ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 9, Issue 3, March 2020

Security in the Migration to a Multi-Modal Environment

Salami Afolabi Kehinde[1], Margaret Kareyo, PhD[2]

PhD Candidate, Department of Information Technology, School of Computing and Information Technology Kampala International University, Uganda[1]

ABSTRACT: Cloud computing is a new paradigm that combines several computing concepts and technologies of the Internet creating a platform for more agile and cost-effective business applications and IT infrastructure. The adoption of Cloud computing has been increasing for some time and the maturity of the market is steadily growing. Security is the question most consistently raised as consumers look to move their data and applications to the cloud. We justify the importance and motivation of security in the migration of legacy systems and we carry out an analysis of different approaches related to security in migration processes to cloud with the aim of finding the needs, concerns, requirements, aspects, opportunities and benefits of security in the migration process of legacy systems.

KEYWORDS: Security; Cloud computing; Migration; Legacy system.

I. INTRODUCTION

IT Risk Management

The purpose of risk management is to protect the values of an organization. This means that risk management first describes methods and procedures for analyzing potential scenarios that, if they occur, could have a negative effect on the organization. Organizations that are reliant on functioning IT operations are, therefore, faced with the challenge of identifying the specific scenarios that could arise from IT operations that have a potential negative impact on the organization.

Second, risk management recommends measures that have a mitigating effect on potential risk. It is at this point that organizations must consider the measures that are adequate and/or appropriate, since resources for implementing measures are finite and it is impossible to be 100 percent safe. This article describes an approach that can be used to establish the correlation among operational IT risk, the appropriateness of mitigating measures and organizational targets. This, in turn, means organizations can assess organizational targets that may be exposed to risk emanating from IT operations and to what extent. How does the risk associated with running an IT system impact organizational targets? When has an organization put in place sufficient measures to ensure an appropriate level of protection? Regardless of how many security measures are put in place to counter a risk, it is impossible to be completely safe. As a result, the key question an organization may ask is, “When have adequate, cost-effective and, therefore, appropriate controls and measures been implemented to ensure a risk does not seriously endanger the achievement of organizational targets?” Risk management is tasked with precisely providing the answer to this question.

What follows is based on the following premise: A risk scenario is manageable when adequate controls/measures have been put in place that reduce the negative consequences a potential incident will have on organizational targets to an appropriate level. Starting from this premise, this article will answer the following questions:

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 9, Issue 3, March 2020

What risk and/or risk scenarios can have a negative impact on organizational targets?
What controls/measures are appropriate? Categorizing Risk

The responsibility for effective risk management lies with organizational management. Accordingly, the challenge for risk management is to handle and summarize the numerous individual incidents of risk associated with running an IT system (referred to as operational risk) in such a way that the organization's management team can make effective decisions regarding risk control.

One example of a risk incident (isolated incident) would be a faulty turnstile system in a data center. This isolated incident arises from the operation of an IT system and is, therefore, an operational risk. The faulty turnstile system could result in unauthorized individuals gaining access to the data center, constituting a potential risk of data and/or infrastructure theft. If an organization runs several sites with access control systems, it is highly probable that faults will occur in these systems on more than one occasion. Furthermore, when an organization is above a certain size, it no longer makes sense to report every isolated incident to the organization's management team because the total number of incidents can be very large. For example, instead of reporting every single denial-of-service (DoS) attack to the management team, an aggregation can be reported (e.g., the number of attacks per day or month). The challenge here is how to group together isolated incidents so that the management team can use a range of aggregations to build up a complete picture of the operational risk that has been identified and, thus, make well-founded decisions.

One aim of risk management is, therefore, to stop talking about individual risk incidents at the management level and instead talk about the nature of similar incidents. It is essential to describe, group together and summarize pertinent incidents, using standardized criteria. When looking at the characteristics of a risk, it is important to consider the characteristics that will ensure a grouping produces sensible results.

Aggregating risk incidents based on the information assets (primary assets) that are affected provides an insight into the information values that are threatened by operational risk and potentially weighing which values are more or less affected. Grouping risk according to information assets brings information closer to business risk, because the IT systems (secondary assets) are excluded at the highest aggregation level.

Another option is to group operational risk according to risk scenarios. A risk scenario is the description of a potential incident that, if it occurs, will impact corporate and/or IT objectives. This impact can be positive or negative. A structure for describing a risk scenario can be found in the COBIT framework and can be used to describe organization-specific risk scenarios.

Risk Scenarios and Risk Categories
Standardization is essential to ensuring results can be compared; in this case, a standardized description of risk scenarios as suggested in COBIT 5 for Risk is described.
A number of scenarios are defined in the framework itself. Some of these scenarios are very generic, but, nonetheless, offer guidance for describing in-house situations. The structure specifications help when standardizing scenarios. The individual structure elements have the following meanings:

Threat—In very general terms, a threat is a set of circumstances or an incident that could result in a loss. This loss relates to a specific value such as an asset, expertise, objects or health. Transposed to the world of IT, a threat is a set of circumstances or an incident that could have an adverse impact on the availability, integrity or confidentiality of information, thereby potentially resulting in loss for the owner and/or user of the information. Examples of threats include force majeure, human error, technical failure and intentional acts.

