International Journal of Cyber Criminology
Vol 14 Issue 1 January – June 2020

A Basic Principle of Physical Security and Its Link to Cybersecurity

Seungmug (Zech) Lee[1]
The University of Texas at Arlington, United States of America

Abstract

The need for security is human nature and instinct. It is about our survival and security. Humans have practiced it as a natural reaction to our surroundings. Historically, physical security has existed in the earliest known forms of prehistoric civilizations. Many traditional principles and practices are still used and valid. What has changed is technology. Technology can be applied as a powerful tool in well-conceived physical security programs as well as the cybersecurity field. Fundamental security concepts and their practical measures are as old as human beings' nature for survival and protection, as well as new technologies that are improving these basic concepts and applications. The world of computers and information are constantly changing. Change exposes vulnerabilities. Security and IT professionals are facing challenges and problems targeting cyberspace and organization's information by gaining unauthorized access to breach security lines. Both traditional security professionals and technology-oriented IT and cybersecurity professionals must work together to protect the organizations and the individuals they serve by utilizing and applying the same principles of layered security protection lines in both physical and cyber worlds.

Keywords: Physical security, Cybersecurity, Four layers of security defense, Technology.

Introduction

The need for security is human nature and instinct. It is for our safety and survival. Since the time human beings came into existence, the practice of some form of security has been a natural reaction to our surroundings. Historically, physical security has existed since the earliest known forms of prehistoric civilizations. For example, the prehistoric hunter and food gatherer limited physical security to the safety and protection of persons and their social arrangements. As animal husbandry evolved alongside agriculture, land, animals, buildings, and crops became central in the lives of our ancestors, which required better and sustainable protection and safety. Around the time of 3000 B.C., people dwelled in settlements complete with streets, squares, and mud-brick houses centered around a palace-like structure (Collins, Ricks, & Van Meter, 2015; Johnson & Ortmeier,

[1] Ph. D., Associate Professor, Department of Criminology and Criminal Justice, The University of Texas at Arlington, Arlington, Texas, USA. Email: seungmug.lee@uta.edu

2018; McCrie, 2016; Smith, Schmalleger, & Siegel, 2017) with various protection devices and technology.

Technology has been applied as a powerful tool in well-conceived physical security programs. Contemporary physical protections depend on electronic components and systems to achieve security objectives. Technology performs complex monitoring operations and possesses control features beyond the capacities of individual security personnel. Innumerable developments and advances in technological communications, sensing, and computing have reshaped the means and quality by which security services are performed. The cybersecurity field has also become a subject of such technological developments. Today, the overall security practice and industry are not just a single entity. Rather, they are a series of internal and external commercial activities that sometimes overlap each other but which are generally distinct, including traditional security services (e.g., guarding, alarm monitoring, investigations, and escorting) and technological security services (e.g., cybersecurity technology and software, computer hardware, and information protection measures). Government at all levels—federal, state, and local—has become a major consumer of security services and products, and it is true even for government units that provide criminal justice and emergency response services to the public (McCrie, 2016).

This article will discuss the brief historical background of traditional physical security and its groundwork to imply the security developments in modern day culture and the field of cybersecurity. The discourse includes the definitions of security, together with two major themes, physical security and cybersecurity, followed by the principles of physical security and their applications in contemporary society and the discussion of their link to cybersecurity.

1. Definitions of Security

Security can be defined in numerous ways, depending on its focus and direction. The concept and understanding of security have evolved progressively throughout the history of human civilizations around the world, designed and advanced by a wide variety of institutions and cultural developments. In a broad perspective, McCrie (2004, p. 11) argued that "… security is defined as the protection of assets from loss. The proposition of the importance of security is based on the premise that vulnerability eventually is exploited or results in systematic declension." Here security implies three fundamental aspects: the object of protection, the method of protection, and the need for protection. Security exists to protect the assets which include various forms of items and possessions (Smith et al., 2017). Among them are humans, the most valuable asset to protect. Security also requires diverse methods and techniques to be implemented for the protection of items and possessions. The third aspect of security is the need for protection. It stems from losses that occur against the protected items and possessions. It can be loss of lives of humans and animals, injury to humans, damage of constructed buildings, malfunction of equipment, and so forth. Such loss can be inevitable because of vulnerabilities to which all items and possessions are exposed.

Another definition described by Fischer, Halibozek, and Walters (2013, p. 3) argued that security "implies a stable, relatively predictable environment in which an individual or group may pursue its ends without disruption or harm and without fear of disturbance or injury." Here, the goal of security is to create the environment which is supposed to be stable, maintaining the constant status of normal routines and lives from various sources of

disruptions and disturbance, such as natural and man-made disasters (Johnson & Ortmeier, 2018). Just like how we predict and expect a warm spring and a hot summer right after a cold winter, when the stable and secure environment is settled down, then the members of such settings can be better predictable toward unpredictable futures in amassing available resources and practicing schemes in order to manage them, not only to survive but to mitigate and minimize loss so as to be prosperous. When we repeat such a short-term practice, it can help us to be able to predict a long-term future and to plan to prepare ourselves for the future.

The subject of a secured environment is an individual or group of people. A secured environment which is created by a collective effort has paved the way for human beings to pursue our ends, which include protection, freedom, happiness, and prosperity by means of controlling any possible disruption or harm as best as possible. Such disruption can result from two major sources: man-made disasters (e.g., homicide, robbery, burglary, auto theft, cybercrime, mass shootings, and so forth) and natural disasters (e.g., volcanic eruptions, earthquakes, hurricanes, floods, wildfire tornados, and other extreme weather conditions) (Johnson & Ortmeier, 2018; Smith et al., 2017). The harm from innumerable disasters may include various types of physical, emotional, psychological damage, loss, and malfunction. Therefore, security can be described to include countless activities and measures to protect people and assets from harm and loss. Alongside this paper's theme, this all-encompassing term, security can be divided into *physical security* and *cybersecurity*.

