011). In the days leading up to the November 2 committee meeting and final hearing for this dissertation, within the community surrounding Lehigh University, approximately 175,000 customers were without electrical power (Express Times, 2011). The university's power went out at 5:30 p.m. on October 29 and was not fully restored until the morning of November 2 (Brown and White Staff, 2011). Despite enduring an extensive period without external electrical power, Lehigh University's ET services continued uninterrupted, resulting in full business continuity capability for the institution. Vice Provost for Library and Technology Services Bruce Taggart and his team had in place a stand-by natural gas

powered generator. Thus, the technology that supported Lehigh University's programs and services was fully protected. The decisions to fund this and other back-up systems were made seven years before because the technology infrastructure was considered mission critical. None of these systems was used until this emergency situation. The circumstances under which the hearing for this dissertation occurred could hardly have been more fitting or compelling.

References

Agee, A., & Yang, C. (2009). Top-10 IT issues 2009. *EDUCAUSEreview, July/August,* 45-58.

Ahmed, S., Bixler, M., & Payne, E. (2006, February). Severe weather, tornadoes kill dozens across South. Retrieved July 1, 2008 from http://www.cnn.com/2008/US/weather/02/06/tornadoes/index.html .

Ambrose, J. (Ed.). (2003). *Improving governance and administration in international schools.* Search Associates.

American Overseas Schools Advisory Council. Retrieved January 12, 2007 from http:www.state/gov/m/a/os/c6971.htm . *Overseas Schools Advisory Council.*

American Red Cross (2006). Challenged by the storms: The American Red Cross response to hurricanes Katrina, Rita and Wilma (HIS 20170 (2-06). Washington, DC: Author.

Anderson, R., & Becker, H. (2001). *School investments in instructional technology.* (Report No. 8). Retrieved from the University of California Center for Research on Information Technology and Organizations website: http://www.crito.uci.edu/tlc/html/findings.html .

Armstrong, D. (2005). *Pro ASP.NET 2.0 website programming*. Berkeley, CA: Apress.

Banks, J., Higgs, J., Emeagwai, A., Walters, M., Guy, R. (2010). *Pilot study for business continuity planning best practices for small businesses [PDF file]*. Southeast Region Research Initiative, Oak Ridge, TN.

Baptiste, M. (2010, October 5). Email interview.

Barbara, M. (2006). Determining the critical success factors of an effective business continuity/disaster recovery program in a post 9/11 world: A multi-method approach. M.Sc. dissertation, Concordia University (Canada), Canada. Retrieved September 17, 2009, from Dissertations & Theses: A&I.(Publication No. AAT MR20809).

Barbour, M. & Reeves, T. (2009). The reality of virtual schools: A review of the literature. *Computers & Education, 52,* 402-416.

Bergman, D. (2010, December 2). Personal communication.

Billig, S., Sherry, L., & Havelock, B. (2005). Challenge 98: Sustaining the work of a regional technology integration initiative. *British Journal of Educational Technology. 36,* 987-1003.

Bird, D. (2008). The effect of a yearlong one-to-one laptop computer classroom program on the 4th-grade achievement and technology outcomes of digital divide learners. *UMI ProQuest Digital Dissertations.* (UMI No. 3338837).

Botha, J., & Von Solms, R. (2004). A cyclic approach to business continuity planning. *Information Management and Computer Security, 12,* 328-337.

Brown and White Staff. (2011, November). *Gryphons, administration discuss recent snowstorm.* Retrieved November 15, 2011 from http://www.lehighvalleylive.com/thebrownandwhiteblog/index.ssf/2011/11/gryphons_and_administration_di.html .

Bull, G. & Garofalo, J. (2010). Connected classroom: Data in the cloud. *Learning and Leading with Technology, May,* 10-12.

Burton, J. (2005). When disaster strikes: IHEs are implementing wide-ranging plans to protect their technology systems in the event of natural or man-made disasters. Retrieved October 13, 2008 from http://findarticles.com/p/articles/mi_m0LSH/is_9_8/ai_n15377867/print?tag=artBody;col1 .

Business Resiliency (n.d.). *Business resiliency, a new paradigm*. Retrieved April 2, 2009 from http://www.businessresiliency.com/index.htm .

Carlisle, V. (2005). Protecting vital records in a crisis. *School Administrator, 62*(11), 47-49.

Carlson, C. (2008). Rise in tornadoes, floods poses risk to colleges. *The Chronicle of Higher Education 54*(43), 1A. Retrieved June 30, 2008 from http://chronicle.com/temp/email2.php?id=cf4d6FytnVv5prcDjqXvRrbsKckxGyy8 .

Carmeli,, A., & Schaubroeck, J. (2008). Organizational crisis-preparedness: The importance of learning from failures. *Long Range Planning, 41*, 177-196.

Cerullo, V., & Cerullo, M. (2004). Business continuity planning: A comprehensive approach. *Information Systems Management, 21(3)*, 70-78.

CNN Wire Staff. (2011, October). *About 1.7 million without power as Northeast recovers from storm.* Retrieved November 15, 2011 from http://www.cnn.com/2011/10/31/us/east-coast-storm/index.html .

Chojnacki, J. (Ed.). (2007). *International trustee handbook: A guide to effective governance for independent school boards*. Washington, D.C.: National Association of Independent Schools.

Condie, R., & Livingston, K. (2007). Blending online learning with traditional approaches: Changing practices. *British Journal of Educational Technology, 38,* 337-348.

Consortium for School Networking. (2006). *Crisis preparedness: Networking for IT disaster recovery.* Washington, D.C.: Author.

Decker, J., & Thamer, J. (2008). *Introduction to the mission continuity initiative: University of Pennsylvania's criticality matrix.* [PowerPoint slides]. Retrieved from www.upenn.edu/missioncontinuity/tools_terms.html .

Dewey, B.I., & DeBlois, P.B. (2006). Top-10 IT issues 2006. *EDUCAUSEreview, May/June,* 58-79.

Disaster Recovery Journal and DRI International. (2007). Generally accepted practices for business continuity practitioners. *Disaster Recovery Journal*. Author.

Educause. (2009, August). 7 things you should know about....cloud computing. Boulder, CO: Author. Retrieved from http://www.educause.edu/Resources/7ThingsYouShouldKnowAboutCloud/176856 .

Elliot, D., Swartz, E., & Herbane, B. (2002). *Business continuity management: A crisis management approach.* London: Routledge.

Elrod, R. (2005). *So you think you have a good business recovery plan? Steps an asset management company can take to recovery from a major disaster.* Retrieved October 3, 2008 from http://www.infosecwriters.com/text_resources/pdf/Good_Business_Recovery_Plan.pdf

Emergency Response and Crisis Management Technical Assistance Center. (2006).Creating emergency management plans*. ERCMExpress 21* (8)*,* 1-12. Washington, D.C.: United States Department of Education.

Express Times Staff and Wire. (2011, November). *Storm knocks out power, downs trees.* Retrieved November 15, 2011 from http://www.lehighvalleylive.com/breaking-news/index.ssf/2011/10/post_79.html .

Fayad, J. D. (2011). Making mission statements operational: Perceptions of principals from Tri-Association schools. Ed.D. dissertation, Lehigh University, United States -- Pennsylvania. Retrieved September 26, 2011, from Dissertations & Theses @ Lehigh University (Publication No. AAT 3456133).

Foster, G., Hendrickson, D., & New Freeland, L. (2006). Lessons from the ashes: Advice after a campus fire. *Chronicle of Higher Education, 52*(25), B9.

Fryer, W. (2003). A beginner's guide to school security. *Tech & Learning, September 2003,* unpaginated digital version. Retrieved June 28, 2008 from http://www.techlearning.com/showArticle.php?articleID=14700427.

Fullick, A. (2010). Exercising over testing. *Disaster Recovery Journal. 23*(4). Unpaginated digital document. Retrieved November 21, 2010 from http://www.drj.com/fall-2010-volume-23-issue-4/view-issue.html.

Glennan, T. K., & Melmed, A. (1996). Fostering the use of educational technology: Elements of a national strategy (MR-682-OSTP/ED). Santa Monica, CA: RAND. Retrieved April 5, 2009, from http://www.rand.org/publications/MR/MR682/.

Golden, C., & Oblinger, D. (2007). The myth about business continuity and disaster recovery: "We've got backups, so we're ready for any disaster." *EDUCAUSEreview,* May/June, 10-11.

Gregory, E., & Hover, C. (2007). Business continuity certification in higher education. *EDUCAUSE Center for Applied Research Bulletin.* (2007, May).

Henderson County Public Schools (2005). *Business continuity planning: Executive summary, information technology.* (2005, November). Henderson County, NC: Author. Retrieved October 5, 2008 from www.co.henderson.k12.nc.us/technology-web/plan/procedure/HCPScp.pdf - .

Henke, K. (2008). Surviving disaster. *Technology and Learning*. 21-24.

Hoover, J. (2011, February 11). White House issues federal cloud strategy. *InformationWeek*. Retrieved from http://www.informationweek.com/news/government/cloud-saas/229218475?cid=RSSfeed_IWK_ALL .

Huett, J., Moller, L., Foshay, W., & Coleman, C. (2008). The evolution of distance education: Implications for instructional design on the potential of the web. *TechTrends, 52*(5), 63-67.

Ithaca City School District Department of Information & Instructional Technology (2006). *Technology budget for the Ithaca City School District.* Ithaca, NY.: Author. Retrieved September 18, 2008 from www.icsd.k12.ny.us/legacy/board/budget/2006-07/2006-2007BudgetBackground-IIT.pdf - .

Jang, S. (2008). Exploration of secondary students' creativity by integrating web-based technology into an innovative science curriculum. *Computers & Education, 52,* 247-255.

