Physical and Infrastructure Security IT

Carlos H. Ramos Santa
Master in Computer Science
Juan Ramírez, Ph.D.
Electrical & Computer Engineering and Computer Science Department
Polytechnic University of Puerto Rico

***Abstract* —** *This article summarizes all of the important aspects to consider when managing physical security and IT infrastructure issues. To include natural disasters, environmental, technical and threats caused by human interaction and errors. There are various physical security precautions and mitigation measures that can be implemented to prevent, minimize, and mitigate IT disasters in any enterprise. These include access control, preparation and simulations for an upcoming natural disaster, recovery and mitigation of security gaps, and accounting for human factor issues that create problems. This article also explains how to react and recover from a physical security infiltration. Implementing technical tools like Unified Threat Management (UTM). To finalize this article described the implementation of a security program; a company must conduct a threat assessment, planning and implementation of the plan to determine the amount of resources you can assign to physical security and resource allocation against different kind of attacks.*

Key Terms *— Cloud Storage, Contingency plan, Disaster recovery plan, Unified Threat Management*

INTRODUCTION

The most important asset of a company is the information that it safeguards. Protecting this information is a very critical task for any organization. The security of information for several decades was not as difficult as it is today because most computer systems were mainframes that were located in specific places and only few persons anyway knew how to operate them. However today computers are everywhere and of different types such as Servers, laptops, PC and mobile [1].

All these kinds of devices are connected to each other through cable or Wi-Fi for enterprise and remote, taking computers and resources outside the institution. Providing adequate protection of these computer systems, networks, facilities, and employees has become an overwhelming task for many companies. There are many types of threats that can affect an organization's information. For example; environmental, natural disasters, human and techniques threats grow on a daily basis. Each of these above mentioned threats can be prevented or if not preventable mitigate the effects from them. For example, we have natural hazards including hurricanes, earthquakes, floods, storms, etc. These types of natural disasters cannot be prevented but it can be mitigated with good preparation process. Another serious threat the environmental, when guarded information must comply with established environmental parameters that maintain secure data. The third serious threat the technique, this refers to the electric power and the electromagnetic emissions. Finally the human threat, these threats can be access unauthorized information, malicious attacks and misuse of resources. For information systems, the role of physical security is to protect physical assets that support the storage and processing of information. Physical security should prevent damage to the physical infrastructure that supports information systems. In general terms the infrastructure includes: hardware, physical installation, support facilities and personnel information system.

THREATS TO PHYSICAL SECURITY

There are different types of situations that may constitute a threat to the physical security. It is important to understand the risks of these threats to the information systems so that those responsible for managing security can establish preventive

measures that minimize damage. We classify these threats in the following categories: natural disaster, environmental threats, technical threats and threats of human origin.

Natural Disaster

A natural disaster is an event of great magnitude caused by nature. Some of them are tornadoes, hurricanes, earthquakes, storms, and floods. These types of events cause great damage to the structure and the IT staff. It is possible to assess the risk of several types of natural disasters and take proper precautions for catastrophic loss caused by natural disasters by doing this, damage is dramatically diminished. A tornado can exceed the winds of a hurricane, but it only damages anything that is caught in its path. Physical structures damages and loss of electricity in those affected areas can result from this natural disaster. A hurricane, depending on its size and strength, can also create structural damages with power loss in a much larger area compared to a tornado. An earthquake of great intensity does not provide areas of safety like tornados and hurricanes by moving away from them. Earthquakes can destroy the IT infrastructure completely. Flooding is a concern in areas that are subject to them. The damage can be severe, with long term effects and recovery period.