1.a. **Physical security**: Physical security is concerned with those means by which and individuals or organizations protect their life and their facilities against natural and man-made disasters. Such facilities that require security may include a plant, building, office, or any governmental, industrial, or commercial structure or complex with all the attendant structures and functions that comprise an integrated operation (Fischer et al., 2013; Johnson & Ortmeier, 2018; McCrie, 2016; Smith et al., 2017).

1.b. **Cybersecurity:** The term *security* can also embrace the construct of cyberspace, where a holistic and comprehensive approach to protection and methods is imperative. The origin of cybersecurity dated back to the 1970s in the U.S. when the federal government recognized that open access to computer systems could create security breaches (Johnson & Ortmeier, 2018; Kremling & Parker, 2018; McCrie, 2016; Smith et al., 2017). Ever since that time, the federal government has developed numerous policies and laws to deal with ever-increasing real threats targeting computer systems and network communications systems to protect people and information.

The definition of cybersecurity often depends on the individuals or entity doing the defining. Nevertheless, cybersecurity is concerned with numerous measures, just like physical security, to protect and secure the cyberspace which is created by technology-based computer and network systems, storing the immeasurable amount of information and data, and which communicates among innumerable users connected by the Internet from intended malicious attacks, with countless security policies and protective activities. With the rapidly growing integration of technology and security operations, cybersecurity, rather than being used for an exclusive term to indicate only a certain field, should be used broadly and encompasses a wide scope of information and Internet security-related issues (Johnson & Ortmeier, 2018; Kremling & Parker, 2018; Smith et al., 2017). Therefore, the

term "cybersecurity" in this article is contextually used interchangeably with such other terms as "information security," "computer security," "Internet security," "communications security," and "network security."

2. A Basic Principle of Physical Security

2.1. Mycenaean fortresses of layered physical security

The need and practice for security can be traced back to the ancient civilizations and predate the establishment of state-sponsored policing agencies by many centuries (Smith et al., 2017). Historically, security heavily relied on physical aspects for survival and safety. The earliest known forms of civilizations used both security technology and techniques to provide greater protection for their dwellings and possessions. Some ancient cities and palaces were often surrounded by walls of great thickness and height. For example, the Mycenaean fortresses normally consisted of a mud-brick rampart, 26 feet high, surrounded by a wall, built of burnt brick and bitumen, and enclosed by a moat, canal, or river. One of the most prominent principles of the ancient physical security practice was developed by the Mycenaeans (12000-1500 B.C.) with four zones of physical protection layers: (1) *the first line of defense*: using water either as a moat, canal, or river; (2) *the second line of defense*: constructing the outermost wall against intruders which functioned as a perimeter wall; (3) *the third line of defense*: erecting the wall surrounding the sacred precincts and palace; and (4) *the final line of defense*: constructing the wall of the building used as quarters for the royalty and their valuable possessions (Collins et al., 2015).

Though actual applications of this four-zone physical security principle have varied across civilizations and cultures, the basic idea of different layers of protection can be found in a similar fashion. The number of protection layers depended on the location, size, content, and material resources. For example, during the same period of time with the Mycenaean, the Egyptians constructed not only the great temples and pyramids but also tombs which could represent some of the most noteworthy examples of ancient physical security and crime prevention techniques (Collings et al., 2015; Johnson & Ortmeier, 2018; McCrie, 2016; Smith et al., 2017). What the ancient civilizations leave to the modern era is the basic principle of security design and its application. It was designed based on physical layout and security protection but had been applied to various security environments where protection and safety were required. What hat has been changed over the last several millenniums is, first, technology to be developed and added for better and effective security operations and, second, contents to be protected and secured.

2.1.a. Technology: Ancient physical security designs and measures include innovative and creative technology to provide protection and safety measures. For example, the tombs of the kings of ancient Egypt were designed to discourage would-be looters over the centuries by building a maze-like connection between the separate chambers inside the tombs with a well-perceived design and the latest technology. The Egyptians are also credited with developing some of the first advanced security devices, such as the lock. Egyptian locks dated back to about 2000 B.C., which are considered forerunners to the modern pin tumbler lock. The Greeks refined bar and bolt locks that permitted a door to be unbarred from the outside as well as from the inside. They are also credited to be the first to use keyholes. Roman advanced technology included the first metal locks, the

earliest padlocks, the introduction of small keys, and the development of warded locks (Collins et al., 2015; Johnson & Ortmeier, 2018; McCrie, 2016).

The entire area of physical security thinking in history has been changing as technology continues to advance. Not only are the devices used in physical security more sophisticated, but also the ability to integrate various physical security operations is possible and becomes the standard. That is not to say that numerous traditional security and protection measures and devices are no longer in use, but in many modern-day operations, the old technology and resources have been gradually replaced by, in particular, modern computer-based operations (Fischer et al. 2013; McCrie, 2016).

2.1.b. Contents: Ancient civilizations had built defensive fortresses to provide physical protection for contents within them. Obviously, people who dwelled beyond the second line of defense were the most critical object to be protected. Besides humans, various items and building structures needed to be secured and protected, such as houses to live in, warehouses to keep equipment and animals, and barns to store grains. Most building structures to keep the items scattered around within the perimeter of the second zone of defense. In the third line of protection which was typically the wall surrounding the sacred precincts and palaces, items required to be protected include documents, important articles, and military equipment, and so forth. The innermost final line of protection was designed to protect the royalty and their valuable possessions (Collins et al., 2015).