Jarriel, J., & Shomper, C. (2005). Lemons to lemonade: Disaster preparation and recovery. *EDUCAUSE Center for Applied Research Bulletin.* (2005, March). Retrieved February 6, 2007 from net.educause.edu/ir/library/pdf/erb0505.pdf .

Jeroski, S. (2008). *Wireless writing program (WWP): Peace River North summary report on grade 6 achievement: 2008.* Ft. St. John, British Columbia: Horizon Research and Evaluation, Inc.

Johnson, L., Smith, R., Levine, A., & Haywood, K. (2010). *2010 Horizon report: K-12 edition.* Austin, Texas: The New Media Consortium.

Johnston, S. (2011). *Amazon's cloud outage—a touch of stormy weather?* Retrieved April 26, 2011 from http://www.internetnews.com/bus-

news/article.php/3931831/Amazons+Cloud+Outage++A+Touch+of+Stormy+Weather.htm .

Kano, M., & Bourque, L. (2008). Correlates of school disaster preparedness: Main effects of funding and coordinator role. *Natural Hazards Review ASCE.* (2008, February).

Kiernan, V. (2005). Ready for the next Katrina? *The Chronicle of Higher Education. 52,* 31-38.

Kimber, K., & Wyatt-Smith, C. (2006). Using and creating knowledge with new technologies: A case for students-as-designers. *Learning, Media and Technology. 31,* 19-34.

Kirchner, T., Karande, K., & Markowski, E. (2006, March 17). *Perceived organizational business continuity readiness: Scale development and validation.* Paper presented at Old Dominion University, Richmond, VA.

Knorr, E., & Gruman, G. (2008). What cloud computing really means. InfoWorld. Retrieved April 21, 2011 from http://www.infoworld.com/d/cloud-computing/what-cloud-computing-really-means-031?page=0,2 .

Kuzyk, R. (2007). Serving through disaster. *Library Journal. 132*, 26-29.

Ligon, G. (2006). *The optimal reference guide: Data driven decision making 2016.* Washington DC: ESP Solutions Group.

Ligon, G., & Mangino, E. (2005). *The optimal reference guide: Disaster prevention and recovery for school system technology.* Washington, DC: ESP Solutions Group.

Lowther, D., Ross, S., & Morrison, G. (2003). When each has one: The influences on teaching strategies and student achievement of using laptops in the classroom. *Educational Research, Design & Technology. 51*(3), 23-44.

Machin, S., McNally, S., & Silva, O. (2007). New technology in schools: Is there a payoff? *Forschungsinstitut zur Zunkunft der Arbeit Institute for the Study of Labor.* Bonn,

Germany: Institute for the Study of Labor. Retrieved September 14, 2008 from http://www.voxeu.org/index.php?q=node/812.

McGrath, D. (2003). Measuring the 4:11 effect: The power failure and the Internet. *The Blackout*. Washington, DC: The IEEE Computer Society.

Ng, W. & Nicholas, H. (2009). Introducing pocket PCs in schools: Attitudes and beliefs in the first year. *Computers & Education, 522*, 470-480.

Nguyen, C.X. (2007). Estimating the effort costs of information technology disaster recovery projects: A model based on a mixed methodology investigation. *UMI ProQuest Digital Dissertations.* (UMI No. 3253632).

Nwosisi, C., & Nieto, A. (2007). *Eleven patterns for IT disaster recovery.* Washington, DC: Retrieved October 9, 2008 from http://dps.csis.pace.edu:8077/files/team4/Biometricis_authentication.pdf .

O'Hanlon, C. (2007). Disaster recovery: Courting disaster. *T.H.E. Journal*. *September, 2007.* Unpaginated digital document. Retrieved October 6, 2008 from http:www.thejournal.com/articles/21236/.

Omar, A., Udeh, I., & Mantha, D. (2010). Contingency planning: Disaster recovery strategies for successful educational continuity [PDF file]. *Journal of Information Systems Applied Research, (3),* 11.

Panther Paws (2010). Evaluation report H2L2 architects. Port au Prince, Haiti: The Union School.

Peck, C., Cuban,L., & Kirkpatrick, H. (2002). Techno-promoter dreams, student realities. *Phi Delta Kappan, 83,* 472-481.

Pitrelli, E. (2007). The effects of instructional pressures, teachers' view of the importance of technology for instruction, and teachers' overall beliefs about teaching and learning on teacher-directed student use of technology. *UMI ProQuest Digital Dissertations* (UMI No. 3286100).

Pirani, J., & Yanosky, R. (2007). Shelter from the storm: IT and business continuity in higher education. *EDUCAUSE Center for Applied Research Bulletin*. (2007, March).

Pitt, M., & Goyal, S. (2004). Business continuity planning as facilities management tool. *Facilities, 22,* 87-99.

Plant, R. (2011, April 25). To cloud or not to cloud: That is the big IT question for a lot of companies. *The Wall Street Journal,* p. R9.

Pritchard, S. (2007). Continuity in disaster. *Infosecurity, 4,* 24-25.

Qayoumi, M. (2002). *Mission continuity planning: Strategically assessing and planning for threats to operations.* Washington, D.C: National Association of College and University Business Officials.

Roblyer, M. (2006). Online high school programs that work: Five common strategies for making online high school programs effective in your school district. *The Education Digest. 72,* 55-63.

Rojas, C. (2006, November). Fixing Katrina's schools. Place of publication. Retrieved August 21, 2008 from http://www.dailytitan.com/news/2006/11/01/News/Fixing.Katrinas.Schools-2414650-page2.shtml .

Savage, M. (2002). Business continuity planning. *Emerald Work Study, 51,* 254-261.

Seid, J. (2006). New Orleans small businesses survive. *CNNMoney* Unpaginated digital document. Retrieved July 7, 2008 from http://money.cnn.com/2006/08/24/smbusiness/katrina_followup/index.htm

Shroads, D. (2005). Disaster recovery of critical business information systems in colleges and universities: A descriptive and exploratory study. *UMI ProQuest Digital Dissertations.* (UMI No. 3197034).

Sieberling, C. (2005). Cyber security: a survival guide. Place of publication? Retrieved June 28, 2008 from http://www.techlearning.com/showArticle.php?articleID=60400188 .

Siegle, D. (2010). Cloud computing: A free technology option to promote collaborative learning. *Gifted Child Today, 33(4), 41-45.*

Silva, E. (2008). Measuring skills for the 21st century. *EducationSector Reports. November, 2008.* Washington, D.C.: Author. Retrieved August 16, 2008 from http://www.educationsector.org/usr_doc/MeasuringSkills.pdf.

Smith, R. (1995). Business continuity planning and service level agreements. *Information Management and Computer Security, 3*, 17-21.

Solomon, M. (2006). How to: Add IT up. Place of publication? Retrieved June 28, 2008 from www.edtechmag.com/k12/issues/january-february-2006/how-to.html.

Sutherland, R., Armstrong, V., Bares, S., Brawn, R., Breeze, N., Gall, M., Matthewman, S., Olivero, F., Taylor, P., Wishart, J., & John, P. (2004). Transforming teaching and learning: Embedding ICT into everyday classroom practices. *The Journal of Computer Assisted Learning, 20,* 413-425.

Swanson, M., Wohl, A., Pope, L., Grance, T., Hash, J., & Thomas, R. (2002). *Contingency planning guide for information technology systems: Recommendations of the national*

institute of standards and technology (National Institute of Standards and Technology Special Publication 800-34). Washington, D.C: U.S. Department of Commerce.

Swoyer, S. (2003, December). Disaster recovery: Best practices. Place of publication? Retrieved June 15, 2008 from http://esj.com/it_info_center/article.aspx?EditorialsID=25.

Taggart, B. (2011, November 2). Personal communication.

Tondeur, J., van Braak, J., & Valcek, M. (2007). Curricula and the use of ICT in education: Two worlds apart? *British Journal of Educational Technology, 38,* 962-976.

Trecek D., Trobec, R., Pavesic, N. & Tasic, J. (2007). Information systems security and human behavior. *Behavior & Information Technology. 26,* 113-118.

Trotter, A. (2003). Cyber viruses infect schools across nation. Place of publication. Retrieved October 15, 2008 from http://www.edweek.org/login.html?source=http%3A%2F%2Fwww.google.com%2Fsearch%3Fclient%3Dsafari%26rls%3Den-us%26q%3DCyber%2Bviruses%2Binfect%2Bschools%2Bacross%2Bnation%2BTrotter%26ie%3DUTF-8%26oe%3DUTF8&destination=http%3A%2F%2Fwww.edweek.org%2Few%2Farticles%2F2003%2F09%2F10%2F02virus.h23.html&levelId=2100&baddebt=false .

Trump, K., & Lavarello, C. (2003). No safe havens: Are schools vulnerable to terrorism? A new national survey raises troubling questions. *American School Board Journal, 190*, 19-21.

Twining, P. (2001). Planning to use ICT in schools. *Primary Education, 29*, 9-18.

United States Department of Education, Office of Educational Technology. (2004). *Toward a new golden age in American education: How the Internet, the law and today's students are revolutionizing expectations.* Washington, DC: Author.

United States Department of State Office of Overseas Schools. (n.d.). *Office of Overseas Schools.* Washington, D.C. Retrieved November 4, 2007 from http://www.state.gov/m/a/os/.

United States Department of State Office of Overseas Schools. (n.d.). *Teaching in International Schools Overseas.* Washington, D.C. Retrieved November 9, 2007 from http://www.state.gov/m/a/os/c16899.htm.

Union University. (2008). *Blog leads communication efforts in aftermath of tornado.* Unionite Special Edition. Jackson, TN: Author.

Villano, M. (2009). Business continuity: Eureka! *Campus Technology, April,* unpaginated digital document.

Voss, B. (2006). What would Ozymandias think about disaster planning? *EDUCAUSEreview, March/April,* 76-77.