Vulnerability—A vulnerability is a security-relevant fault in an IT system or institution. Causes can lie in the design, algorithms used, implementation, configuration, operation and organization. A vulnerability can result in a threat taking effect and an institution or system incurring a loss as a consequence. A vulnerability makes a subject (institution or system) susceptible to threats.4 In this context, it is important to note that both a threat and a vulnerability must be

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 9, Issue 3, March 2020

present when describing a risk. For example, fire is irrelevant as a threat to nonflammable substances, due to the absence of the associated vulnerability (burning)

Asset/resource—In general terms, an asset/resource can be described as an item of property belonging to an organization. In the case of Telekom Security, a distinction is made between primary assets (i.e., information) and secondary assets (e.g., people, buildings, IT assets).

Time—Time plays a crucial role in the description of risk as time is, among other things, an indicator for the probability of an incident taking place.

Threat type—A threat type describes in general terms the cause of an incident, i.e., whether an incident has been caused deliberately or by mistake.

Actor—Who is the actor? Is it an internal employee or external third party?

The first step in aggregating operational risk incidents is to group them according to scenarios. In complex environments, the number of risk scenarios can quickly rise to three figures, making it a good idea to further aggregate the incidents. In COBIT, risk scenarios are allocated to risk categories. The advantage of aggregating into risk categories is that this classification is generic enough to be applied to any organization and the number of categories remains stable over time. This type of aggregation and the stability of categories has an enormous advantage in reporting. If category-based reporting is introduced, the number and meaning of the categories will not change significantly over an extended period. This makes it easier for the people receiving the reports to read and understand the issues that are being presented.

Figure 1—Risk Categories Defined in COBIT

Number	Scenario
1	Portfolio Establishment and Maintenance
2	Program/Project Life Cycle Management
3	IT Investment Decision Making
4	IT Expertise and Skills
5	Staff Operations
6	Information
7	Architecture
8	Infrastructure
9	Software
10	Business Ownership of IT
11	Supplier
12	Regulatory Compliance
13	Geopolitical
14	Infrastructure Theft or Destruction
15	Malware
16	Logical Attacks
17	Industrial Action
18	Environmental
19	Acts of Nature
20	Innovation

Source: ISACA, *COBIT® 5 for Risk*, USA, 2013. Reprinted with permission.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 9, Issue 3, March 2020

COBIT defines 20 risk categories (figure 1) above comprising a total of 112 risk scenarios.

Figure 2—Scenarios in Regulatory Compliance

Number	Scenario	
1201	Noncompliance with regulations	There is noncompliance with regulations, e.g., privacy, accounting, manufacturing.
1202	Unawareness of potential regulatory changes	Unawareness of potential regulatory changes has an impact on the operational IT environment.
1203	Regulatory prevention of cross-border data flow	The regulator prevents cross-border data flow due to insufficient controls.

Source: ISACA, *COBIT® 5 for Risk*, USA, 2013. Reprinted with permission.

Figure 2 illustrates the correlation between riskcategories and risk scenarios by setting out the risk scenarios for the risk category Regulatory Compliance (line 12 in figure 1).

II. APPLYING CATEGORIZATION

Once the risk scenarios have been described and allocated to a risk category, this categorization can be applied, i.e., risk incidents or risk from IT operations (operational risk) can be allocated to a risk scenario. During practical application, it quickly becomes apparent that a risk incident cannot always be allocated one-to-one to a risk scenario. A certain learning curve is required, and a series of discussions are needed to make the process of allocating a risk scenario more practicable within an organization. However, this effort pays for itself twice over, first by improving the quality of results and, second, by initiating a substantive discussion that boosts risk affinity in the organization. When operational risk is allocated to one of these risk scenarios, a picture begins to emerge. Figure 3 shows an example. Without delving too deeply, it is clear that the operational risk can be restricted to five risk categories. The other risk categories are either irrelevant in terms of numbers, have not been found or are simply not relevant to the organization. This picture or, to put it another way, risk portfolio, initiates two key questions:

• What does the percentage distribution say about how safe the enterprise's IT operations are? For example, are the enterprise's operations safe enough from risk incidents in the Logical Attacks category?

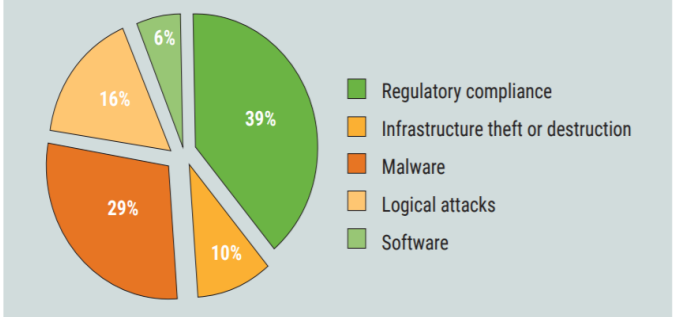
• How does this risk portfolio affect the enterprise's targets?