In the modern era in the U.S., one of the most significant developments in the security field is electronic systems (McCrie, 2014). For example, by during the 1960s-70s, the private sector entered security in another form from heavily physical and manned security to information security where common businesses and industries created central repositories of information and data which were deemed important to all of their common interests nationwide and made it available in various ways to their separate groups. The primary purpose was to decrease possible loss by networking information (Fischer et al., 2013; Grabosky, 2016; Johnson & Ortmeier, 2018; Kremling & Parker, 2018; Smith et al., 2017).

2.2. The first line of defense: Outer and perimeter security

Physical security approach should start outside the grounds around the protected facility as the first line of defense with two major tenets of reliable and durable security system design – delay and deny (Carroll, 1996; Johnson & Ortmeier, 2018; McCrie, 2016; Smith et al., 2017). With well-prepared security planning in place, the premises should be protected from criminal attacks by denying ready access toward interior spaces or areas in the event that a motivated intruder surmounts exterior controls by means of barriers, fences, walls, gates, and lighting (Fischer et al., 2013; Johnson & Ortmeier, 2018; Smith et al., 2017).

2.2.a. Barriers, fences, and walls: Defense begins at the perimeter—the first protection line that can be crossed by a motivated intruder. A facility's perimeter is usually determined by the function and location of the facility itself, and the perimeter is the boundary of the property owned and managed by the organization. Often, natural and structural barriers can be the components by which boundaries are defined, wherein penetration against the facility is delayed, deterred, or detected. Natural barriers can consist of any terrain or feature that is difficult to traverse, while structural barriers can be

permanent or temporary measures, including fences, walls, doors, or any other construction that can serve as a deterrent to unauthorized entry (Carroll, 1996; Fischer et al., 2013; Johnson & Ortmeier, 2018; McCrie, 2016; Smith et al., 2017). Since both structural and natural barriers are less effective in preventing penetration from a motivated, determined, and resourceful criminal (i.e., easily climbed, scaled, bypassed, etc.), all such barriers must be supposed by additional security layers.

2.2.b. Gates: Every opening in the perimeter line can be a potential security breach. For the purpose of the first line of protection, these openings typically attached to barriers, fences, or walls should be kept to the minimum number necessary to support the workflow of the organization, balancing safety concerns with smooth business operations (Fischer et al., 2013; Smith et al., 2017).

2.2.c. Lighting: Another critical consideration for perimeter protection is the lighting. Protective security lighting should produce sufficient light to create a psychological deterrent to any attempt of intrusion as well as to provide detection virtually certain in the event an entry is successfully made. Since no one type of lighting is applicable to all protective lighting situations, additional considerations, besides the perimeter security planning, should be paid to select a particular type of perimeter lighting amid the great profusion of lighting and equipment in the market (Carroll, 1996; Fischer et al., 2013; Johnson & Ortmeier, 2018; McCrie, 2016; Smith et al., 2017).

2.3. The second line of defense: Exterior and interior security

This level of defense concerns the physical building itself which forms part of the perimeter barrier as in many urban settings or part of the interior, or both. The primary security vulnerability can be unauthorized attempts to gain access toward the facility to disturb the normal business operations and legitimate activities (Carroll, 1996; Fischer et al., 2013; Johnson & Ortmeier, 2018). The durable security measures should focus on windows, doors, locks and keys, roofs, common walls, and new technological additions to them.

2.3.a. Windows: In most circumstances, windows are viewed as potential weak entry spots in any building's defenses. Most forced break-ins are through window glass. For most security situations, windows and other openings should be protected with grillwork, metal bars, heavy screening, or chain-link fencing when they are constructed close enough from the ground or away from the perimeter barrier. Windows for security concern can be strengthened by the use of either burglary-resistant glass or polycarbonate glazing material (Fischer et al., 2013; Johnson & Ortmeier, 2018; McCrie, 2016; Smith et al., 2017). In many settings, it is critical to screen windows to protect their use.

2.3.b. Doors: Doors are frequently much weaker than the surface into which they are positioned. Therefore, every door, whether exterior or interior, should be carefully evaluated to decide the degree of demanded security, such as the type of construction where doors are attached and the locking system which is used on each door. Doors that penetrate the perimeter walls should be of heavy construction and fitted with strong locks. Heavy wood or metal doors with reinforced jambs should be constructed, and hinges should be installed with the screws concealed and with the hinge pins either welded or

flanged to prevent removal (Carroll, 1996; Fischer et al., 2013; Johnson & Ortmeier, 2018; Smith et al., 2017).

2.3.c. Locks and keys: Attacks against locks can be the most practical means of ingress to gain forcible or unauthorized entry even if the door and the jamb are well designed and installed impervious to forcible attack. Picking the lock, or duplicating a key by impression, are the commonly used methods against traditional locking systems. Two effective and durable defenses against these attacks can be, first, the installation of special pick-resistant, impression-resistant lock cylinders, and, second, the use of magnetic cards in place of traditional keying systems. Equally critical security aspect for keys is to establish key management systems. Whether traditional keying systems or state-of-the-art digital operations, every effort should be exerted to develop managerial ways whereby keys and access to keying information must be restricted to the hands of security or management personnel. As the technology advances fast, old lock and key systems are being supplanted by the latest technological developments. A careful evaluation of the current applications and conscientious selection of technology-oriented lock and key systems are an essential part of robust security practices for the second line of physical defense (Carroll, 1996; Fischer et a., 2013; Johnson & Ortmeier, 2018; McCrie, 2016; Smith et al., 2017).

2.3.d. Roofs and common walls: An important, though often overlooked part of the second line of defense, is the roof of the building. In many circumstances, entry through the roof can be workable and successful. Such access to inside can be made through skylights or by chopping through the roof whose illegal activity is rarely detected by a passerby or even by patrols, especially during nighttime. In addition, buildings sharing a common wall with adjacent buildings can be entered frequently by simply breaking through the wall from a poorly secured neighboring occupancy (Carroll, 1996; Fischer et al., 2013; Johnson & Ortmeier, 2018). A thorough inspection and well-devised security program with technological support should be in place to protect roofs and common walls.