Voss, B., & Siegel, P. (2009). Keeping the guard up in a down economy: Investing in IT security in hard times. *EDUCAUSEreview, September/October,* 10-22.

Wan, S., & Chan, Y. (2008). Improving service management in campus IT operations. *Campus-Wide Information Systems, 25,* 30-49.

Weishen, W., Huey-Por, C., & Chorng-Jee, G. (2009). The development of an instrument for a technology-integrated science learning environment. *International Journal of Science and Mathematics Education, 7,* 207-233.

Wilson, T. (2005). Priority no.1: Data protection. *Network Computing, 16*(26), 13-14.

Wood, E., & Yates, C. (2008, February). Union students recall shock of tragic tornado. Union News February 8, 2008. Jackson, TN: Edunews. Retrieved July 1, 2008 from http://www.uu.edu/news/NewsReleases/release.cfm?ID.

Yanosky, R. (2007). *Shelter from the storm: IT and business continuity in higher education.* (Research Study No. 2). Boulder, CO: EDUCAUSE.

APPENDIX A: AASSA Member Schools

School and country	Approximate Student Population	Official A/OS
Asociacion Escuelas Lincoln, Argentina	750	Yes
American Cooperative School, Bolivia	350	Yes
Santa Cruz Cooperative School, Bolivia	550	Yes
The American International School of Bolivia	250	Yes
Associacao Escola Graduada de Sao Paulo, Brazil	1300	Yes
American School of Belo Horizonte, Brazil	150	Yes
American School of Brasilia, Brazil	600	Yes
American School of Campinas, Brazil	450	No
American School of Rio de Janeiro, Brazil	800	Yes
Escola Maria Imaculada, Brazil	1200	Yes
International School of Curitiba, Brazil	500	No
Our Lady of Mercy, Brazil	500	No
Pan American Christian Academy, Brazil	350	No
School of the Nations, Brazil	600	No
Escola Pueri Domus/Global, Brazil	450	No
Pan American School of Porto Alegre, Brazil	300	No
Sant'Anna American International School, Brazil	300	No
Freeport Mining Schools in South America, Chile	15	No
International School of Nido de Aguilas, Chile	1400	Yes
Karl C. Parrish, Colombia	750	No

Colegio Nueva Granada, Colombia	1800	Yes
The Columbus School, Colombia	1500	No
Colegio Albania, Colombia	200	No
Colegio Bolivar, Colombia	1200	No
Colegio Panamericano, Colombia	650	No
GI School, Colombia	600	No
Colegio Bureche, Colombia	550	No
Lincoln School, Costa Rica	1300	Yes
Academia Cotopaxi, Ecuador	450	Yes
Alliance Academy International, Ecuador	450	No
American School of Quito, Ecuador	2250	No
Colegio Alberto Einstein, Ecuador	650	No
Colegio Americano de Guayaquil, Ecuador	1600	No
Inter-American Academy of Guayaquil, Ecuador	200	Yes
American School of Guatemala	1500	No
Georgetown International Academy, Guyana	100	Yes
Union School, Haiti	260*	Yes
American School of Tegucigalpa, Honduras	1150	Yes
Escuela Internacional Sampedrana, Honduras	1600	No
Discovery School, Honduras	250	Yes
American International School of Kingston, Jamaica	250	Yes
American School Foundation, A.C., Mexico	2600	Yes
International School of Curacao, Netherlands Antilles	500	Yes

American-Nicaraguan School, Nicaragua	950	Yes
Crossroads Christian Academy, Panama	250	No
The International School of Panama, Panama	800	Yes
American School of Asuncion, Paraguay	650	Yes
Asociacion Educativa Davy, Peru	750	No
Colegio Franklin D. Roosevelt, Peru	1500	Yes
International School of Port of Spain, Trinidad and Tobago	400	Yes
Uruguayan American School, Uruguay	300	Yes
Colegio Internacional de Carabobo, Venezuela	450	Yes
Colegio Internacional de Caracas, Venezuela	200	Yes
Colegio Internacional Puerto La Cruz, Venezuela	250	No
Escuela Bella Vista, Venezuela	300	No
Escuela Campo Alegre, Venezuela	600	Yes
Escuela Las Morochas, Venezuela	100	No
International School of Monagas, Venezuela	200	No

Note: All numbers were rounded to the nearest fifty.
**Due to the earthquake of 2010, the student population of the Union School remains erratic.*

APPENDIX B: BCPIT Survey Document

Business Continuity Planning for IT in AASSA Schools

Information and consent

Business Continuity Planning for Information Technology in Overseas American Schools Pilot Study

You are invited to be in a research study of business continuity practices for IT among AASSA schools. You were selected as a possible participant because you are the director or superintendent of an AASSA school. We ask that you read this form and ask any questions you may have before agreeing to be in the study.

This study is being conducted by: Kelly Broyles Metaline, College of Education, doctoral candidate under the supervision of Roland K. Yoshida, College of Education professor and provost emeritus.

Purpose of the study
The purpose of this study is:
To acquire data pertaining to the business continuity planning practices that occur among AASSA member schools. The study will identify the practices that occur frequently and infrequently, as well as barriers to and triggers of continuity planning. In addition, the study will look for relationships between a school's business continuity practices and the school's size, status as an A/OS or non A/OS, and previous disaster experience.

Procedures
If you agree to be in this study, we would ask you to do the following things:
Participate in an online survey about your school's business continuity practices. You may also designate a member of your administration team, such as a principal or head of technology, to complete the survey on your behalf.

Risks and Benefits of being in the Study
Possible risks:
Participants are asked to provide information and opinions about their workplaces, thus a minimal risk exists that information pertaining to a particular school could be disclosed. Precautions have been taken to prevent the disclosure of individual responses. The completed surveys will only be accessible to the researcher and will be destroyed and deleted at the end of the study. Participation is voluntary and the participant may stop the survey at any time.

The benefits to participation are:
The results of this survey will provide data about the business continuity practices that occur among AASSA schools. These data will provide a picture of ways that schools are meeting recommended practices, and will also identify areas where help or improvement are needed.

Compensation
Participants will not be compensated.

Confidentiality
The records of this study will be kept private. The report will not include any information that will make it possible to identify a subject or school. Research records will be stored securely and only researchers will have access to the records.

Voluntary Nature of the Study
Participation in this study is voluntary:
Your decision whether or not to participate will not affect your current or future relations with the Lehigh University. If you

Page 1

decide to participate, you are free to withdraw at any time without affecting these relationships.

Contacts and Questions
The researchers conducting this study are:
Roland Yoshida and Kelly [illegible]. You may ask any questions you have now. If you have questions later, you are encouraged to contact them at: Kelly [illegible], Georgetown International Academy, Guyana, [illegible], [illegible]@georgetowninternationalacademy.org. Advisor: Roland K. Yoshida, Lehigh University, [illegible], [illegible]@lehigh.edu.

Questions or Concerns:
If you have any questions or concerns regarding this study and would like to talk to someone other than the researcher(s), you are encouraged to contact [illegible] at [illegible] (email: [illegible]@lehigh.edu) or [illegible] at [illegible] (email: [illegible]@lehigh.edu) of Lehigh University's Office of Research and Sponsored Programs. All reports or correspondence will be kept confidential.

BY CLICKING ON THE SURVEY LINK YOU ARE ACKNOWLEDGING THAT YOU HAVE READ AND UNDERSTAND THE ABOVE INFORMATION.

Introduction

Thank you for participating in this study of business continuity practices for IT among AASSA member schools. Our testing suggests that it will require 12-15 minutes to complete this survey. Your name, position, and school will be kept strictly confidential. You are free to exit this survey at any time.
American Overseas schools depend upon information technology (IT) to support business operations and student learning experiences. IT's fragility compared to buildings and other physical resources makes it vulnerable to potential compromise from a variety of threats. Threats to IT include natural disasters, human created risks, and environmental dangers. In order to make certain that their IT is adequately protected, many schools participate in business continuity planning. Business continuity practices include procedures for safeguarding an organization's technology and data in order to keep a business operational throughout a disaster or IT failure. This study will examine the business continuity planning practices among AASSA member schools.
Please note that * denotes an item that may not be skipped.

School's Approach to Business Continuity Planning

Business continuity planning is a process for keeping an organization operational throughout a disaster.

The primary objectives of IT business continuity planning are:
- identifying major risks of business interruption
- developing a plan to reduce the impact of the risks
- implementing, testing, and maintaining the plan.

*** 1. At my school, business continuity planning for IT is given high priority.**

- ◯ Strongly agree
- ◯ Agree
- ◯ Disagree
- ◯ Strongly disagree

Business Continuity Planning for IT in AASSA Schools

*** 2. What are the primary drivers for business continuity planning for IT at your school? (select up to three responses)**

- [ ] Threats specific to our geographic location
- [ ] Hazards arising from our school's operations
- [ ] School leadership mandate
- [ ] Demand from constituents (e.g. faculty, students)
- [ ] Audit requirements
- [ ] Regulatory compliance
- [ ] Keeping current with generally accepted business practices or best practices
- [ ] Awareness of recent global natural disasters (e.g. hurricanes, tsunamis)
- [ ] Terrorism/security concerns
- [ ] A recent incident at our school causing or threatening disruption to operations

Other (please specify)

Risk Assessment

Risk assessment involves:
- Identifying threats or potential events that could cause IT or facilities to be unavailable or damaged.
- Characterizing the consequences of disruption in an effort to predict the degree of potential loss that could result from certain IT disasters.
- Determining the likelihood that a particular threat will occur.