Defining an Appropriate Security Level

The question of what constitutes an appropriate security level in a risk scenario should be answered by the premise defined in the introduction: A risk scenario is manageable when adequate controls/ measures have been put in place that reducethe negative consequences of an incident to an appropriate level.

The following hypothesis is being established as a metric for adequate controls/measures: The controls/measures are adequate when the associated control processes can be considered to meet a high maturity level as per International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) 15504.

Figure 3—An Example of Risk Portfolio Based on Scenarios



ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 9, Issue 3, March 2020

If both hypotheses are combined, the following statement emerges: The maturity level of the control processes assigned to a risk scenario is a key performance indicator (KPI) for an appropriate security level.

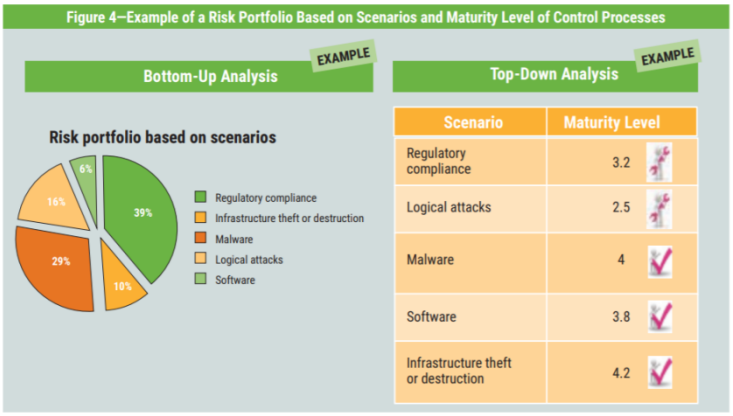
This statement necessitates reexamining the risk categories from COBIT. Control processes are allocated to each risk category. If these control processes have a high maturity level, it can be argued that the organization is well protected against risk incidents arising from that particular risk category. By contrast, if the maturity level is lower, there is a higher probability that the organization can expect negative consequences from risk incidents arising from that particular risk category.

Quantitative Correlation Between Organizational Targets and Security Level

Allocating risk incidents from IT operations to risk scenarios and combining these to form risk categories enables one to comment on the organization's risk portfolio. This approach is the equivalent of a bottom-up analysis. Evaluating the control processes' maturity level allocated to a risk scenario enables the enterprise to determine a maturity or security level. This approach is the equivalent of a top-down analysis. The bottom-up approach delivers the relevant risk scenarios for the company. Knowing them, the organization can focus on these scenarios during the top-down analysis. The maturity level for each scenario is calculated through a self-assessment of the relevant control processes. If the standard COBIT scenarios are used, the relevant controls are the process enablers assigned to each risk scenario. The assessment can be based on the COBIT Process Assessment Model. At the end of the self-assessment of each control process for onescenario, an average must be calculated to get to one aggregated number—the maturity level. The next step is to compare the bottom-up and top down analyses, as shown in figure 4.

In the Infrastructure Theft or Destruction category, as an example (line 14 in figure 1), it can be seen that there is real, concrete risk in IT operations that infrastructure could be stolen. Compared to the overall number of risk factors, the number of risk factors in this particular category is low. At the same time, figure 4 shows that the control processes the organization uses to mitigate the risk in this category have scored a high maturity level. In this example, it can, therefore, be said that the measures to protect against infrastructure theft constitute an appropriate security level. Nonetheless, there can—and will—be cases when infrastructure (e.g., cellphones, laptops) is stolen. It goes without saying that these isolated incidents must be analyzed and evaluated for potential improvements to be identified. However, from the viewpoint of the organization management team, there is no immediate need for action because an appropriate security level has been achieved in relation to infrastructure theft.

Figure 4–Example of a Risk Portfolio Based on Scenarios and Maturity Level of Control Processes



Once a systematic correlation has been established between operational risk from IT and the risk categories, COBIT also provides a concept for analyzing how organizational targets can be dependent on risk categories. According to COBIT, the achievement of IT objectives supports the achievement of organizational targets. In turn, risk emanating from IT operations influences the achievement of IT objectives.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 9, Issue 3, March 2020

Therefore, the following correlations apply:
• Corporate objectives depend on IT objectives.
• IT objectives depend on risk categories.
• Risk categories are groupings of risk scenarios.
• Risk scenarios are groupings of risk incidents from IT operations.
• Risk incidents from IT operations influence organizational targets.
The following approach is used to make a quantitative statement on the dependency of organizational targets:
• Corporate objectives are linked to a revenue expectation.
• Each organizational target is linked to one or more IT objectives.
• Each IT objective is linked to at least one risk category.
• A security level (maturity level) is stipulated for each risk category.
Based on these workings, the organization's management team has three choices:

1. Accept the situation.
2. Instigate immediate measures to improve control processes for the affected risk category.
3. Lower the target maturity level, resulting in a higher target achievement.