2.4. The third line of defense: Inner security

Once the facility's perimeter and building are secured, the next step in physical security layer moves toward the inside of the building with the primary objective of minimizing or controlling access to the interior. The most common security challenges are against the doors and windows of the building within the perimeter. Thus, the primary security consideration should direct toward protection against the free movement of employees and others inside the facility (Fischer et al., 2013). The scope and type of security measures can depend on the nature and function of the facility. One key security aspect is that security operations must not interfere with the facility's normal business while controlling traffic in and out of the protected building. The broadly used security measure for doors and windows tends to focus on intrusion and access control by means of traffic control and identification systems.

2.4.a. Doors and windows: For an effective intrusion and access control, doors leading to equipment rooms, computer installations, research and development (R&D), and other sensitive areas of the facility should be equipped with automatic door-closing devices as well as fitted with strong deadbolts and heavy latches. An electronic strike can strongly be

considered in cases where an area is under heavy security but has any degree of traffic in order to secure the operation and control the traffic. The actual installation of the doors and windows and locking systems on them should be determined by a thorough and comprehensive security survey. Employee entrances, as the authorized points of passage for all employees, should be staffed by security professionals so that these doors can be secured and monitored, denying entrance to unauthorized visitors and attempted entry (Carroll, 1996; Fischer et al., 2013; McCrie, 2016; Smith et al., 2017).

2.4.b. Traffic control: Controlling and monitoring traffic in and out and within a facility is indispensable to the facility's third line of the security program. Perimeter barriers, locked doors, and screened windows can prevent or deter the entry of unauthorized visitors, but since most ongoing traffic in and out of the facility is vital to every business operation, security provision should be established for the control of this movement. The most common practice is to use the identification of employees and visitors, including vehicular traffic, in order to direct or limit their movements, to control all incoming and outgoing packages, and to check trucks and private cars (Carroll, 1996; Fischer et al., 2013; McCrie, 2016).

2.4.c. Identification card (ID) and package control: The most practical and commonly accepted security system for access and instruction control is the use of badges or IDs. Generally speaking, this card system should designate when, where, how, and to whom passes should be displayed. For security purposes, cards must be tamper-resistant, designed to be difficult to reproduce. Recent smart card IDs with the introduction of holography into badge control systems can reduce the chance of counterfeiting cards. All visitors to any facility should be required to identify themselves by carrying visitor/contractor IDs all the time, which limit their movements and control unauthorized access to certain areas. Package control procedures should be in place to control items entering or leaving the premises. Packages brought in should be checked for content as well. They should be dealt with in order to prevent internal/external theft, misappropriation of organization property, and concealment of dangerous materials (e.g., biological or chemical agents or materials) (Fischer et al., 2013; Smith et al., 2017).

2.5. The fourth line of defense: Content security

The final line of defense at any facility is associated with content security, that is, the high-security storage areas where paper, records, data, information, plans, or other especially valuable assets are placed and protected. The primary risky factors include internal theft and fire. Generally, three assorted types of security containers for content protection are utilized: files, safes, and vaults (Fischer et al., 2013; McCrie, 2016).

2.5.a. Files and safes: Burglary-resistant filing cabinets with a combination lock are secure against most surreptitious attacks. Safes are designed to perform a particular mission to provide a certain level of protection with two broadly used types: the record safe (fire-resistant) and the money safe (burglary-resistant). The level of protection and selection of files and safes should be guided with several critical concerns, such as the level of threat of fire or burglary, the value of the safe's contents, and the length of protection time required in the event of a fire or of a burglary attempt (Fischer et al., 2013; McCrie, 2016; Smith et al., 2017).

In particular, with the increase of use of electronic media instead of paper records, most safe manufacturers provide various types of media safes, which are designed with the customized purpose of securing electronic data and information, such as USB drives that are fire- and water-resistant. These drives come with many different choices, depending on the amount of storage, temperature rating, and length of time.

2.5.b. Vaults: Vaults are essentially enlarged safes, typically of high-quality, reinforced concrete, situated at or below ground level, and strong enough to withstand the weight imposed on it in case of building collapse due to fire or explosion. They should be surrounded by narrow corridors, and there should be no power outlets anywhere in the vicinity of the vault (Fischer et al., 2013; McCrie, 2016; Smith et al., 2017).

In short, because no security container can resist attack indefinitely, it must be supported by alarm systems and both frequent inspections with the security officer's patrol and constant inspection with closed-circuit television (CCTV) surveillance (Johnson & Ortmeier, 2018; Smith et al., 2017).

3. Link of the Layered Physical Security to Cybersecurity

As discussed, physical security designs and applications have been evolved based on the four zones of protection, and its basic principle has not changed for the last several millenniums. What has changed and advanced is technology and protected contents. The primary applications of layered physical security systems are flexible and can be adapted to the field of computer systems and cybersecurity.

3.1. Physical security, computer technology, and cybersecurity

What has significantly developed over the last centuries is that the role technology plays has been widened. Security has evolved progressively to protect two types of assets: physical assets and information assets. The former is the primary target for protection in ancient times (e.g., houses and palaces). Of course, information assets were also critical to be preserved among old civilizations, but as technology evolves, the format for storage and safekeeping has changed from physical devices to electronic ones. The types and content of information in the modern day have adopted new technological advances.

In particular, ever since the first viable full-scale computer, ENIAC (Electronic Numerical Integrator and Calculator), was developed by the U.S. Army in 1946, three dramatic trends have been observed for the last several decades: first, government and corporate business sectors have used computers to process, store, and transmit a vast amount of information; second, technology and security operations are integrated at a rapid speed; and third, information systems are becoming primary methods of communications (e.g., email, instant messaging, voice-over-Internet protocol, and social network systems (SNS)) (Carroll, 1996; Fischer et al., 2013; Graboskey, 2016; Johnson & Ortmeier, 2018; Smith et al., 2017). Such changes in government and private corporate sectors result in profuse potentials to effectively and efficiently operate the institutions and formidable challenges to reliably and securely protect assets and information.