Environmental Threats

Another threat that must be carefully considered is the inadequate temperature and humidity in the physical facilities. All electronic equipment is designed to operate within a certain temperature range. The majority of the computer systems must be maintained between 50 and 90 degrees Fahrenheit [2]. High humidity also poses a threat to the electrical and electronic equipment. Prolonged exposure high humidity may result in corrosion. Condensation can endanger the magnetic media storage and optical areas. The condensation may cause a short circuit. Electronic equipment has a temperature where the medium would begin to be damaged, the control of the room temperature in the Computer Center is very important. The control of humidity in a computer center and its equipment is essential in sustaining an optimal state of operation. The humidity cannot be very high or low. In general, humidity should be between 40% and 60% for adequate control [3]. Perhaps the most fearsome physical threat is fire. It is a threat to human life and property. The threat is not only the direct flame, but also heat, the release of toxic gases, damage caused by water from fire and smoke damage. Another element that may affect the area of information technology is dust. The size of these dust particles can be as small as a few microns or as large as hundreds of microns. The larger and denser particles tend to settle, while the smaller and lighter can stay in the air indefinitely. Dust particles may contain moisture, organic matter, various minerals, or various chemical products. All this can affect the reliability time and the common life of electronic equipment that are overexposed to dust [4].

Technical Threats

Electrical power is essential for the functioning of an information system. All electrical and electronic appliances in the system require energy, and most require uninterrupted power supply. Utility power problems can be grouped into these three categories; low voltage, overvoltage, and noise. The low voltage occurs when computing teams receive less voltage than they need to operate normally for an extended period of time, problems in the supply, and power outage. The majority of computers are designed to withstand prolonged reductions in voltage of about 20% without having to turn off and without malfunction. These drops or interruptions of energy lasting a few milliseconds trigger a " shutdown " of the system [5]. In general, the system does not suffer damage, but service is interrupted. The overvoltage is much more dangerous than the drop in voltage. The overvoltage is a prolonged increase in tension where the power comes from. These surges can cause much damage and rapidly damage the equipment. A high-voltage can destroy components, including processors and memories.

Noises, in many cases, these non-essential signals may be through the power line circuits and interfere with the signals inside electronic devices, causing errors. Possible types of line noise interference are Electromagnetic interference (EMI) or Radio Frequency Interference (RFI).

Physical Threats Caused by Humans

The latest threat to physical security is caused by humans. Threats caused by humans are more difficult to manage than with the technical and environmental threat. The threats caused by humans are less predictable than other five types of physical threat. Man-made threats are specifically designed to overcome the prevention measures or seek the most vulnerable point. We can group these threats in the following categories: access not authorized theft, vandalism, and misuse. Unauthorized physical access: non-employees should not be in the building or complex of buildings, if not accompanied by an authorized person. This leads to computer theft and theft of data by copying. Theft of valuable information can be in the hands of an external or internal source which has obtained unauthorized access. The threat of vandalism includes the destruction of the equipment and the destruction of data. The misuse of hardware or software includes the abuse of resources by those who are authorized to use them, as well as the use of resources by persons not authorized to use.

PREVENTION OF PHYSICAL SECURITY AND MITIGATION MEASURES

To protect computers for the staff using them a well-designed and administered physical facility is needed. The process of managing the physical environment includes the definitions of the physical needs of the place, the selection of appropriate facilities and the design of effective processes to control environmental factors and physical access management [1]. The following factors lead to the implementation of good security plan to mitigate a natural disaster, environmental and technical threats, and human error.

Prepare for a Natural Disaster

As stated at the beginning, natural disasters cannot be prevented, but you can be prepared when one arises. Each of these natural disasters can be classified as incidents. We can classify responses to incidents, disaster recovery and planning of continuity of the business, as components of the Contingency plan. Contingency plan (CP) is the planning carried out by the entire organization for the preparation, response and recovery from events that threaten the security of assets and information on the Organization, and the subsequent restoration of the normal processes of the company's operations. Incident response planning (IRP) is the process of planning related to the identification, classification, response, and recovery from an incident. Disaster recovery plan (DRP) is the process of planning related to the preparation and recovery from a disaster, whether natural or artificial. Business continuity planning (BCP) is the process of planning related to the warranty that the critical functions of a business to continue if a catastrophic incident or disaster occurs. The main functions of these three types of planning are: IRP focuses on the immediate response, but if the attack intensifies or disastrous process changes to BCP and disaster recovery. DRP normally focuses on the restoration of the system after disasters occur, and as such, it is closely related to the BCP. The Business continuity planning describes the restoration of critical business operations during a disaster affecting operations at the primary site. If a disaster has made the current location of the company's useless for continuous operations, there must be a plan that allows the business to keep running [6].