It is not possible to comment here on the most appropriate target maturity level for each risk category, as this will vary depending on how risk-averse the organization is. An organization that is more willing to accept risk will stipulate a lower target maturity level than an organization that is less prepared to accept risk.

III. RESULTS AND DISCUSSIONS

Every risk incident must be subjected to a detailed risk analysis and assessment. Not even standardization will change that. Furthermore, it will always be essential that the organization's management team is kept informed about matters in line with their importance and value. However, the standardization of operational IT risk does present organizations with an opportunity to identify systematic problems. Moreover, standardization on the basis of risk scenarios provides an opportunity to link organizational targets with risk incidents arising from IT operations. Determining the maturity level of the control processes for a risk category is a simple means of establishing a correlation between the achievement of organizational targets and risk incidents from IT operations. Clearly, this methodological approach still requires further practical evidence. However, the initial results from implementing it in organizational units at Deutsche Telekom AG gives cause to be optimistic that this is the right direction.

Protect, Detect and Correct Methodology to Mitigate Incidents Insider Threats

In terms of cybersecurity, many organizations tend to worry about external threats such as hacking or distributed denial-of-service (DDoS) attacks. These, after all, are what news organizations are likely to broadcast the most and, through availability bias, are likely to be what many executives and administrators tend to focus on when implementing information security controls for their organizations.

Unfortunately, external threats are not the only hazards organizations face, and the internal threat can be more common and the most catastrophic. This article explores the insider threat by defining the problem and examining what makes an insider threat. The article then presents strategies to mitigate the threats posed by insiders. Finally, it looks at mitigation strategies in terms of people, processes and technologies, and how each of these pillars can be used to protect, detect and correct insider threat activities and ultimately safeguard an organization's information.

The Insider Threat

While there is much focus on external threats such as hackers, according to a recent survey by the SANS Institute, insider threats cause the most damage to an organization's security. As per the2014 Breach Level Index report from Gemalto, insider threats are the second leading cause of data loss in general and, according to the Verizon "2018 Protected Health Information Data Breach Report" (PHIDBR) (figure 1), the number-one cause of protected health

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

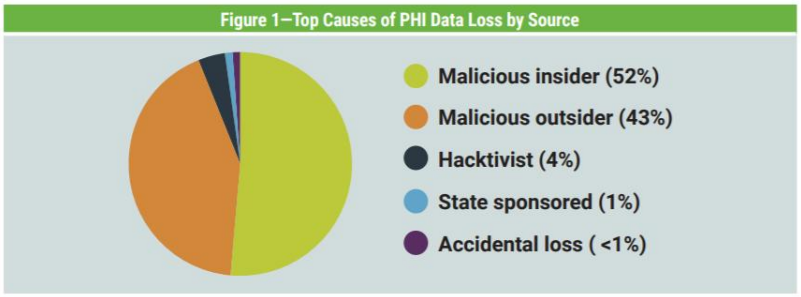
(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 9, Issue 3, March 2020

information (PHI) breaches. In the most glaring example, former US National Security Agency (NSA) contractor Edward Snowden caused exceptionally grave damage to US nationalsecurity by releasing terabytes of data to WikiLeaks and, in turn, to the United States' adversaries. More recently, another NSA contractor, Harold T. Martin III, was also accused of stealing terabytes of data, some of which related to the NSA's most sensitive operational element, the Tailored Access Operations (TAO) group, and providing it to the hacking group the Shadow Brokers. Although the full extent of the damage caused by these individuals may never be known, a recent US House Intelligence Committee report labeled Snowden's actions as causing "tremendous damage," endangering the lives of US troops and providing information that terrorists and enemy adversaries could use to create defensive measures against the United States. Obviously, the actions of these two individuals were detrimental to national security and exposed vulnerabilities in the NSA's information security. Fortunately, they were caught, but, unfortunately, not before they inflicted irrecoverable damage. Ideally, the US federal government would want to identify and stop insider threat activity before it causes damage.

The first step in mitigating these insider threat activities is defining who is or can be an insider threat. While there are numerous definitions of what constitutes an insider threat, many of them tend to vary regarding the insider's intentions. Previously, most definitions focused on an insider acting with malice; however, these definitions leave out a significant portion of insider threat activity. Therefore, the recently updated definition by Daniel Costa from Carnegie Mellon University's (Pittsburgh, Pennsylvania, USA) Software Engineering Institute is the most comprehensive. Costa's definition states an insider threat is:



The potential for an individual who has or had authorized access to an organization's assets to use their access, either maliciously or unintentionally, to act in a way that could negatively affect the organization

This definition paints with a broad brush and encompasses both intentional acts and unintentional acts. With this broader definition, administrators and executives can implement more effective countermeasures to mitigate these threats. Knowing that insider threats can be anyone with access to information, the next step for administrators is to determine what motivates them to act.