Information systems have become increasingly essential to the efficient operations of private businesses and government organizations. Both sectors have responded by creating and placing senior executives to direct strategic and tactical operations associated with the creation, processing, transmission, storage, and protection of information. Virtually all major corporations and government organizations have chief information officers (CIO)

or chief information security officers (CISO) in place (Fischer et al., 2013; McCrie, 2016). These C-suite executive positions have various functions and responsibilities, but one of the most critical and collective efforts is for security and protection of the confidentiality, integrity, and availability of information in boundless cyberspace, where fundamental principles of cybersecurity are applied.

There might be assorted perspectives to approach and describe the basics of cybersecurity (Fischer et al., 2003; Grabosky, 2016; Kremling & Parker, 2018; McCrie, 2016; Smith et al., 2017; Kremling & Parker, 2018). As discussed earlier, however, the time-honored principle of physical security can be applied to cybersecurity, which maintains multiple layers of protection methods. For adequate security protection for broad cybersecurity idiom, it is essential to identify major subset areas in cybersecurity. Such a task is not easy at all, partly because of how cybersecurity is defined which largely depends on the individual or entity doing the defining (Kremling & Parker, 2018).

However, it can cautiously have at least the following subset areas as an object of cybersecurity discourse and policy applications: computer systems, networks/communications systems, and database/information systems. As discussed earlier in this paper, principles and applications of physical security recognized several idiosyncratic "zones of protection" lines, depending on location, size, content, and surrounding environment of the protected asset. The protective security lines typically start from the outside perimeter to the inside space. The objectives of physical security can be achieved by placing barriers in the path of attackers in order to deter them from infiltrating, to delay them if they decide to penetrate, and to deny them access to high-value targets or assets if they succeed in breaching the security system (also known as security 3-D tactics) (Carroll, 1996; Fischer et al., 2013; Grabosky, 2016; Johnson & Ortmeier, 2018; McCrie, 2016; Smith et al., 2017).

Likewise, cybersecurity protection lines can also start from outer assets to inner content. Just as controlling access control is one of the most significant aspects of physical security, protecting access to computer systems, networking systems, and information systems only by authorized users are also one of the most critical cybersecurity measures. While sustainable and reliable barriers of physical security against multifarious natural and man-made disasters are imperative, cybersecurity measures must also deal with harms and losses from possible fire, flood, earthquake, theft, embezzlement, arson, accident, unknown flaws in policy and implementation, and so forth with physically durable protection measures.

3.2. The first line of protection for cybersecurity: Networks/Communications systems

Protection for the outer asset as the first line of defense in cybersecurity may include communications systems or networks, which physically connect independent and separate computer systems to link among them via either wired or wireless, enabling to create spider-webs like networks and inviable cyberspace for communications and information storage. As technology advanced, computers were gradually wired in the 1970s, expanded to other locations during 1980s, and eventually built a cobweb like wired/wireless networking systems (Bosworth & Jacobson, 2014; Carroll, 1996; Grabosky, 2016; Johnson & Ortmeier, 2018; Kremling & Parker, 2018; McCrie, 2016; Smith et al., 2017).

3.2.a. LANs, WLANs, and WANs: A simple understanding of a network is that just two or more computers are connected to communicate with each other and to share computer resources with several types: local area networks (LANs), wireless LANs (WLANs), wide

area networks (WANs), and Internet (Carroll, 1996; Fischer et al., 2013; Grabosky, 2016; McCrie, 2016).

Local area networks (LANs) consist of two or more computers physically connected with normally coaxial or fiber optic wire or cable which forms a data path over which information is transferred. Communications to a computer on the LAN are instantly broadcasted to all the computers connected to the LAN, which is wired in a short distance within a limited geographic area, such as the same department, office, building, or group of buildings (Kessler, 2014; Pritsky et al., 2014). On the other hand, wide area networks (WANs) are more powerful networks that can function across wide geographic areas at greater speeds than LANs. Most WANs used to be connected via telephone lines in the 1970s and 1980s with limited accessibility and communication lines (Fischer et al., 2013; McCrie, 2016).

The advent of new technology has led many organizations to adopt wireless LANs (WLANs), operating on the open air and eliminating hardwire applications and their limitations with great flexibility in connectivity (Fischer et al., 2013; Tagg et al., 2014). However, WLANs face real problems for those assigned to the protection of assets. The federal government would not allow any government-funded agency to introduce wireless technology until security is improved (Carroll, 1996; Fischer et al., 2013; Grabosky, 2016; Kremling & Parker, 2018). With LAN and WLAN systems, security procedures should begin by locking up everything that can be physically secured. With the strong trend toward concentrating control at hubs, the LAN and WLAN systems become increasingly vulnerable and an easy target for security breaches and attacks (McCrie, 2016; NCPI, 2001).

3.2.b. WWW: New technological advances of the Internet Protocol (IP) packet and transmission control protocol (TCP) in the 1970s enabled to have better, speedy, and reliable communications beyond limited geographical areas. Since then, WAN Internet has evolved to provide many services, such as electronic mail (email), finger services, Usenet, file transfer protocol (FTP), and gophers. The prime advance of the Internet system is the development of the World Wide Web (the Web or WWW), which is a hypertext-based tool that allows users to retrieve and display data. It quickly became the most popular tool on the Internet due to both graphics and hypertext which enables data to be linked to other data (Fischer et al. 2013; Grabosky, 2016). However, the Web/WWW is attached to many new problems, including spam problems, cookies, viruses, and data breaches.