There are six steps in the process of contingency planning. The first is the identification of mission critical business functions. The second is the identification of resources that support critical functions. The third is the possible contingencies or disasters forecast. Then, a Fourth is the selection of contingency planning strategies. The fifth is the

application of contingency strategies. The latter is testing and revision of the strategy [6].

Prepare for Environmental and Technical Threats

Environmental factors such as heat, humidity, airflow, smoke and electricity are equally devastating to the server room equipment and operations of IT as any other kind of threat. To prevent this threat, it is mainly a matter of appropriate sensors that control the environment and the maintenance of the power supply. Register and graphically analyze these measurements from the sensors over time this can help administrators identify trends such as temperature peaks during peak operation or fluctuations when building's HVAC systems are limited on weekends. To maintain a network room or data center temperatures have to be set where these computers can work without having to endure a warming problem. (CRAC) unit is a device that monitors and maintains the temperature, the distribution of air and moisture. Another system that helps control the temperature, humidity and cleaning of the air for a data center is the air handler unit (AHU). The most important components of this device are: filters that help to clean the air, the cooling elements and humidifier that provides cooling for changing the temperature and humidity of the air flow of the data center. To deal with Fire and smoke install hand extinguishers and fire detectors, provide good maintenance to equipment, place equipment strategically with written emergency procedures and instructions with a certified Fire Department inspection of the facility. The Clean Agent Fire Suppression system are the most appropriate fire extinguishers for a data center, these can be activated by smoke, infrared, or ultraviolet detectors or manual pull stations. Some examples are: FM-200, 3M Novec 1230 Fire Protection Fluid and FE-13. To deal with the technical challenges such as lack of electricity, backup power surge equipment should be provided and should be connected to each of the network equipment. If the power interruption is longer than expected then all of the equipment and data center must be connected to an external generator that automatically starts when needed.

When an incident occurs that affects the company's information system, the most important element of recovery is the retrieval of the lost information. This is called retrieval redundancy, redundancy does not undo any breach of confidentiality, the theft of data or documents, but it provides for the loss of data. The ideal environment would be that all important data in the system must be available outside the building and updated as closely as possible to real time.

With Broadband connection, you can have your Backup in two different methods to choose from; "Online Backup" with companies such as Carbonite, Acronis, IDrive and Mozy, or "Cloud Storage" with companies like Dropbox, Google Drive, Microsoft Skydrive and Amazon Web Services. A "hot site" should be created out of the place that would be ready to take charge of operation instantly and have at its disposal a copy almost real-time operational data [7].

The recovery of the physical damage to the equipment depends on the nature of the damage. Fire, smoke and water damage can leave hazardous materials that must be thoroughly removed from the place prior to normalize operations. In many cases, this requires to take recovery specialists disaster outside the Organization to do the cleaning.

Human Factor

The conduct of the employees in a company is critical to ensuring and maintaining the computer security system and information assets. No matter the security system implemented the adverse actions of employees would endanger the security of the information systems. The main problems associated with the behavior of employees are errors and omissions, fraud and actions of disgruntled employees. Understanding the importance of the appearance of safety, training and education programs can reduce the problem of error and omissions. These programs can serve as a deterrent to fraud and actions by disgruntled