Motivations

The motivations of insider threats are as varied as the threats. Unintentional insiders may not have malicious intent but may be more motivated out of a desire to be helpful or efficient. Conversely, malicious insiders are likely motivated by their own self-interests or by revenge.

Unintentional Insider Threats Insiders can have myriad motivations that may cause them to act in a way that harms their organization's information security posture.

Unintentional insider threats, though not motivated by malice and in many cases occurring out of ignorance, are more likely to be driven by the desire to help. This innate desire to help can be leveraged by social engineers to infiltrate an informationsystem with the purpose of exfiltrating data.

Social engineering, or the manipulation of human beings to achieve a goal or objective, is a common tactic for hackers, scam artists and would-be infiltrators. For instance, according to a report by Phish Labs, the number-one cyberattack vector isphishing emails. With phishing emails, users receive an email they believe to be legitimate and then interact

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 9, Issue 3, March 2020

with the email, infecting their system. In many cases, the emails may appear to come from friends, coworkers or superiors, and the employee is manipulated into opening the email in a desire to be helpful or to provide a response, often filled with proprietary information, to an unauthorized person.

Phishing is a technical form of manipulation, where an employee unintentionally allows an unauthorized user to have access to an information system or is tricked into providing sensitive information. There are also physical forms of manipulation, such as hackers arriving at a building with their hands full, causing an empathetic employee to behave helpfully by holding the door open, thereby giving the unauthorized individuals access to the facility or information the intruders are not permitted to access. Moreover, employees are humans and, therefore, are prone to make mistakes. In some cases, an employee may inadvertently disclose classified data to unauthorized personnel or may mistakenly dispose of information in a way that makes it available to unauthorized persons through dumpster diving. In these cases, although the disclosure is unintentional, the impact may still be as grievous as the disclosures by malicious insiders Snowden and Martin.

Malicious Insider Threats

Regarding malicious insiders, their motivations are more sinister. Many US Central Intelligence Agency (CIA) case officers report that the motivations for espionage, which tend to mirror insider threat activity, can be described by the money, ideology, coercion and ego (MICE) acronym. Although these four motivations by no means encompass every possible motivation for espionage or insider threat activity, they do provide a good starting point for the conversation about what motivates malicious insiders.

In the case of Snowden, he claims to have had objections to the NSA's expansive surveillance of Americans. This ideological objection to the NSA's spying could have led Snowden to act in such a way as to expose what he may have thought to be illegal acts. However, the amount of data and the type of data Snowden released also indicate that his motivations were more than simply benevolence on his part. They suggest, in part, that ego may have also played a role in his activities. Since his revelation, he has not shied away from the media and seems to enjoy providing interviews and basking in the attention he has received as a modern-day Daniel Ellsberg, who, in the Vietnam era, released the Pentagon Papers.

Other insider threats may not arise from a sense of ideological generosity but may result from the insider's decision to compromise the organization's information security out of a desire for self-preservation or career advancement. In many cases, employees may steal data to sell to a competitor, damage the reputation of their previous employer or enhance their marketability. Unfortunately, this form of insider threat is more common than many executives and administrators realize. Other factors that could contribute to an insider's motivation to steal data or endanger the organization in some other way may be linked to an organization's culture or the recent business climate of the organization. These events may affect the ego or stability of an employee and result in the employee seeking retribution. In the case of an organization undergoing massive layoffs or downsizing, these developments may motivate an employee to commit acts of violence, fraud or theft of intellectual property. A study by security company Biscom revealed that 85 percent of employees take proprietary data with them when they leave a company to bring to another company. This staggering figure highlights that almost anyone is or can be an insider threat. This statistic—conjoined with Deloitte's analysis that the cost of a data breach extends beyond the loss of data and encompasses legal fees, damage to reputation, loss of intellectual property, and the new research and development needed to innovate newer technologies to replace what was lost—can easily become a devastating financial liability for an organization, a liability from which it may not recover.

Awareness of these motivations can help administrators recognize potential insider threat behavior. With awareness, organizations can also craft mitigation policies to help protect, detect and correct insider threat actions. The following section details how organizations can implement appropriate policies and put into place the right people and technologies to mitigate these threats.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 9, Issue 3, March 2020

People, Processes and Technology

The basis for information security management is to protect the confidentiality, integrity and availability (CIA triad) of an organization's data. To this point, this article has focused on the confidentiality of data. However, an insider threat can also cause damage to an organization's data integrity and availability, as an insider can manipulate the data to make the contents incorrect or damage information systems, making the data unavailable when needed. Any compromise to this CIA triad can adversely impact an organization. As such, any strategy an organization adopts should encompass measures to safeguard the entire information security spectrum.