Today, most of both stand-alone personal computers (PCs) and additional computer systems (see the below section regarding "Computer Systems") are connected to either LANs, WLANs, or WANs. Furthermore, more and more people are being mobile and need access to ever-increasing online resources. A decade ago, public and private organizations paid little attention to monitoring network use, whether it was LAN, WLAN, WAN, or the Internet, but today with the ubiquitous use of the Internet, organizations cannot ignore looking at who is accessing the network systems, using the service, and what they are doing while on the network and communications line. In particular, the wireless connection makes cybersecurity more vulnerable and challenging. Vulnerabilities due to remote access through the network systems can fall into several categories: hacking, voice systems, remote and traveling employees, and disgruntled

employees (Fischer et al., 2013; Grabosky, 2016; Johnson & Ortmeier, 2018; Levine, 2003; McCrie, 2016).

In recent years, monitoring of information has been added to the tools available. For example, software packages allow organizations to block out non-work-related entertainment, gaming, pornography, and other websites, while still permitting Internet access for organization-related work. Furthermore, many organizations have developed policies explicitly addressing access to social network service (SNS) sites (e.g., Facebook, Twitter, and so forth). Generally, access for personal (or non-organization business) use is prohibited, but many organizations are using SNS sites for their legitimate business purposes by allowing access within that context (Fischer et al., 2013; Smith et al., 2017).

For basic and practical approaches for networking/communications security, the following aspects can be applied. For LANs, the wiring closets should be secured with an appropriate lock system, and another entry point for obtaining data from a LAN system should be through the wiring itself. In most settings of government and corporate companies, the wiring is concealed in the ceiling, walls, or under the carpet, which can easily give a wiretapper a choice of points of entry. One approach against possible wiretapping is that all original and necessary wiring needs to be documented and diagrammed. With the routine checking of the diagrams against existing wiring, new or suspicious additions should alert security to a potential problem (Fischer et al., 2013; Grabosky, 2016; NCPI, 2001).

3.2.c. Network security policy: In addition, it is vital that organizations have a clear policy statement of network use. A setup of a network security policy (NSP) is imperative in developing other cybersecurity solutions. For example, most NSPs define the problems, list the requirements, discuss solutions, and set out sanction for infractions. Employees should know their rights and the expectations of the organization (Carroll, 1996; Fischer et al., 2013; Grabosky, 2016; Smith et al., 2017).

3.3. The second line of protection for cybersecurity: Computer systems

The object for the second line of defense is computer systems, which may include various types of computer machines and essential functions. When the first computer was developed, it was a single, bulky machine to execute just a few calculating tasks. With the fast advent of remarkable technology, it becomes interlinked computer systems which are used to produce information, to share information, and to communicate. Generally, computers available today can be categorized with five systems: microcontrollers, microcomputers, minicomputers, mainframe computers, and supercomputers. What categorizes them is how much information the computer can store, the processing speed of the system, and the size of the computer system (Fischer et al., 2013; Williams & Sawyer, 2015).

3.3.a. Computer systems: *Microcontrollers*, also called embedded computers, are the tiny, specialized microprocessors installed in "smart" appliances and automobiles. For example, these microcontrollers enable microwave ovens to store data about how long to cook potatoes and at what power setting. They have been used to develop a new universe of experimental electronic appliances—e-pliances and other devices, including single-function products, digital cameras, digital music players, and refrigerators, blood-pressure monitors, airbag sensors, gas and chemical sensors for water and air, and vibration sensors.

Microcomputers, also called personal computers (PCs), are quite small in size and are designed primarily for individuals and small businesses and can be connected to networks of larger computers via a special cable or wirelessly. Several types of them are available: (1) non-portable PCs (e.g., desktop PCs or tower PCs), (2) portable PCs (e.g., laptop computer, notebooks, netbooks, tablets, mobile devices, and personal digital assistant—handheld computers or palmtops), and (3) workstations (Fischer et al., 2013; Williams & Sawyer, 2015).

Minicomputers make up the middle class of computer size and power, typically being used as servers or network servers. They are central computers that can hold collections of data (databases) and programs for connecting or supplying services to many PCs or terminals, called clients, which are linked by a computer network wired or wirelessly. *Mainframe computers* are capable of great processing speed and data storage and enable multiple users to utilize the system simultaneously. They are used in many large businesses and occupy specially wired, air-conditioned rooms. *Supercomputers* are the largest, most powerful, expensive computers and high-capacity machines that require special air-conditioned rooms and specially trained staff. Due to the cost, these computers are used primarily by the government, large companies, and universities (Fischer et al., 2013; Grabosky, 2016; Williams & Sawyer, 2015).

Regardless of the type of computer system used by any government and corporate business sectors, there are four common elements: input, processing, storage, and output. Input refers to entering data and programs into the computers by using a keyboard, mouse, scanner, voice recognition software, or telecommunications methods (e.g., traditional phone lines or wireless transmissions). Processing transforms the input into machine instructions which exist in the executable form within computer systems through a central processing unit (CPU), memory, and basic input/output system (BIOS). Storage is a generic term that refers to the areas of a computer and associated media that store such information as data and programs (e.g., internal or main memory, tapes, zip drives, hard disks, CD-ROMs, and memory sticks). The output is any on-screen result or printed report generated by the computer through printers, monitors, and communication data (Carroll, 1996; Fischer et al., 2013).

As the second line of cybersecurity protection, any PCs placed on a person's desk should have a lock-down system installed, attaching the equipment to the desk. Four types of lock-down systems can be utilized: cages, plates, cables, and alarms. The primary objective of them is to discourage theft of the equipment. Equipment covers should be tamper-resistant. Portable computers, such as laptop computers, tablets, and notebook computers, should be kept in one's constant physical possession (Carroll, 1996; NCPI, 2001).