workers, informing them of their responsibility for their acts and the penalties for endangering the security of the company. Employees cannot be expected to follow the policies and procedures that are not aware. Employees can claim ignorance when caught in a violation, if not trained properly by employers. Therefore it is important to create policies and rules in writing to provide to the employees. The existence of security policies is essential to the company practice and drills of their physical security program. Security policies define the acceptable behavior and practices and expected responsibilities. Without written rules, users and administrators are left by themselves to decide important issues related to security. Without policies in writing, the employees are free to assume that a task can be completed in any form without security precautions. In addition employees may assume that physical security is the responsibility of someone else and believe that they can commit a security breach to the information system because they were not informed officially. The complete set of policies should be written in a clear and concise manner, but it must be comprehensive. For a large company, the policy document will be daunting, especially for non-technical staff. For this reason, it may be preferable to create a few documents divided by specialty and aimed at different groups of employees. Finally, the use of e-mail and the Internet is very common in companies today. It is therefore very important to establish clear policies that specified work related areas of usage. For example, the use of the internet must be used by employees solely for the purpose of carrying out the company's business.

IT INFRASTRUCTURE SECURITY

Protect the company's information every day; it is complicated due to the fact that complex methods are increasing to gain access to company information by malicious individuals. For this reason companies are investing more to maintain the security of their data in order to deal with the present and future challenges. This protection must be in Logical and Physical form.

Physical Security

Physical Security are procedures and controls put in place to prevent intruders accessing physically a system or installation.

There are some devices that can be implemented as part of physical security. The first is Closed-circuit television (CCTV); a CCTV is the use of video cameras that transmit a signal to a limited set of monitors. The purpose of the CCTV is to detect, evaluate and/or identify unauthorized persons. Another element that should be assessed is if you work indoors or outdoors, visual monitoring, of aerial fields, large or small areas, and last evaluate lighting to integrate with other controls of physical security, such as guards, IDS, and alarms. All of these described factors above must be evaluated before buying a product for CCTV purposes. There are many different types of cameras, lenses, and monitors to be considered for CCTV. It is important to understand what is expected of this physical security control, so that you can purchase and apply the correct type. CCTV is composed of cameras, transmitters, receivers, a recording system, and a monitor. The camera captures the data and transmits it to a receiver, which allows the data to be displayed in a monitor. The data is recorded so that they can be reviewed at a later time, if necessary. Most of today's CCTV cameras use sensitive chips to activate the light Charge-coupled device (CCD). CCD is an electrical circuit that receives light from the entrance of the lens and converts it into an electronic signal, which then appears on the monitor. Images are focused through a lens to the surface of the CCD chip, which is the power optical image representation. Another element for physical security is security guards who are protecting the assets of the companies who control access to the facilities. Mostly the company hires a private security company to provide these functions. Security guards monitor the CCTV monitors, and

established recorded entrance procedures with ID Cards to control access to a restricted area.

Physical Access Control

Information is a company's most important asset and people is one of most dangerous threats to such asset. To minimize those threats, we need to establish control measures or security protections, which are controls that we can establish to safeguard important information. An example of such information control measures is Electronic systems, which control people's access to it. User authentication is the first line of defense to protecting the information.

A system identifies a user in four ways. First, a password, which people knows. There are personal identification numbers (PIN) or answers to a set of established questions. The most positive aspect of a PIN is that the person that knows the password is the one that can get into restricted areas but, the most negative aspect is that if someone with bad intentions knows the password could have access to the areas that he or she is not authorize to get into. The second are electronic keycards, smart cards and physical keys. They are objects that the individual possesses that give him access to a limited or controlled area. The most positive aspect of the keycards or smart card is that only the person that has the card is the only one that can get into a restricted area and, the most negative aspect is when the card is stolen or lost. If a person finds the card, they will have access to the unauthorized areas. The third is static biometrics such as fingerprints, facial characteristics, hand geometry, retinal pattern and iris. The most positive aspect of static biometrics is that they are very secure and only the person that has those specific and unique characteristics can get in to the restricted areas. The most negative aspect is that many times, people are reluctant to let a device read the pattern of their retina, fingers or even the geometry of their hands. This lack of enthusiasm has diminished the widespread use of biometric systems in our society. The enrollment phase requires action during several times to capture a clear and unique record. People do not particularly love the biometric method because they take more time and energy than the identification card. When a person attempts to be authenticated by a biometric system, sometimes they will be prompted to complete the action on several occasions if the system was unable to get a clear reading of an iris scan or geometry of the hand. The last one is the dynamic biometrics, for example voice recognition and digital Signature. The most positive and negative aspects of the dynamic biometrics are the same ones as the static biometric ones [8].