Moreover, an organization's security strategy should provide protection to information in its three states. Data can be at rest, such as when data are stored on a computer or server. Data can also be in a state of processing, such as when an application is using or retrieving the data. Data can also be in transit, such as being sent via email or downloaded from the server. Regardless of the state of the data, administrators should seek to protect data as they move from state to state.

Further, the security strategy policy should encompass three key elements to be successful: people, processes and technology. Without a combination of these core elements, any security policy will fall short of providing the desired outcome.

People

People are the backbone of any information security ecosystem. Regarding insider threats, people are probably more critical, as people are both the threat and part of the security strategy. Security begins with individual employees, as they are often the weakest link in any security program. Having well trained employees who can recognize the behaviors and motivations discussed previously in this article can strengthen an agency's security posture. People are also necessary to monitor and respond to incidents created by insider threats. Without trained incident responders, the other key elements of processes and technology are meaningless. Having appropriate staff will enhance the effectiveness of controls designed for protection, detection and correction.

Processes

Of course, those control measures are heavily dependent on processes to guide the incident responders on what actions to perform. Researchers stress that processes are guided by policies, procedures, guidelines and work instructions. These documents should provide high-level instructions regarding the organization's security policy; dictate how, when and by whom communication takes place with external agencies in the event of an incident; and outline standard operating procedures to be followed to protect, detect and correct incidents. The policies should also dictate what constitutes risky behavior and should seek to increase monitoring on those deemed to have a higher risk. Two of the most basic processes an organization can adopt to ensure it hires and retains the best people are implementing rigorous pre-hire background checks and conducting periodic reexaminations of employees' backgrounds. Background checks provide insight into past behavior and indications of trustworthiness. Two questions worth considering include, "How honest was an employee on the job application?" and "Is an employee or prospective employee experiencing financial problems that may make him or her more likely to commit fraud?" While background checks are not a panacea to prevent or predict all insider threat behavior, they do provide a solid and cost-effective foundation.

Technology

Having the right technology can serve as a force multiplier for the organization's information security program. Although organizations do not always need the latest and greatest technology, they do require some tools to augment their employees and assist them with monitoring and responding to incidents. Tools assist with analysis and make managing large datasets across an entire enterprise more manageable. Without tools, it is hard for an organization to establish controls, which makes it difficult to protect information, detect when a problem arises and correct the problem, preventing further damage.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 9, Issue 3, March 2020

Protect, Detect and Correct

In selecting technological tools to mitigate the effects of a potential insider threat, administrators should first conduct a risk analysis and determine what information needs protecting, how much protecting it needs and for how long it needs protecting. They should also conduct a risk assessment to determine what vulnerabilities exist within the organization, such as employees providing their two-weeks' notice, and determine what level of risk these vulnerabilities pose. Once administrators understand the risk their information security faces, they can then begin to implement countermeasures for those identified vulnerabilities to mitigate risk to an acceptable level.

Preventive Controls

The first countermeasure that administrators should employ are controls designed to protect information (see figure below for an example controls matrix). One of the most basic controls is both policy- and technology-based: role-based access control (RBAC). RBAC operates under the premise of least privilege, or providing access to only the information or systems that a person needs based on the individual's position and need to know. RBAC inherently limits the distribution of information, reducing the chances of its unauthorized disclosure. Additionally, RBAC operates across all the various states of information, as long as people follow established processes and keep the information within controlled channels. Additionally, administrators can employ other technical controls, such as encryption, to protect information from unauthorized access.

Encryption is another basic control that administrators should use to protect the confidentiality of data. Encryption secures data by obfuscating plaintext data with unintelligible ciphertext data through the use of mathematical equations based on large prime numbers. When data are at rest or in transit, they can be encrypted, thus keeping the data confidential and available to only those authorized to view it.

Detective Controls

Unfortunately, not all protective measures for securing data are 100 percent effective. Hackers can obtain unauthorized access to the data or, in the case of insider threats, authorized persons can access the data and use them in an unauthorized manner, such as downloading the data to removable media before quitting the company. In these instances, it is important that an organization has controls to detect when unauthorized access or use has occurred.

To detect insider threat activity, administrators must rely on logs from various systems and witness devices, implying the existence of a technical solution for storing and reviewing security logs. Detection requires knowing what right looks like and realizing when behavior patterns do not fit within the standard deviation, which means having a trained staff to review the logs. It also means that there must be a policy that directs the security staff to review these logs with some frequency to determine that a problem exists. While there are expensive tools specifically created to detect insider threat activity through an automated review and analysis of these logs, an organization does not necessarily require having these tools to monitor their employees. Nevertheless, an organization does benefit from having, at a minimum, a data and log aggregator, such as Splunk, to compile logs and find patterns of irregularity. It also needs technically savvy auditors to comb through the data and look for events that violate the organization's security policies.