3.3.b. Virus scanning: Now it is a common practice for organizations to scan their computer systems to scan for viruses manually or automatically. Some form of antivirus software should protect every computer system or stand-alone computer. While several well-known virus-scanning software is generally effective, no developer can claim to be 100 percent effective in blocking, detecting, and treating suspicious and malicious tries because new viruses appear regularly. It is almost impossible for the end-user to keep up with what is current (Fischer et al., 2013; Kremling & Parker, 2018).

3.3.c. Email filtering and web monitoring: Due to countless spam and phishing attacks, email filtering software, including spam filtering function, has become common in most organizational cybersecurity programs. Most of the commercial software enables the end-user to set rules or protocols that incoming and outbound emails must meet. When the email fails to meet the criteria, it is blocked. Just as the email filtering software controls for monitoring and blocking of email, the Web monitoring software also allows the end-user to filter or restrict access to certain sites, as well as monitor what Websites employees are using and for how long (Carroll, 1996; Fischer et al., 2013; Grabosky, 2016).

3.3.d. Physical security: The basic principle of physical security can also be adapted to protect computer systems. For example, electronic data processing (EDP) centers have the same physical security needs as any other government or industrial establishments. Most EDP centers use the traditional security approach, beginning with the protection of the exterior area around the building, then moving toward the building's very perimeter, the building's interior, and the contents of the building (Carroll, 1996; Fischer et al., 2013; McCrie, 2016; NCPI, 2001). The outer wall of an EDP center should provide perimeter protection by means of walls, fences, or partitions. Entrance security (e.g., the main entrance gate, other openings, and emergency exit doors attached to the building) should be in place with tightly controlled access control. Electronic access control mechanisms (e.g., badge-reading locks) should be installed, and badges must only be issued to authorized personnel and also be time-stamped to restrict access to authorized times. In all circumstances, the computer rooms should be restricted to operations personnel, where computer programs, data/information, and computer equipment are all brought together. A uniformed security officer or a receptionist should be stationed at each important entry point during all business hours (Fischer et al., 2013; Johnson & Ortmeier, 2018; McCrie, 2016).

In addition, computer centers should not be in a basement, below grade level, or on first-floor sites due to the possible entry of surface water from flooding or hurricane and possible forcible attack, surreptitious intrusion, civil commotion, or terrorist activities. The top floor also presents ample opportunities for illegal entry through skylights or by cutting through the roof (Fischer et al., 2013; Miroa, 2014a).

3.3.e. Fire protection: Constructed buildings housing computer systems or centers should be of a noncombustible structure to reduce the chance of catching fire through constant monitoring for temperature, humidity, smoke, fire, and water leakage. Dry pipe sprinkler systems, rather than a wet pipe system, should be installed since water and electrical equipment does not mix. A fire extinguisher within 50 feet of every equipment cabinet should be available for use (Fischer et al., 2013; Miroa, 2014a).

3.3.f. Hardware backup: Hardware backup is also a critical part of protection for computer systems. Disruptions against computer hardware can come from non-disasters (e.g., system malfunctions or equipment failures), disasters, and catastrophes. In case of disasters, the entire facility may be inaccessible for several days, while catastrophes may entail the destruction of the facility where critical businesses involved computer systems are afoot, including data processing, data storage, and data sharing. Depending on the extent of the disruption against the computer systems and organizations, alternative locations as a hardware backup method can be hot, warm, or cold sites (Fischer et al.,

2013). Hot sites are fully configured and ready to operate within several hours. Warm sites are partially configured but are missing the central computer. In such a case, it may take several days or weeks to locate and install the main computer and full operation. Cold sites are ready to receive equipment but do not have any components installed in advance; thus, it may take at least several weeks to become operational. In addition, these various computer systems are typically linked wired or wirelessly via the Internet. They are "always on" the Internet for better communications and information storing and sharing (Fischer et al., 2013; Grabosky, 2016).

3.4. The third line of protection for cybersecurity: Database/Information systems

Integrity and confidentiality of inner content as the third line of cybersecurity defense is database/information, the very asset created by the organized, constant workflow of government and private business sectors via networks and communication lines which can be perceivable of a vein for the vital lifeline of cyberspace. As discussed earlier, two major common elements of the computer systems are processing and storage. Computer systems not only produce a vast amount of information by executing programs but also store such information and programs in the database. The data collected for business in both government and private corporate sectors have become the backbone of most organizations (Fischer et al., 2013; Johnson & Ortmeier, 2018). However, since data are stored in computer systems and shared via networking systems, data management, security of networking, and data management systems have become a critical part of cybersecurity policies and programs. Safeguarding the inner content of data and information is a daunting task.

Generally, protection of data and information systems includes the three major aspects: (1) integrity, which makes sure that data are changed only in intended ways; (2) confidentiality, which makes sure that only authorized individuals view the information; and (3) availability, which makes sure that the data are available when needed to authorized persons. However, with even proper measures for inner content, data and information are challenged by at least two problems: first, authorized users sometimes use data improperly, and second, unknown flaws in policy and its implementation can allow for unintended data access and data changes (Fischer et al., 2013; Johnson & Ortmeier, 2018).

3.4.a. Encryption: In general, one of the best ways to protect any type of inner content of data and information is to encrypt it. It also applies as one of the best ways to protect data on portable computers (e.g., laptop computers, tablets, smartphones, etc.). Encryption scrambles the information and data so that it is not usable unless the changes are reversed. Today there are at least five different approaches for encrypting data and information: Data Encryption Standard (DES) algorithm, Rivest, Shamir, and Adleman (RSA) algorithm, Pretty Good Privacy (PGP) algorithm, Skipjack algorithm, and Privacy Enhanced Mail (PEM) (Fischer et al., 2003; Grabosky, 2016; Kremling & Parker, 2018; McCrie, 2016).