To mitigate the most negative aspect of electronic control accesses, we need to combine two or three different control access methods. How many methods you need to combine depends on the security levels that the area requires. For example, most websites require only one method to get in. For some of the DOD websites, you need to use a different method. For example, to get into a restricted webpage of the Army Knowledge Online (AKO) website you need to use a password and a smartcard. In that situation, you use what you know and what you have. There are very sensitive areas like financial, human resource and classified information in which you need three different methods to access the information.

Logical Security

Logical security is one of the most discussed topics these days concerning the security of the companies. We have the example of the PlayStation Network' Data Center that was attacked located in San Diego, California. Sony Entertainment Network shut down the PlayStation Network and Qriocity services on 20 April 2011, in order for the company to undergo an investigation and make enhancements to the overall security of the network infrastructure [9]. The PlayStation Network (PSN) breach had an estimated lost around $171 million [10].

The following security measures were implemented:

- They worked closely with several respectable security businesses.

- The company has implemented new security measures that strengthen the safeguards against unauthorized activity.
- The company has made significant enhancements to the data security, including updating and adding advanced security technologies, additional software monitoring and penetration and vulnerability testing, and increased levels of encryption and additional firewalls.
- The company also added a variety of other measures to the network infrastructure including an early warning system for unusual activity patterns that could signal an attempt to compromise the network [9].

When we talk about network security we must mention the term Unified Threat Management (UTM). UTM is a security platform solution that consolidates important applications of network security like firewall, VPN, intrusion prevention, and antivirus, Spam blocking, Spyware prevention and URL filtering in the same tool. UTM protects against different attacks such as: Spyware, Trojans, Worms, Web exploits, Viruses, Spam, Blended threats, Bots, SQL injections, Buffer overflows, DoS/DDoS attacks and Policy violations.

The advantages of UTM consist of having everything in a single device costs less than buying multiple dedicated systems. UTM's reduces the maintenance costs due by having only one device to support. It also reduces the overall space used because you don't have to use one device for each of the security threats. One power supply means less power used and less lost while reducing line voltage to the levels network devices use. Finally, many features of the UTM device are designed to work together without leaving holes in your protection or creation of interoperability challenges. The disadvantages of UTM are: having several services in one device could lack some of the more important features a dedicated box provides. If UTM fails, all of network security system can crash. Finally, if there is an attack on different fronts at the same time on a large scale, it can affect the overall performance of the network [11].

Nowadays companies increasingly use remote access to connect to customers, and employee that are physically located outside the enterprise or remotely connect through the internet. For this reason it is necessary to protect those data travelling through to a public network. Virtual Private Networking (VPN) is a method by which allow users to have access to the internal network of an organization over the internet in a safe way. A VPN provides users who are not in the internal network, secure access to it resources. The way that works is the creation of tunnels that wrap those packets to send them across the Internet destined for the internal network and then encrypting data packets. It is also very important to use the Hypertext Transfer Protocol Secure (HTTPS) Protocol. This communication protocol ensures that sensitive information safe social, number of credit card, etc. arrives safely without being intercepted.

Figure 1 gives an example of a medium enterprise IT infrastructure with the implementation of an UTM (Unified Threat Management) Solution. Traffic regenerated from the internet inside the corporate Services will be manage and filter by the External Firewall and according with the policies in place by the ISO and in compliance with industry standards and regulatory organizations, Services like the IPS (Intruder Protection Service), Antivirus Server, Gateway Anti-Spam service and VPN service, inspect, filter, manage, blocked and reports attacks and vulnerabilities associated to this traffic in real time and in an active way in order to protect the Corporate network and therefore the integrity of its data and assets. VPN Client to Server (SSL) and VPN Site to Site (IKE) services are managed at the External Firewall and ensure this traffic are encrypted and secure from the internet vulnerabilities. At the same time traffic generated from inside the corporate LAN is managed and filtering effectively by the Internal Firewall using the UTM features of Web Filtering, Data Leak Prevention and Load Balancing Service.