*** 3. Has your school undertaken a formal overall risk assessment to evaluate the events/threats (e.g. natural disasters, accidents, terrorism) that can cause interruptions to the school's operations?**

- ◯ No risk assessment is anticipated
- ◯ A risk assessment is planned for the future
- ◯ A risk assessment is in progress
- ◯ A risk assessment has been completed

Page 3

4. What are the primary reasons why your school has not conducted a formal overall risk assessment at this time? (select up to three responses)

- [ ] Threats do not justify effort
- [ ] Benefits do not justify investment
- [ ] Prefer an ad hoc approach
- [ ] Lack of adequate funding
- [ ] Lack of institutional leadership's support
- [ ] Business/academic units have not defined business continuity needs
- [ ] Lack of staff expertise
- [ ] Difficulty developing campus policies and procedures

Other (please specify)

5. My school's effort to complete an overall risk assessment

- [ ] Has been assigned a completion date
- [ ] Has been assigned staff
- [ ] Has been allocated funds
- [ ] Has executive or management sponsor
- [ ] Has participation from functional business/academic units

6. Our school's overall risk assessment is kept up to date

- ◯ Strongly agree
- ◯ Agree
- ◯ Neutral
- ◯ Disagree
- ◯ Strongly disagree

7. Does your school have documented plans or processes that do the following:

	Yes	No	I don't know
Identify the probability of disruptive events/threats	◯	◯	◯
Assess the potential impact of disruptive events/threats on business and academic processes	◯	◯	◯
Prioritize risks from disruptive events/threats	◯	◯	◯

Business Continuity Planning for IT in AASSA Schools

Formal Written Plans for Business Continuity

Many schools have created a business continuity planning document, whereas others take a more ad hoc or non-sequential approach.

8. Does your school have a formal, documented plan for overall institutional business continuity?

- ◯ Yes
- ◯ No
- ◯ I don't know

9. Does your school have a formal process for updating its overall business continuity plan?

- ◯ Yes
- ◯ No
- ◯ I don't know

10. Has your school's central IT unit conducted an IT risk assessment to evaluate the impact that disruptive events/threats would have on IT systems and assets?

- ◯ Yes
- ◯ No
- ◯ I don't know

Page 5

Business Continuity Planning for IT in AASSA Schools

11. Has your central IT unit documented procedures for the following, either as part of a formal plan or as a separate procedure?

	Yes	No	I don't know
Declaring an IT emergency when disruption falls outside normal operating bandwidth	◯	◯	◯
Activating (escalating) IT emergency response	◯	◯	◯
Notifying appropriate parties of emergency	◯	◯	◯
Performing damage assessment	◯	◯	◯
Prioritization of systems for purposes of recovery	◯	◯	◯
Recovery of IT operations	◯	◯	◯
Moving necessary activities/equipment to alternate sites	◯	◯	◯
Transportation/lodging support for staff to alternate sites	◯	◯	◯
Notifying cancellations of system outages	◯	◯	◯
Returning activities/equipment to primary locations	◯	◯	◯
De-escalation of IT emergency response	◯	◯	◯
Declaring resumption of normal operations	◯	◯	◯
Evaluation of post-recovery IT environment (i.e. establishing "new normal")	◯	◯	◯

12. Which of the following best describes the status of a formal, documented central IT plan for business continuity and/or disaster recovery at your school?

- ◯ No plan yet developed
- ◯ Planned for the future
- ◯ Work in progress
- ◯ Plan is complete

Testing, training, and maintenance

IT systems can be prepared through the inclusion of fault-tolerant upgrades, staffing cutback controls, or some organizational patterns.

Ongoing maintenance and testing of business continuity planning procedures helps to ensure that procedures are kept up to date with IT changes and upgrades.

13. Does your school provide IT staff with the following types of training for business continuity support:

	Yes	No	I don't know
Formal training about overall institutional business continuity plans/procedures	◯	◯	◯
Formal training about IT plans and procedures to support business continuity	◯	◯	◯

Other (please specify)

Business Continuity Planning for IT in AASSA Schools

14. Does your school conduct tests to assess IT readiness for supporting business continuity?

- Yes
- No
- I don't know

15. How many times per year does your school conduct tests of the following types to assess IT readiness for supporting business continuity:

	Never	Less than 1	1	More than 1	ad hoc basis	I don't know	Not applicable
Full-scale rehearsal involving personnel, equipment, facilities, etc.							
Simulations (performing actions in response to scenario)							
Table-top tests (discussion/analysis response to scenario)							
Technical recovery testing at primary site (typically on campus)							
Technical recovery testing at alternate site (off campus or away from campus data center)							
Tests of supplier facilities/services							

Other (please specify)

16. Does your school test IT readiness for supporting business continuity when the following events occur?

	Never	On a regular basis	On an ad hoc basis	I don't know	Not applicable
When implementing new equipment and systems					
When facilities changes take place					
When significant personnel changes take place					
When business continuity plans or procedures change					

Alternate Sites

Alternate sites provide a means for an organization that is facing an IT threat to shift its operations to a predetermined location, thereby avoiding a disruption.

A cold site usually consists of a facility with adequate space and infrastructure such as electric power and telecommunications equipment, but not IT equipment. The affected organization provides and installs the necessary equipment at the time of the emergency.

Page 7

Business Continuity Planning for IT in AASSA Schools

Hot sites are pre-configured with system hardware, infrastructure, and personnel, thereby enabling an organization to shift its IT operations almost seamlessly.

Cloud computing refers to the practice of accessing and using IT resources via the Internet from specialized data centers as opposed to hosting and operating these resources on campus. Many cloud computing resources such as Dropbox, Flickr, and Amazon's Elastic Compute Cloud provide data storage for schools and other organizations.

*** 17. Does your school have at least one hot site capable of assuming key IT operations?**

- ◯ Not planning to do so
- ◯ Planned for the future
- ◯ In development
- ◯ Operational

18. What are the primary reasons why your school does not have a hot site? (select up to three responses)

- ☐ Do not believe it to be necessary
- ☐ Do not believe cost justifies expense
- ☐ Lack of adequate funding
- ☐ We are not far enough along in our business continuity planning
- ☐ Lack of staff resources
- ☐ Lack of staff expertise
- ☐ Technical issues
- ☐ Lack of leadership support

Other (please specify)

Page 8

Business Continuity Planning for IT in AASSA Schools

19. Describe the geographic location of your primary hot site in relation to your school's central IT operations?

- Same building
- Different building, same campus
- Off campus, less than 5 miles distant
- Off campus, 5 to 20 miles distant
- Off campus, 20+ to 50 miles distance
- Off campus, more than 100 miles distant
- I don't know

*** 20. Does your school have at least one cold site capable of assuming key IT operations?**

- Not planning to do
- Planned for the future
- In development
- Have already

21. What are the primary reasons why your school does not have a cold site? (select up to three responses)

- Do not believe one is necessary
- Do not believe benefit justifies expense
- Lack of adequate funding
- We have not thought along in our business continuity planning
- Lack of staff resources
- Lack of staff incentive
- Technical issues
- Lack of leadership support

Other (please specify)

Page 9

22. Describe the geographic location of your primary cold site in relation to your school's central IT operations.

- ○ [illegible]
- ○ [illegible]
- ○ [illegible]
- ○ [illegible]
- ○ [illegible]
- ○ [illegible]
- ○ [illegible]

23. Describe your school's current approaches to central IT data storage and recovery.

	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
[illegible]	○	○	○	○	○
[illegible]	○	○	○	○	○
[illegible]	○	○	○	○	○
[illegible]	○	○	○	○	○
[illegible]	○	○	○	○	○
[illegible]	○	○	○	○	○

24. Which cloud computing resources does your school use? (select up to four responses)

- ☐ [illegible]
- ☐ [illegible]
- ☐ [illegible]
- ☐ [illegible]
- ☐ [illegible]

Business Continuity Planning for IT in AASSA Schools

25. Over the next year, do you expect your school's use of cloud computing resources to:

- Increase
- Decrease
- Remain the same

26. I feel that cloud computing provides a secure, cost-effective, reliable means of storing data.

- Strongly agree
- Agree
- No opinion
- Disagree
- Strongly disagree

Incident Exposure

IT business continuity planning attempts to protect an organization from three classifications of threats:
- natural disasters (e.g. weather-related incidents, seismic events, fires)
- human threats (e.g. error, sabotage, terrorism)
- environmental dangers (e.g. equipment failure, power outage, software error).

*** 27. Has your school experienced any disruptions to normal business and academic operations in the past five years that caused central IT to implement formal or ad hoc emergency response procedures?**

- No
- Yes
- I don't know

Business Continuity Planning for IT in AASSA Schools

23. Choose from the options below, any events that occurred in the last five years and the response that best matches the central IT emergency response.

	None	Impact on a few processes	Impact on many processes	Campus-wide impact	Campus-wide & regional impact	I don't know
Severe weather (hurricane, tornado, flooding)	○	○	○	○	○	○
Earthquake	○	○	○	○	○	○
Terrorism	○	○	○	○	○	○
Fraud	○	○	○	○	○	○
Other severe weather	○	○	○	○	○	○
Extreme or unusual temperatures	○	○	○	○	○	○
Fire	○	○	○	○	○	○
Electrical failure	○	○	○	○	○	○
Hazardous materials spill	○	○	○	○	○	○
Computer failure	○	○	○	○	○	○
Vandalism and criminal behavior	○	○	○	○	○	○
Theft	○	○	○	○	○	○
Cyber-war	○	○	○	○	○	○
Cyber-attack	○	○	○	○	○	○
Terrorism	○	○	○	○	○	○

Other (please specify)

24. If your school experienced a disruption or disruptions in the past five years, please rate how severe it was or they were.

- ☐ No impact
- ☐ Minor impact
- ☐ Moderate impact
- ☐ Substantial impact
- ☐ Severe impact

Page 12

Business Continuity Planning for IT in AASSA Schools

*** 30. What are the primary barriers to business continuity planning at your school? (select up to three responses)**

- [ ] Lack of adequate funding
- [ ] Lack of acceptable return on investment
- [ ] Technology issues
- [ ] Lack of leadership's support
- [ ] Business or academic units have not defined business continuity needs
- [ ] Lack of staff expertise
- [ ] Difficulty developing campus services and procedures
- [ ] Other (please specify)

Demographic data

*** 31. What is the name of your school?**
(Please note that the answers you have provided will remain confidential. This information will help us to ensure that we have not received more than one response per school.)