Corrective Controls

Automated tools such as data loss prevention can take action if they recognize a violation of an organization's security policy and prevent the activity from continuing, such as stopping a massive download of files to a removable media device. In cases where prevention is not possible, once an auditor or a technical solution discovers potential insider threat activity, administrators should immediately seek to correct the problem. Corrective actions should also be based on policy, and there should be an established process for incident responders to follow.

Ultimately, the earlier the problem is detected, the faster responders can mitigate the potential impact. Corrective actions could be as simple as notifying employees that they are committing a violation or as extensive as notifying law enforcement and investigating the incident. Once the incident is corrected, operations should resume and again focus on the protection of information and the detection of incidents.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 9, Issue 3, March 2020

Conclusion

Insider threats pose a tremendous risk to an organization's information security because, due to their nature, insiders "already have access to an organization's most sensitive data." The impactthey cause can be detrimental to an organization because insiders violate the trust the organization places in them and can damage the organization financially, reputationally and legally. Due to the risk insiders pose, organizations must take steps to mitigate the impact of their adverse actions.

An organization's security strategy should aim to protect the confidentiality, integrity and availability of its data. To protect this CIA triad, organizations should use an approach based on the three pillars of people, processes and technology. Supported by these pillars are the information security controls of protect, detect and correct. With the implementation of these controls, administrators should seek to protect data in all of their states, recognize when there may be a compromise and then strive to restore normal operations by minimizing the impact of the incident through corrective actions.

Security in Depth

Over the past 25 years, the methodology of network security has changed almost beyond recognition. With the aggressive pace at which data have grown and the need for constant real-time access becoming the norm, paying increased attention to securing networks and data has become critical. As data become ever more available online and organizations are obliged to offer access to their information across a publicly mistrusted medium, the potential for and reality of data compromise have become very real. Organizations lose billions of dollars each year through this very phenomenon.

Security breaches seem to be a daily occurrence, one of the most recent being the Equifax breach, in which tens of millions of records were stolen. Although, at the time of writing, the actual cost of this breach remains unknown, it could easily approach the US billion-dollar mark. With this level of loss becoming a real risk, businesses are committing increasing amounts of resources to bolstering their data security. Such efforts have seen the movement to a layered defense model becoming the norm. Experts in the field are designing security measures so that information entering and leaving an organization must pass through several layers, in an effort to fill the gaps left by using a single security device. Some of these methods will be discussed in detail in this article.

Layered security is part of a larger strategy known as "defense in depth." Although these terms are sometimes used interchangeably, they are not the same. Defense in depth, which was developed by the US military as a policy and method of defense, is best described as: "A defense in depth approach to security widens the scope of your attention to security and encourages flexible policy that responds well to new conditions, helping ensure you are not blindsided by unexpected threats."

Malware Defense

The prevention of malware is a significant factor when designing network security. How can one prevent malware from infiltrating the network? This pernicious software can be introduced in many ways. As an example, an email with a link prompting a user to download malware may be received; a user may mistype a web address and land on a rogue website designed to deliver malware; or a user may insert a malware-infected Universal Serial Bus (USB) stick into their computer. Once introduced, malware such as worm viruses can spread extremely rapidly to other unprotected, vulnerable computers and servers in the network.

With so many ways in which malware can enter a network, a single layer of protection is no longer sufficient. A popular method of layering defense against malware is to ensure that all data are scanned at least twice when entering and leaving the network.

To add another layer of protection, the scanning devices should be obtained from multiple vendors when possible. Malware protection typically works on signatures; using different vendors, with different signature databases, will fill in the gaps between signature update times to help protect against zero-day malware outbreaks. Security designers usually accomplish this goal by using malware protection end-point solutions for end-point scanning and layering these

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

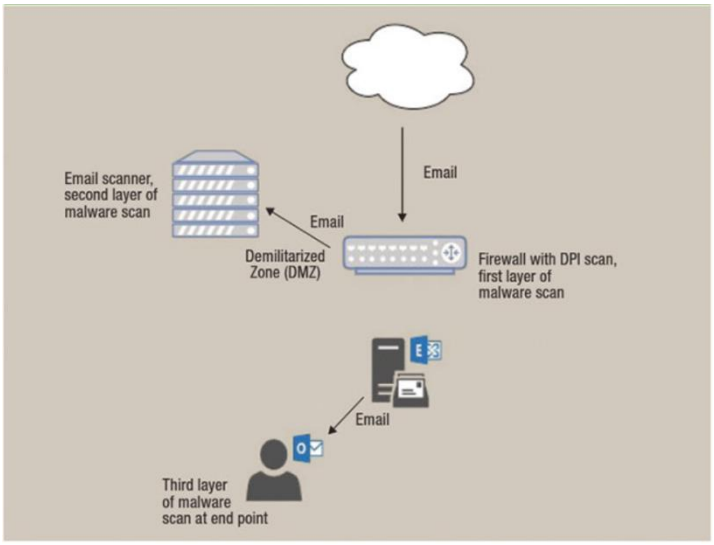
(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 9, Issue 3, March 2020

with email-scanning solutions and deep-packet malware scanning with a border device such as a firewall. This produces a multilayered scanning scenario. If someone sends an email to a user, the email is scanned for malware by the email scanner, then scanned again at the firewall level and then a third time by the end-point security software (see figure below). According to the US Federal Communications Commission, "The idea of layering security is simple: You cannot and should not rely on just one security mechanism to protect something sensitive. If that security mechanism fails, you have nothing left to protect you.