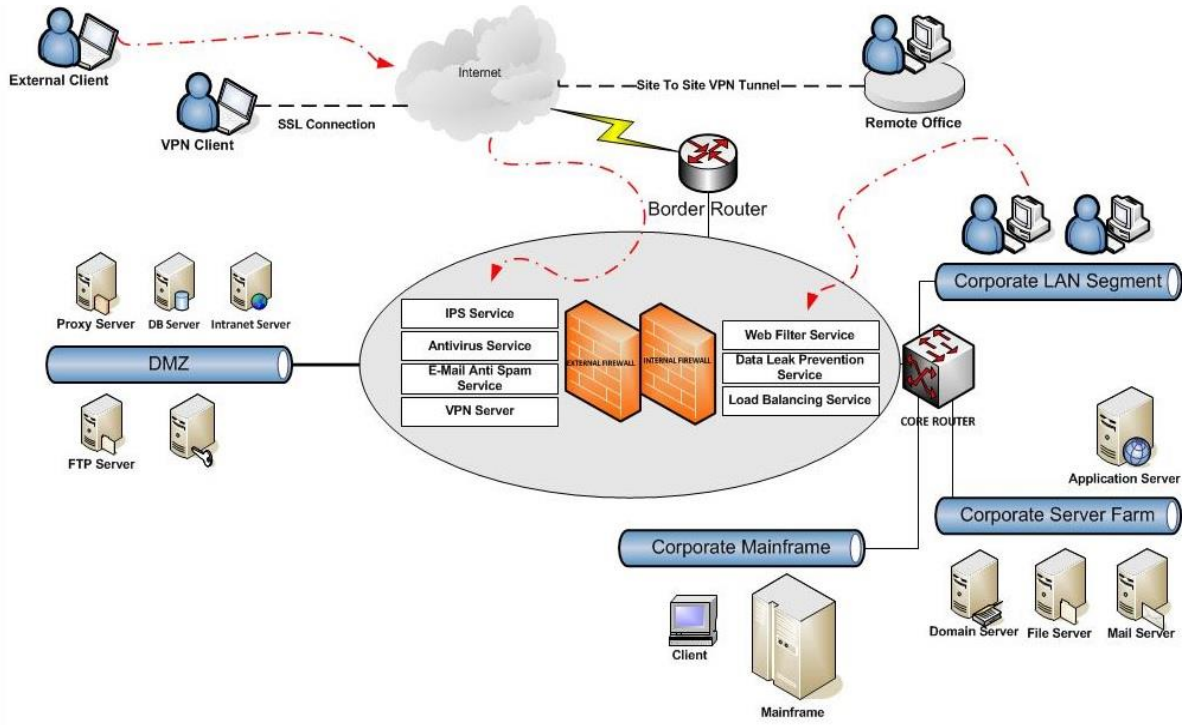

Figure 1
Medium Enterprise IT Infrastructure

This ensures that traffic is scan for data security breach and optimized for maximum bandwidth optimization. The UTM has a customized OS holding all the security features at one place; wish can lead to better integration and throughput than a collection of disparate devices.

SECURITY TESTING PLAN

It is good to have all sorts of equipment which helps to deal with emergency situations, but people also need to be properly trained to know what to do when an emergency occurs. Evacuation and emergency response plans should be developed and put into action. The plan should be documented and be accessible when a crisis occurs. People who are assigned to specific tasks should be trained and informed on how to complete tasks while performing drills that simulates different types of emergencies. Training exercises and drills must be executed at least once a year, and the entire program must be continuously updated and improved. Tests and exercises prepare staff for situations that need immediate response during an emergency. These tests and exercises also point to issues that were not planned for in a previously designed planning process. The exercise must have parameters that are found in a normal company day before the implementation of an emergency plan setting that execute alarms to implement contingency procedures. The test team must agree on what needs to be tested and how to correctly determine the success or failure of the training exercise. The team must agree on the time and the duration of the exercises, who will participate in the exercise, who will receive assignments, and what measures should be taken. This includes a full listing of employee names and identification for evacuation purposes. This list is for the team responsible for this task to ensure that no one is left inside the company.