*** 32. What is your position or title?**

*** 33. I am personally involved in decisions pertaining to business continuity planning for IT at my school.**

- ◯ Strongly agree
- ◯ Agree
- ◯ Disagree
- ◯ Strongly disagree

Survey completed.

Thank you for taking the time to participate in this survey. The results will be published in AASSA's newsletter. The identity of respondents and their schools will remain strictly confidential.

Page 13

APPENDIX C: IT Readiness for Business Continuity Survey Questionnaire

IT Readiness for Business Continuity
Survey Questionnaire

May 2006

Thank you for participating in the study being conducted by the EDUCAUSE Center for Applied Research (ECAR). This survey is a critical part of the study and seeks to understand your institution's plans, infrastructure, experience, and capability in the area of IT support for business continuity. Our testing suggests that it will require 30–40 minutes to complete this survey. If you wish to print a copy of the survey before completing it online, a .pdf version is available from the header on each survey page and at
http://www.educause.edu/ir/library/pdf/ecar_so/ers/si/esi06c.pdf

By "business continuity" we mean the institution's ability to maintain or restore its business and academic services when some circumstance threatens or disrupts normal operations. As used in this survey, business continuity encompasses disaster recovery—the activities that restore the institution to an acceptable condition after suffering a disaster—and also includes activities such as risk and impact assessment, prioritization of business processes, and restoring operations to a "new normal" after an event.

Note that our survey asks about business continuity activities at two levels:

- *institutional business continuity*, referring comprehensively to activities relating to overall business continuity across the whole institution; and
- *central IT support for business continuity*, referring to the activities specific to central IT's contributions to institutional business continuity, such as providing IT expertise to institutional business continuity planning activities, testing IT readiness for business continuity, and restoring IT services when a disruption takes place.

As you work on the survey, we encourage you to consult with other offices, such as your office of emergency preparedness, auditors, and managers of major business units.

Our survey software allows you to:

> Print a blank survey. To **print a blank copy of the survey** before completing it, click "Printable version of this survey" in the header. Once you have completed the online survey, you can **print your responses** by clicking the "Review" button at the end of the survey.

> Save partially completed surveys. The survey need not be completed at a single sitting. To save and return to a partially completed survey, set a Favorite or Bookmark for the survey and then click the SAVE button at the bottom of the screen. If cookies are enabled, when you return to the survey you will be taken to the place you left off.

> Review, revise, print, and save your responses. You may review and revise your answers before clicking the "Finish" button to submit your response. On the last screen of the survey, select the "Review" button to review, revise, print, and save your responses. Always print a copy of your completed survey and retain it for your records.

Please complete this survey by Tuesday, May 23, 2006. As thanks for your time and valuable input, each participant is entitled to receive a summary of key findings from the study.

We appreciate your time and participation. If you have any questions or concerns, please e-mail <ecar@educause.edu>.

Click the Next button to begin the survey. Once again, thank you for your input!

Section 1: About You and Your Institution

1.1 Survey ID <Required> _____ <Survey ID Lookup>

1.2 Your name <Required> _____

1.3 Your position.

( ) President/chancellor
( ) Vice president/provost/vice provost or equivalent (non-CIO)
( ) CIO (or equivalent)
( ) Director of administrative computing
( ) Director of academic computing
( ) Auditor
( ) Other IT management
( ) Other administrative management
( ) Other academic management
( ) Other

1.4 I am personally very involved in central IT support for business continuity at my institution.

( ) Strongly disagree
( ) Disagree
( ) Neutral
( ) Agree
( ) Strongly agree

1.5 What best describes the budget climate of your central IT organization in the past three years?

( ) Decreasing budgets ( ) Flat budgets ( ) Increasing budgets

1.6 What best characterizes your institution in terms of adopting new technologies?

( ) Early adopter ( ) Mainstream adopter ( ) Late adopter

1.7 What best describes your institution's goals for IT?

( ) Provide reliable IT infrastructure and services at the lowest possible cost
( ) Provide appropriate IT infrastructure and services to different users, based on their needs
( ) Provide IT infrastructure and services that further the institution's strategic goals
( ) Provide IT infrastructure and services to create institutional competitive advantage

1.8 Is the senior-most IT leader (e.g., CIO) at your institution a member of the president/chancellor's cabinet?

( ) No ( ) Yes

1.9 Does your institution have a hospital that serves the general public?

( ) No ( ) Yes

1.10 What percentage of your students live in campus residences?

( ) Do not have campus residences
( ) Less than 25 percent
( ) 25–50 percent
( ) 51–75 percent
( ) 76–100 percent
( ) Don't know

1.11 Is your institution part of a university system or community college district organization?

( ) No ( ) Yes

Section 2: Institutional Perspectives on Business Continuity Planning

2.1_2.3 At my institution:

	Strongly disagree	Disagree	Neutral	Agree	Strongly agree	Don't know
2.1 Awareness of the need for business continuity planning is high.						
2.2 Awareness of the need for business continuity planning is higher today than two years ago.						
2.3 Senior management places high priority on business continuity planning.						

2.4_2.14 What are the primary drivers for business continuity planning at your institution? Select up to three.

[ ] 2.4 Threats specific to our geographic location
[ ] 2.5 Hazards arising from our institution's operations (e.g., nuclear reactor, virus lab)
[ ] 2.6 Institutional leadership mandate
[ ] 2.7 Demand from constituents (e.g., faculty, students, etc.)
[ ] 2.8 Audit requirements
[ ] 2.9 Regulatory compliance
[ ] 2.10 Keeping current with generally accepted business directions/best practices
[ ] 2.11 Awareness of recent global natural disasters (e.g., hurricanes, tsunami)
[ ] 2.12 Terrorism/homeland-security concerns
[ ] 2.13 A recent incident at our institution causing or threatening disruption to operations
[ ] 2.14 Other

2.15_2.22 What are the primary barriers to business continuity planning at your institution? Select up to three.

[ ] 2.15 Lack of adequate funding
[ ] 2.16 Lack of acceptable ROI
[ ] 2.17 Technology issues
[ ] 2.18 Lack of institutional leadership's support
[ ] 2.19 Business/academic units have not defined business continuity needs
[ ] 2.20 Lack of staff expertise
[ ] 2.21 Difficulty developing campus policies and procedures
[ ] 2.22 Other

2.23 Has your institution designated at least one senior executive who is responsible for institutional business continuity planning activities? <Required>

( ) No <Go to 2.25>
( ) Yes
( ) Don't know <Go to 2.25>

2.24 The senior executive responsible for institutional business continuity planning activities is:

( ) President/chancellor
( ) Executive vice president/chancellor
( ) Chief academic officer/Provost
( ) Chief business officer
( ) Chief of campus security/police
( ) CIO (or equivalent)
( ) Academic dean
( ) Other

2.25 Has your institution designated an emergency response team to manage the overall institutional response in the event of a disruption to normal operations? <Required>
( ) No <Go to 2.27>
( ) Yes
( ) Don't know <Go to 2.27>

2.26 Is central IT represented on this emergency response team?
( ) No ( ) Yes ( ) Don't know

2.27 Does your institution have an established office for institutional business continuity planning?
( ) No ( ) Yes ( ) Don't know

2.28 Has your institution undertaken a formal overall risk assessment to evaluate the events/threats—such as natural disasters, accidents, terrorism, etc.—that can cause interruptions to the institution's operations? <Required>
( ) No risk assessment anticipated <Go to 2.29_2.37; then to 2.63_2.65>
( ) Planned for the future <Go to 2.38_2.42; then to 2.63_2.65>
( ) Work is in progress <Go to 2.38_2.42; then to 2.43>
( ) Work is completed <Go to 2.43>

2.29_2.37 What are the primary reasons why your institution has not conducted a formal overall risk assessment at this time? Select up to three.
[ ] 2.29 Threats do not justify effort
[ ] 2.30 Benefits do not justify investment
[ ] 2.31 Prefer an ad hoc approach
[ ] 2.32 Lack of adequate funding
[ ] 2.33 Lack of institutional leadership's support
[ ] 2.34 Business/academic units have not defined business continuity needs
[ ] 2.35 Lack of staff expertise
[ ] 2.36 Difficulty developing campus policies and procedures
[ ] 2.37 Other

2.38_2.42 My institution's effort to complete an overall risk assessment:

	No	Yes	Don't know
2.38 Has been assigned a completion date			
2.39 Has been assigned staff			
2.40 Has been allocated funds			
2.41 Has executive or management sponsor			
2.42 Has participation from functional business/academic units			

2.43 Did your institution use or is it using a formal methodology to conduct its overall risk assessment?
( ) No ( ) Yes ( ) Don't know

2.44_2.61 Which functional areas have actively participated in developing your institution's overall risk assessment?

	No	Yes	Don't know	Not applicable
2.44 Academic affairs/provost				
2.45 Academic schools and departments				
2.46 Admissions				
2.47 Audit				
2.48 Business/administrative services				
2.49 Campus security/police				

2.50 Central IT				
2.51 Financial services				
2.52 Housing/residential life				
2.53 Human resources				
2.54 Legal counsel				
2.55 Library				
2.56 Office of emergency planning				
2.57 Public affairs				
2.58 Registrar's office				
2.59 Research administration				
2.60 Risk management				
2.61 Student affairs				

2.62 Our institution's overall risk assessment is kept up to date.
( ) Strongly disagree
( ) Disagree
( ) Neutral
( ) Agree
( ) Strongly agree

2.63_2.65 Does your institution have documented plans or processes that do the following?