3.4.b. Data/Information storage media: One aspect to protect database and information systems, besides protecting the computer itself, is to be concerned with storage media, in particular, removable media (e.g., CDs, memory sticks, flash drives, etc.). The work environment in which those portable and easy-to-conceal storage media are used can be secure enough, but the home environment where employees carry the removable media

and transport them between work and home is not. Media can also be lost between work and home, altering the information or data inside. One method to defend against unauthorized downloads of data and information is to disable USB ports and disc drives on computer systems which contain organizations' most sensitive data (Fischer et al., 2013; Grabosky, 2016; Kremling & Parker, 2018; McCrie, 2016; NCPI, 2001).

3.4.c. Software and information backup: Software includes assorted computer programs, such as operating systems, programming languages, utilities, and application programs. To protect these items from loss, it is required to prepare both the physical storage environment and the frequency of change in data. Information and software backup should be done at on- and off-site locations. On-site files should be housed in a fire-resistant safe designed for computer media. The off-site local backup location should typically be near the computer site (Fischer et al., 2013; Grabosky, 2016; Kremling & Parker, 2018; Miora, 2014b).

Conclusion

The concept and practice of security have been widened its applicability to physical security and cybersecurity. Fundamental security concepts and their practical measures are as old as human beings' nature for survival and protection, as well as new technologies that are improving these basic concepts and applications. While the basics of perimeter, interior and exterior, and inner security theory and principle remain constant, the tools and technology used to establish security systems have improved. Contemporary systems that integrate all aspects of security are becoming commonplace.

The world of computers and the information that is stored, processed, analyzed, and disseminated by them are constantly changing. With change comes vulnerability, while the progress and advent achieved in this dynamic field have remarkably improved the general state of the world, there are always those who use the technology for personal gain or criminal activity. Security and IT professionals are facing challenges and problems targeting cyberspace and organizations' information by gaining unauthorized access to breach security lines. Both traditional security professionals and technology-oriented IT and cybersecurity professionals must work together to protect the organizations and the individuals that they serve by utilizing and applying the same principles of layered security protection lines in both physical and cyber worlds.

Acknowledgment

The author thanks Dr. Robert D. McCrie, Professor, at John Jay College of Criminal Justice in New York City for valuable comments and support in completing this article.

References

Bosworth, S., & Jacobson, R. V. (2014). Brief history and mission of information system security. In: S. Bosworth, M. Kabay, & E. Whyne (Eds.), *Computer Security Handbook* (6th ed.) (pp. 1-1 - 1-21). Hoboken, NJ: John Wiley & Sons, Inc.

Carroll, J. M. (1996). *Computer security* (3rd ed.). Burlington, MA: Butterworth Heinemann.

Collins, P. A., Ricks, T. A., & Van Meter, C. W. (2015). *Principles of security and crime prevention* (4th ed.). New York, NY: Routledge.

Fischer, R. J., Halibozek, E. P., & Walters, D. C. (2013). *Introduction to security* (9th ed.). Waltham, MA: Butterworth-Heinemann.

Grabosky, P. (2016). *Cybercrime*. New York, NY: Oxford University Press.

Johnson, B. R., & Ortmeier, P. J. (2018). Introduction to security: Operations and management (5th ed.). New York, NY: Pearson.

Kessler, G. C. (2014). Local area network topologies, protocols, and design. In: S. Bosworth, M. Kabay, & E. Whyne (Eds.), *Computer Security Handbook* (6th ed.) (pp. 6-1 - 6-31). Hoboken, NJ: John Wiley & Sons, Inc.

Kremling, J., & Parker, A. M. S. (2018). *Cyberspace, cybersecurity, and cybercrime*. Los Angeles, CA: Sage.

Levine, D. E. (2003, March). Content monitoring and filtering. *Security Technology & Design*, 70-74.

McCrie, R. D. (2004). The history of expertise in security management practice and litigation. *Security Journal*, 17(3), 11-19.

McCrie, R. D. (2014). A history of security. In: M. Gill (Ed.), *The Handbook of Security* (2nd ed.) (pp. 21-43). London, UK: Palgrave Macmillan.

McCrie, R. D. (2016). *Security operations management* (3ed ed.). Waltham, MA: Butterworth-Hernemann.

Miora, M. (2014a). Business continuity planning. In: S. Bosworth, M. Kabay, & E. Whyne (Eds.), *Computer Security Handbook* (6th ed.) (pp. 58-1 – 58-36). Hoboken, NJ: John Wiley & Sons, Inc.

Miora, M. (2014b). *Disaster recovery*. In: S. Bosworth, M. Kabay, & E. Whyne (Eds.), Computer Security Handbook (6th ed.) (pp. 59-1 - 59-22). Hoboken, NJ: John Wiley & Sons, Inc.

National Crime Prevention Institute (NCPI). (2001). *Understanding crime prevention* (2nd ed.). Woburn, MA: Butterworth-Hernemann.

Pritsky, N. T., Bumblis, J. R., & Kessler, G. C. (2014). Local area networks. In: S. Bosworth, M. Kabay, & E. Whyne (Eds.), *Computer Security Handbook* (6th ed.) (pp. 25-1 - 25-17). Hoboken, NJ: John Wiley & Sons, Inc.

Smith, C. F., Schmalleger, F., & Siegel, L. J. (2017). *Private security today*. Boston, MA: Pearson.

Tagg, G. L., & Sinchak, J. (2014). 802.11 wireless LAN security. In: S. Bosworth, M. Kabay, & E. Whyne (Eds.), *Computer Security Handbook* (6th ed.) (pp. 33-1 – 33-53). Hoboken, NJ: John Wiley & Sons, Inc.

Williams, B. K., & Sawyer, S. C. (1995). *Using information technology: A practical introduction to computers & communications* (11th ed.). New York, NY: McGraw-Hill Education.