INFORMATION SECURITY AUDIT

Once all systems of information security are implemented and tested the next step is to audit them. The company must have external and internal auditors to ensure that all established controls and

security systems are working as plan. Each security systems such as Disaster Recovery, Business Continuity, Physical Security and Logical Security Plan must be continually verified by auditors and any changes to the system must be informed to update all documents relating to them.

There are two important associations where you can find guides everything relating to information security and audit, these are: Information Systems Security Association (ISSA) and the Information Systems Audit and Control Association (ISACA). There are standards aimed to serve as a basis for audits of computer science. One of them is COBIT (Control Objectives for Information and Related Technology), within the objectives defined as parameter, is guaranteeing the security of systems. COBIT standards include the COBIT 5 for Assurance and COBIT 5 for Information Security [12]. In addition to this standard the ISO 27002 standard (Information technology - Security techniques - Code of practice for information security management), can be used as guidance as an international code of good practice for information security, it is also a guideline for audit support of other information security standards that define the requirements for audit Information security management system, as it is the ISO 27001 standard that defines how to organize the security of the information in any type of organization and ISO 27005:2011 (Information technology - Security techniques - Information security risk management) provides guidelines for information security risk management and is applicable to all types of organizations which seeks to manage risks that could compromise the security of the Organization's information [13].

REFERENCES

[1] Harris S, "Physical and Environmental", *All in One CISSP Exam guide*, Fifth Edition, 2010, pp. 401-402.

[2] Stallings W, et al., "Physical and Infrastructure Security", *Computer Security: Principles and Practice*, 2008, pp. 431.

[3] Stallings W, et al, "Physical and Infrastructure Security", *Computer Security: Principles and Practice*, 2008, pp. 432.

[4] Computer Dust Solutions LLC (2009). Special Report: Effects of Dust on Computer Electronics, and Mitigating Approaches. Retrieved December 3, 2013 from http://www.computerdust.com/downloads/special_report_on_the_effect_of_dust_on_electronics.pdf.

[5] Stallings W, et al, "Physical and Infrastructure Security", *Computer Security: Principles and Practice*, 2008, pp. 434.

[6] Whitman M, et al, "Contingency Planning and its Components", *Principles of Incident Response and Disaster Recovery*, 2007, pp. 23-25.

[7] Information Week (2012). Online Backup vs. Cloud Storage. Retrieved October 10, 2013, from http://www.informationweek.com/consumer/online-backup-vs-cloud-storage/d/d-id/1107440?

[8] Whitman M, et al, "Security Technology: Access Control Devices", *Principles of Information Security*, Third Edition, 2009, pp. 338-342.

[9] PlayStation Network (2011). PlayStation Network Restoration Begins. Retrieved October 10, 2013, from http://uk.playstation.com/psn/news/articles/detail/item369506/PSN-Qriocity-Service-Update/.

[10] IEEE Spectrum (2011). Sony PlayStation Breach Costs Estimated to be $171 Million. Retrieved October 13, 2013, from http://spectrum.ieee.org/riskfactor/telecom/internet/sony-playstation-breach-costs-estimated-to-be-171-million-

[11] GWI Blog (2013). The Pros and Cons of Unified Threat Management. Retrieved November 7, 2013, from http://www.gwi.net/policy/blog/the-pros-and-cons-of-unified-threat-management/.

[12] ISACA Org. COBIT 5 Product Family. (Retrieved December 2, 2013, from http://www.isaca.org/cobit/pages/product-family.aspx.

[13] ISO Org (2013). ISO/IEC 27005:2011 Information technology -- Security techniques -- Information security risk management. Retrieved November 11, 2013, from http://www.iso.org/iso/catalogue_detail?csnumber=56742.