	No	Yes	Don't know
2.63 Identify the probability of disruptive events/threats			
2.64 Assess the potential impact of disruptive events/threats on business and academic processes			
2.65 Prioritize risks from disruptive events/threats			

2.66 Does your institution have a formal, documented plan for overall institutional business continuity? <Required>
( ) No plan anticipated <Go to 2.68>
( ) Planned for the future <Go to 2.68>
( ) Work is in progress
( ) Work is completed

2.67 Does your institution have a formal process for updating its overall business continuity plan?
( ) No ( ) Yes ( ) Don't know

2.68 Does your institution provide departments/units with a framework for developing their own business continuity plans?
( ) No ( ) Yes ( ) Don't know

2.69_2.70 If central IT systems and services were not operational at my institution:

	Strongly disagree	Disagree	Neutral	Agree	Strongly agree	Don't know
2.69 Business units could carry out essential operations.						
2.70 Academic units could carry out essential operations.						

Section 3: IT Perspectives on Business Continuity Planning

3.1_3.4 At my institution, central IT is actively involved in business continuity planning conducted by:

	Strongly disagree	Disagree	Neutral	Agree	Strongly agree	Don't know	Not applicable
3.1 Overall institutional business continuity planners							
3.2 Business units							
3.3 Academic units							
3.4 Local IT units							

3.5_3.8 At my institution, central IT planning to support business continuity is aligned with the business continuity goals of:

	Strongly disagree	Disagree	Neutral	Agree	Strongly agree	Don't know	Not applicable
3.5 Overall institutional business continuity planners							
3.6 Business units							
3.7 Academic units							
3.8 Local IT units							

3.9 Has your central IT unit conducted an IT risk assessment to evaluate the impact that disruptive events/threats would have on IT systems and assets? <Required>

( ) No IT risk assessments done <Go to 3.11>
( ) For some IT systems and assets <Go to 3.10>
( ) For all IT systems and assets <Go to 3.10>
( ) Don't know <Go to 3.11>

3.10 Our IT risk assessment is kept up to date.

( ) Strongly disagree
( ) Disagree
( ) Neutral
( ) Agree
( ) Strongly agree
( ) Don't know

3.11 Does your institution have a documented inventory of central IT systems and assets? <Required>

( ) No inventory <Go to 3.13>
( ) For some central IT systems and assets <Go to 3.12>
( ) For all central IT systems and assets <Go to 3.12>
( ) Don't know <Go to 3.13>

3.12 Our inventory of central IT systems and assets is kept up to date.

( ) Strongly disagree
( ) Disagree
( ) Neutral
( ) Agree
( ) Strongly agree
( ) Don't know

3.13 Does your institution have a documented inventory of local IT unit systems and assets (i.e., those not controlled by central IT)? <Required>

( ) No inventory <Go to 3.15>

( ) For some local IT systems and assets <Go to 3.14>
( ) For all local IT systems and assets <Go to 3.14>
( ) Don't know <Go to 3.15>

3.14 Our inventory of local IT unit systems and assets is kept up to date.
( ) Strongly disagree
( ) Disagree
( ) Neutral
( ) Agree
( ) Strongly agree
( ) Don't know

3.15 The individual responsible for day-to-day management of IT planning to support business continuity is:
( ) CIO (or equivalent)
( ) Chief information security officer
( ) Full-time IT manager for business continuity support
( ) Director of administrative computing
( ) Director of academic computing
( ) Director of networking
( ) Other IT management
( ) Director of institutional emergency response planning
( ) Other administrative management
( ) Other academic management

3.16 Does your central IT unit have a standing committee that is responsible for business continuity planning activities?
( ) No ( ) Yes ( ) Don't know

3.17_3.29 Has your central IT unit documented procedures for the following, either as part of a formal plan or as a separate procedure?

	No	Yes, in plan	Yes, as separate procedure	Don't know
3.17 Declaring an IT emergency when disruption falls outside normal operating/troubleshooting bounds				
3.18 Activating/escalating IT emergency response				
3.19 Notifying appropriate parties of emergency				
3.20 Performing damage assessments				
3.21 Prioritization of systems for purposes of recovery				
3.22 Recovery of IT operations				
3.23 Moving necessary activities/equipment to alternate sites				
3.24 Transportation/logistical support for staff at alternate sites				
3.25 Notifying constituents of system status				
3.26 Returning activities/equipment to primary locations				
3.27 De-escalation of IT emergency response				
3.28 Declaring resumption of normal operations				
3.29 Evaluation of post-recovery IT environment (establishing "new normal")				

3.30_3.46 Which functional areas actively participate in developing your central IT procedures for business continuity?

	No	Yes	Don't know	Not applicable
3.30 Academic affairs/provost				
3.31 Academic schools and departments				
3.32 Admissions				
3.33 Audit				
3.34 Business/administrative services				
3.35 Campus security/police				
3.36 Financial services				
3.37 Housing/residential life				
3.38 Human resources				
3.39 Legal counsel				
3.40 Library				
3.41 Office of emergency planning				
3.42 Public affairs				
3.43 Registrar's office				
3.44 Research administration				
3.45 Risk management				
3.46 Student affairs				

3.47_3.48 How often does your institution carry out the following types of reviews of your central IT procedures to support business continuity?

	Never	On a regular basis	On an ad hoc basis	Don't know
3.47 Comprehensive review				
3.48 Component-level review				

3.49 Our IT procedures for supporting business continuity are kept up to date.

( ) Strongly disagree
( ) Disagree
( ) Neutral
( ) Agree
( ) Strongly agree

3.50 Which of the following best describes the status of a formal, documented central IT plan for business continuity and/or IT disaster recovery at your institution? <Required>

( ) No plan anticipated <Go to 3.51_3.59; then to 3.65>
( ) Planned for the future <Go to 3.60_3.64>
( ) Work is in progress <Go to 3.60_3.64>
( ) Work is completed <Go to 3.65>

3.51_3.59 What are the primary reasons why your institution does not anticipate formulating such a plan? Select up to three.

[ ] 3.51 Our people and processes are sufficient to meet needs
[ ] 3.53 Threats do not justify investment
[ ] 3.54 Lack of adequate funding
[ ] 3.55 Lack of institutional leadership's support
[ ] 3.56 Business/academic units have not defined business continuity needs
[ ] 3.57 Lack of IT staff expertise
[ ] 3.58 Difficulty developing campus policies and procedures
[ ] 3.59 Other

3.60_3.64 My institution's effort to complete a documented central IT plan for business continuity and/or IT disaster recovery:

	No	Yes	Don't know
3.60 Has been assigned a completion date			
3.61 Has been assigned staff			
3.62 Has been allocated funds			
3.63 Has executive or management sponsor			
3.64 Has participation from functional business/academic units			

3.65 What best describes central IT's goals for restoration of IT services in the event of a disruption to normal operations?

( ) Provide minimum acceptable restoration of IT services at the lowest possible cost
( ) Provide quick restoration of high priority IT services, then phase in lower-priority services
( ) Provide quick restoration of all IT services

Section 4: Recovery Objectives

Definition: A recovery time objective, or RTO, is the period of time within which the institution plans to restore a given system after suffering a disruption.

4.1 Does your institution have a formal process for establishing recovery time objectives for central IT systems?

( ) No ( ) Yes ( ) Don't know

4.2_4.17 Does your institution have documented recovery time objectives for the following central IT systems?

	No RTO documented	0-4 hours	5-24 hours	1-2 days	3-6 days	7-14 days	More than 14 days	Don't know	Not applicable
4.2 Institutional Web site									
4.3 E-mail									
4.4 Campus network									
4.5 Campus connection to Internet									
4.6 Voice telephony									
4.7 Purchasing									
4.8 Central finance/accounting									
4.9 Payroll									
4.10 Benefits administration									
4.11 Recruiting									
4.12 Admissions									
4.13 Student billing and payment processing									
4.14 Financial aid									
4.15 Student records/registration									
4.16 Course management system									
4.17 Library management system									
4.18 Grants management									

Definition: A recovery point objective, or RPO, is the maximum acceptable interval between a backup and a potential interruption, during which data will be lost. When a system is recovered, the RPO defines how old the restored data may be relative to the time of the interruption.

4.19 Does your institution have a formal process for establishing recovery point objectives for central IT systems?

( ) No ( ) Yes ( ) Don't know

Section 5: Awareness and Training

5.1_5.3 Please give us your opinion about the following statements:

	Strongly disagree	Disagree	Neutral	Agree	Strongly agree	Don't know
5.1 Business continuity practices are woven into the fabric of my institution's business operations.						
5.2 My institution communicates business continuity awareness issues to its faculty, students, and staff regularly.						
5.3 Support for business continuity is one of the top three IT issues confronting my institution today.						

5.4_5.6 Does your institution conduct formal business continuity awareness programs for constituents?

	Mandatory	Voluntary	No awareness program
5.4 For students			
5.5 For faculty			
5.6 For staff			

5.7_5.9 If you have such programs, give us your opinion about whether they have been effective for:

	Strongly disagree	Disagree	Neutral	Agree	Strongly agree	Don't know	Not applicable
5.7 Students							
5.8 Faculty							
5.9 Staff							

5.10_5.13 Does your institution provide central IT staff with the following types of training for business continuity support?

	No	Yes	Don't know
5.10 Formal training about overall institutional business continuity plans/procedures			
5.11 Formal training about IT plans and procedures to support business continuity			
5.12 Other			

5.13 How often does the central IT organization business continuity officer or CIO make a report to senior management about IT readiness to support business continuity?

( ) Never ( ) Occasionally ( ) Very often
( ) Seldom ( ) Often ( ) Don't know

5.14_5. 20 How does your central IT organization communicate information about business continuity to constituents (e.g., distributing plans and procedures, providing contact information, announcing tests, etc.)?

	No	Yes	Don't know
5.14 Dedicated business continuity Web site			
5.15 Other Web site			
5.16 Broadcast e-mail			
5.17 Newsletters			
5.18 Campus newspaper			
5.19 Press releases			
5.20 Other			

Section 6: Business Continuity Testing

6.1 Does your institution conduct tests to assess IT readiness for supporting business continuity? <Required>
( ) No <Go to 7.1>
( ) Yes
( ) Don't know <Go to 7.1>

6.2_6.7 How often does your institution conduct tests of the following types to assess IT readiness for supporting business continuity?

	Never	Less than once per year	Annually	2-4 times per year	5 or more times per year	On an ad hoc basis	Don't know	Not applicable
6.2 Full-scale rehearsal involving personnel, equipment, facilities, etc.								
6.3 Simulations (performing actions in response to scenario)								
6.4 Table-top tests (discuss/analyze response to scenario)								
6.5 Technical recovery testing at primary site (typically on campus)								
6.6 Technical recovery testing at alternate site (off campus or away from campus data center)								
6.7 Tests of supplier facilities/services								

6.8_6.11 Does your institution test IT readiness for supporting business continuity when the following events occur?

	Never	On a regular basis	On an ad hoc basis	Don't know	Not applicable
6.8 When implementing new equipment and systems					
6.9 When facilities changes take place					
6.10 When significant personnel changes take place					
6.11 When business continuity plans or procedures change					

6.12 Has your institution used third parties to develop tests?
( ) No ( ) Yes ( ) Don't know

6.13 Has your institution used third parties to evaluate the results of tests?
( ) No ( ) Yes ( ) Don't know

6.14_6.18 Please give us your opinion on the following statements about testing of IT readiness for supporting business continuity at your institution.

	Strongly disagree	Disagree	Neutral	Agree	Strongly agree	Don't know
6.14 Our tests are frequent enough.						
6.15 Our tests are challenging enough.						
6.16 We are able to get the right parties to participate in our tests.						
6.17 We formally assess the results of our tests.						
6.18 Results of tests are communicated to all appropriate parties.						
6.19 Results of tests are used to improve our business continuity plans and procedures.						

Section 7: Business Continuity Infrastructure and Technologies

Definition: A hot site is a space with appropriate connectivity, environmental infrastructure, and equipment in place for systems recovery in the event of a disruption that makes the primary operations site unusable.

7.1 Does your institution have at least one hot site capable of assuming key IT operations? <Required>

( ) Not planning to do <Go to 7.2_7.10; then to 7.14>
( ) Planned for the future <Go to 7.14>
( ) In development <Go to 7.11>
( ) Operational <Go to 7.11>

7.2_7.10 What are the primary reasons why your institution does not have a hot site? Select up to three.

[ ] 7.2 Do not believe a hot site is necessary
[ ] 7.3 Do not believe benefit justifies expense
[ ] 7.4 Lack of adequate funding
[ ] 7.5 We are not far enough along in our business continuity planning
[ ] 7.6 Lack of staff resources
[ ] 7.7 Lack of staff expertise
[ ] 7.8 Technical issues
[ ] 7.9 Lack of institutional leadership's support
[ ] 7.10 Other

7.11 Describe the geographic location of your primary hot site in relation to your institution's central IT operations.

( ) Same building
( ) Different building, same campus
( ) Off campus, less than 5 miles
( ) Off campus, 5–25 miles distant
( ) Off campus, 26–100 miles distant
( ) Off campus, more than 100 miles distant
( ) Don't know

7.12 Which best describes the status of your primary hot site?

( ) Institutionally owned/leased
( ) Owned/leased by other higher education institution
( ) Ownership/lease shared with other higher education institution
( ) Owned/leased by higher education system, district, or consortium
( ) Commercial site available by contract
( ) Owned/leased by public sector entity

( ) Other
( ) Don't know

7.13 Does at least one other higher education institution use this hot site?
( ) Yes ( ) No ( ) Don't know

Definition: A cold site is a space with appropriate connectivity and environmental infrastructure to which equipment can be moved for systems recovery in the event of a disruption that makes the primary operations site unusable.

7.14 Does your institution have at least one cold site capable of being provisioned to assume key IT operations? <Required>
( ) Not planning to do <Go to 7.15_7.23; then to 7.27_7.31>
( ) Planned for the future <Go to 7.27_7.31>
( ) In development <Go to 7.24>
( ) Operational <Go to 7.24>

7.15_7.23 What are the primary reasons why your institution does not have a cold site? Select up to three.
[ ] 7.15 Do not believe a cold site is necessary
[ ] 7.16 Do not believe benefit justifies expense
[ ] 7.17 Lack of adequate funding
[ ] 7.18 We are not far enough along in our business continuity planning
[ ] 7.19 Lack of staff resources
[ ] 7.20 Lack of staff expertise
[ ] 7.21 Technical issues
[ ] 7.22 Lack of institutional leadership's support
[ ] 7.23 Other

7.24 Describe the geographic location of your primary cold site in relation to your institution's central IT operations.
( ) Same building
( ) Different building, same campus
( ) Off campus, less than 5 miles
( ) Off campus, 5–25 miles distant
( ) Off campus, 26–100 miles distant
( ) Off campus, more than 100 miles distant
( ) Don't know

7.25 Which best describes the status of your primary cold site?
( ) Institutionally owned/leased
( ) Owned/leased by other higher education institution
( ) Ownership/lease shared with other higher education institution
( ) Owned/leased by higher education system, district, or consortium
( ) Commercial site available by contract
( ) Owned/leased by public sector entity
( ) Other
( ) Don't know

7.26 Does at least one other higher education institution use this cold site?
( ) Yes ( ) No ( ) Don't know

7.27_7.31 Describe your institution's current approaches to central IT data storage and recovery.

	Not used	Used for some systems	Used for many systems	Used for all systems	Don't know
7.27 Backup to media that is stored on campus					
7.28 Backup to media that is stored off campus					
7.29 Batch electronic vaulting via network					
7.30 Continuous data mirroring to direct-access device via network					
7.31 High-availability redundant transaction systems with failover capability					

7.32_7.36 When restoring operations following a disruption, how does your institution currently plan to replace central IT hardware that is damaged or unavailable?

	Not for any systems	For some systems	For many systems	For all systems	Don't know
7.32 Use redundant hardware reserved solely for this purpose					
7.33 Repurpose hardware from lower-priority systems (e.g., test environments)					
7.34 Acquire/lease new hardware via expedited shipping or Quickship process					
7.35 Acquire new hardware via normal purchasing process					
7.36 Commercial hot site					

7.37_7.47 Which of the following has your institution implemented or formally arranged to have available when needed?

	Not planning to do	Planned for the future	Work is in progress	Work is completed	Don't know
7.37 Special emergency Web site					
7.38 Alternate host for institutional Web site					
7.39 Alternate host for e-mail					
7.40 Alternate ISP					
7.41 Alternate voice telephony provider					
7.42 Pagers					
7.43 Walkie-talkies					
7.44 VOIP telephony					
7.45 Satellite phones					
7.46 Automated phone/e-mail notification system					
7.47 Backup power for central IT site(s)					
7.48 Institutional emergency command center					

Section 8: Incident Management

8.1 Does your institution have an IT emergency response team? <Required>

( ) No <Go to 8.3_8.6>
( ) Yes
( ) Don't know <Go to 8.3_8.6>

8.2 Who leads this team during an emergency?

( ) No assigned leader
( ) CIO
( ) Other specific IT manager
( ) Assignment rotates
( ) Other
( ) Don't know

8.3_8.6 Does your institution have documented protocols in place for the following?

	No	Yes	Don't know
8.3 Assigning powers to designated individuals to declare an IT emergency			
8.4 Notifying the IT response team of an emergency			
8.5 Notifying senior management of an emergency			
8.6 Providing backup communications channels for notification if standard channels are unavailable			

8.7 Does your institution have a designated spokesperson to make public statements regarding an IT emergency?

( ) No ( ) Yes ( ) Don't know

8.8 In an emergency, is central IT formally empowered to assume control over systems, facilities, or processes that it does not normally control?

( ) No ( ) Yes ( ) Don't know

Definition: A mutual aid agreement is a reciprocal arrangement in which participating institutions or organizations that are unaffected or not seriously affected by a disruption render assistance to other participants that have been more seriously affected.

8.9 Does your institution participate in formal mutual aid agreements? <Required>

( ) No <Go to 8.15_8.21>
( ) Yes
( ) Don't know <Go to 8.15_8.21>

8.10_8.13 With which of the following do you participate in formal mutual aid agreements?

	No	Yes	Don't know
8.10 Other higher education institution(s)			
8.11 Local government agencies			
8.12 State government agencies			
8.13 Other entities			

8.14 Does your central IT unit have documented plans or procedures in place to provide IT support to other participants in your mutual aid agreements when needed?

( ) No ( ) Yes ( ) Don't know

8.15_8.21 Please give us your opinion on the following statements about your institution.

	Strongly disagree	Disagree	Neutral	Agree	Strongly agree	Don't know
8.15 We keep contact information for IT emergency response personnel up to date.						
8.16 We keep contact information for non-IT emergency response personnel up to date.						
8.17 We keep contact information for faculty and staff up to date.						
8.18 We keep contact information for students up to date.						
8.19 We keep contact information for student next-of-kin up to date.						
8.20 We are prepared to handle a surge of inbound phone calls during an emergency.						

8.21 We are prepared to send a large quantity of outbound notifications to institutional constituents during an emergency.						

8.22_8.25 Rate the impact that the following contingencies would have on your central IT unit's ability to support business continuity during a disruption at your institution.

	Very little impact	Little impact	Moderate impact	Severe impact	Very severe impact	Don't know
8.22 Inability to gain access to primary IT facilities						
8.23 Inability of IT emergency response personnel to meet in person						
8.24 Inability to communicate with senior management						
8.25 Insufficient staff depth if key IT personnel were unavailable						

Section 9: Incident Experience and Effects

9.1 Has your institution experienced any disruptions to normal business and academic operations in the past five years that caused central IT to implement formal or ad hoc emergency response procedures? <Required>

( ) No <Go to 10.1>
( ) Yes
( ) Don't know <Go to 10.1>

9.2 How many such disruptions have occurred in the past five years?

( ) 1	( ) 4	( ) 7	( ) 10
( ) 2	( ) 5	( ) 8	( ) More than 10
( ) 3	( ) 6	( ) 9	( ) Don't know

9.3_9.18 Describe the impact of the following types of events that triggered an emergency response by central IT in the last five years.

Event	None	Impact on a few facilities/business processes	Impact on many facilities/business processes	Campus-wide impact	Campus- and region-wide impact	Don't know
9.3 Seismic — earthquake, tsunami						
9.4 Hurricane						
9.5 Tornado						
9.6 Flood						
9.7 Other severe weather						
9.8 Disease outbreak/pandemic						
9.9 Fire						
9.10 Electrical failure						
9.11 Hazardous materials spill						
9.12 Hardware failure						
9.13 Cooling/IT environmental failure						
9.14 Theft						
9.15 Cable cut						
9.16 Cyber attack						

9.17 Terrorism						
9.18 Other						

9.19_9.31. Has your institution experienced any of the following consequences from the disruptions that triggered an emergency response by central IT in the past five years?

	No	Yes	Don't know
9.19 Network unavailable			
9.20 Web site unavailable			
9.21 Communications (e-mail or phone) unavailable			
9.22 Business application unavailable			
9.23 Academic application, including course management system, unavailable			
9.24 Loss of access to primary IT facilities			
9.25 Loss of access to other campus facilities			
9.26 Damage to hardware			
9.27 Damage to software			
9.28 Damage to data			
9.29 Injury to faculty, staff, or students			
9.30 Loss of life			
9.31 Evacuation of campus			

9.32 Briefly describe the disruption that had the most serious impact, and your response to it.

_____

_____

9.33 Rate the impact of this specific disruption:

( ) Impact on a few facilities/business processes
( ) Impact on many facilities/business processes
( ) Campus-wide impact
( ) Campus- and region-wide impact

9.34 During this specific disruption, did central IT assume control over systems, facilities, or processes that it does not normally control?

( ) No ( ) Yes ( ) Don't know

9.35_9.45 Rate the performance of the following during this specific disruption.

	Poor	Fair	Average	Good	Excellent	Don't know	Not applicable
9.35 Communications infrastructure							
9.36 Communications process							
9.37 Business continuity plans and procedures							
9.38 Senior leadership							
9.39 IT leadership							
9.40 IT emergency response team							
9.41 IT staff							
9.42 Public affairs/media relations							
9.43 Technology availability							

9.44 Institutional emergency command center							
9.45 Alternate IT facilities							

9.46_9.47 The central IT response to this specific disruption:

	No	Yes	Don't know
9.46 Met institutional business continuity objectives			
9.47 Met central IT business continuity support objectives			

9.48_9.49 Following this specific disruption, central IT:

	No	Yes	Don't know
9.48 Assessed our response to the disruption			
9.49 Updated our documented business continuity plans and procedures as a result of the disruption			

Section 10: Funding

10.1_10.3 Please give us your opinion on the following statements.

	Strongly disagree	Disagree	Neutral	Agree	Strongly agree	Don't know
10.1 We have the necessary funding to deliver IT support for business continuity.						
10.2 We have the necessary staff resources to deliver IT support for business continuity.						
10.3 Senior management understands the costs of IT support for business continuity.						

10.4 Approximately what percentage of the central IT budget is currently dedicated to supporting business continuity, including staff costs and goods and services?

( ) 0%
( ) 1%
( ) 2%
( ) 3%
( ) 4%
( ) 5%
( ) 6%
( ) 7%
( ) 8%
( ) 9%
( ) 10%
( ) 11%
( ) 12%
( ) 13%
( ) 14%
( ) 15%
( ) More than 15%
( ) Don't know

10.5_10.8 How do you anticipate the following categories of central IT spending on business continuity will change over the next 12 months?

	Decrease more than 15%	-15%	-10%	-5%	0%	+5%	+10%	+15%	Increase more than 15%
10.5 Staffing									
10.6 Products									
10.7 Services									
10.8 Education/training									

10.9 What is the primary source of funding for IT upgrades and improvements related to business continuity?

( ) Augmentation to annual IT budget
( ) Reallocation within annual IT budget
( ) Annual contributions to a reserve fund
( ) Capital budget allocation
( ) Legislative allocation
( ) Bond issue
( ) Grants
( ) Other
( ) Don't know

Section 11: Outcomes

11.1_11.5 Please give us your opinion on the following statements.

	Strongly disagree	Disagree	Neutral	Agree	Strongly agree	Don't know
11.1 IT capacity to support business continuity at my institution is aligned with senior management expectations.						
11.2 My institution is prepared to restore centrally controlled systems in the event of a disruption.						
11.3 My institution is better prepared to restore centrally controlled systems in the event of a disruption than it was two years ago.						
11.4 My institution is prepared to restore locally controlled systems in the event of a disruption.						
11.5 My institution is better prepared to restore locally controlled systems in the event of a disruption than it was two years ago.						

11.6 What level of performance has your institution achieved in its IT readiness to support business continuity?
( ) We are at risk.
( ) We are adequate.
( ) We are leaders.
( ) We are exemplars.
( ) Don't know.

Section 12: Conclusion

12.1 May we contact you to obtain further insights or clarifications on your responses?
<Required>
( ) No <Go to 12.3>
( ) Yes

12.2 What is your e-mail address? _____

12.3 If you have any other comments or insights about IT readiness for business continuity, please share them with us.

_____

12.4 We are committed to continually improving our surveys. All comments are welcome and will be considered.

_____

You have reached the end of the survey. Thank you! Choose the "Review" button to review, revise, and print your answers (always print a copy of your completed survey and retain it for your records). Once this is done, submit the survey by clicking "Finish."

Full ECAR studies are available either through subscription or purchase at the ECAR Web site, http://www.educause.edu/ecar/ . If you have any questions or concerns, please e-mail ecar@educause.edu .

– END SURVEY –

APPENDIX D: Comparison of IT Readiness for Business Continuity instrument and BCPIT

IT Readiness for Business Continuity item	Corresponding BCPIT item and modifications
1.1 Survey ID	Excluded
1.2 Your name	31
1.3 Your position	32
1.4-1.11	Excluded
2.1-2.3	1; question has been rephrased
2.4-2.14	2
2.15-2.22	29
2.23-2.27	Excluded
2.28	3
2.29-2.37	4
2.38-2.42	5
2.43-2.61	Excluded
2.62	6
2.63-2.65	7
2.66-3.49	Excluded
3.50	8
3.51-5.0	Excluded
5.10-5.13	5.1
5.14-5.20	Excluded
6.1	5.2
6.2-6.7	15

6.8-6.11	16
6.12-6.19	Excluded
7.1	17
7.2-7.10	18
7.11	19
7.12-7.13	Excluded
7.14	20
7.15-7.23	21
7.24	22
7.25-7.26	Excluded
7.27-7.31	23; a cloud computing question has been added to the matrix of choices
7.32-8.25	Excluded
9.1	27
9.2	Excluded
9.3-9.18	28
9.19-12.4	Excluded

APPENDIX E: Letter of Invitation

Date

School head's Name
School
School Address Line 1
School Address Line 2

Dear *Head of School:*

My name is Kelly Mekdeci. I am the director of the Georgetown International Academy in Guyana and a doctoral candidate at Lehigh University, under the advisement of Dr. Ron Yoshida. I am conducting a dissertation that will examine the business continuity practices for information technology (IT) that are practiced in overseas international schools. The target sample for this study will be AASSA member schools.

In order to obtain accurate data, I wish to include as many AASSA schools as possible. I would greatly appreciate your participation. If you agree to take part, your role will be to complete a twelve-minute online survey about your school's current business continuity practices for IT. You also have the option of designating a member of your staff (e.g. technology coordinator, principal) to complete this survey on your behalf. I appreciate that you and your staff members are very busy, and will certainly value your participation in this study.

Strict confidentiality will be maintained throughout this study in accordance with the *Federal Policy for the Protection of Human Subjects* (Federal Register, 1991) and the *Ethical Principles in the Conduct of Research with Human Participants* (APA, 1982). Data will be reported with no identification of individuals or schools. Your participation is strictly voluntary, as is the participation of anyone you designate to complete the survey on your behalf. The only risk to your school is the potential breach of confidentiality, which I am taking specific steps to avoid. For example, school names will not be a part of the data. Therefore, if anyone should come in contact with the data, they would be unable to determine from which school or individuals it originated.

To indicate your willingness to participate in the study, please access the survey link that has been provided to you, and complete the survey or ask your designee to do so. Please retain this letter for your reference and information about informed consent. If you have any questions about the study, please contact me directly at my office at the Georgetown International Academy – 592.226.0770 or on my cell phone – 592.600.8347. You may also contact my advisor Dr. Ron Yoshida at Lehigh University – 610.758.6249. Any problems or concerns that may result from your participation in this study may be reported to Ruth Tallman, Office of Research, Lehigh University – 610.758.3024.

With sincere appreciation,

Kelly Mekdeci
Director,
Georgetown International Academy
Georgetown, Guyana

Ron Yoshida
Professor of Education
Lehigh University
Bethlehem, Pennsylvania

M.J. Bishop
Professor of Education
Lehigh University

Bruce Taggart
Professor of Education
Lehigh University

Leona Shreve
Superintendent (Retired)
Gilbert School District