Layered Malware Scanning



Border Protection

The network security perimeter is the first layer of defense in any network security design. Network traffic flows in and out of an organization's network on a second-by-second basis. The data move from an untrusted to a trusted network and vice versa, which is a huge concern to security designers. How can this "border" between the two areas be protected to ensure the trusted network remains secure?

It was once held that the implementation of a firewall at the border and the network would be enough. That methodology is no longer sufficient in today's environment, where the untrusted network (the Internet) is a playground for hackers that is open 24/7. Restricting security to the implementation of a firewall alone is like locking the doors to a house with no alarm system.

Organizations need layered defenses at their borders, and the most effective way of obtaining that is through the use of both a firewall and an intrusion detection and prevention system (IDPS), preferably from different vendors so as to cover any vulnerabilities in the protection engendered by relying on a single vendor; any suspicious activity can then be reported (figure shown below).

Firewalls may be extremely effective, but they cannot be relied on as the sole means of securing a network perimeter. In fact, the SANS Institute has determined this to be one of the seven most common mistakes made by management that jeopardize network security.4 Protecting the border, although a high priority, is not sufficient. Security needs to evolve from protecting the edge of the network from unauthorized access and malware into a layered security approach.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

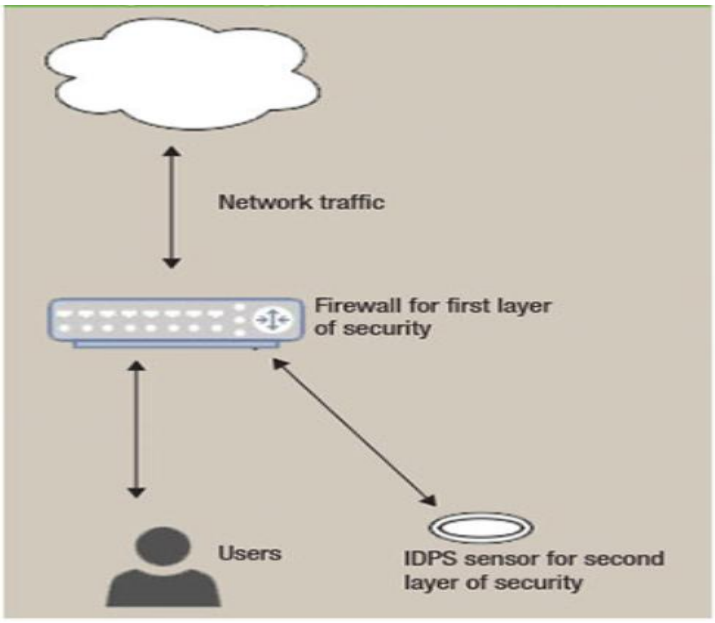
Visit: www.ijirset.com

Vol. 9, Issue 3, March 2020

Network Design

One of the most effective ways of achieving the goal of layered defense is through the design of the network. A flat network is the most vulnerable of all; networks with one single segment are vulnerable because publicly accessible resources must be accessed directly inside the network via the untrusted network (the Internet). For example, if an email server is positioned inside the network and accessed directly from the Internet and provides only one set of firewall rules, the security lacks any layers and is, therefore, weak.

Layer with Firewall and IDPS



How is the layered security model applied to offset this weakness? In short, security designers implement a separate segment between the two networks called a demilitarized zone (DMZ). This requires traffic coming from the Internet, and bound for the email server, to pass through the DMZ area first. Then, once authorized, the request for email access passes from the DMZ back through another, more restrictive, set of firewall rules to the actual email database. This allows the security administrator to be much more restrictive in terms of access. Without the DMZ, all network traffic bound for the email server passes. In contrast, with the DMZ in place, the administrator restricts traffic only from the web server front end to the email database in the trusted network, thereby accomplishing the goal of layered security via network design. An IDPS will also scan the network traffic, creating yet another layer of security.

In addition to adding a DMZ segment at the network entry point, additional steps can be taken to section off high-priority assets on the network. For example, in the banking industry, typically at least one segment is used that possesses the highest level of security in the internal network. In industries with extremely high-risk assets, protecting the data from the outside is extremely important, as is protecting them from the inside. When customers go into a bank, they do not just see the cash sitting on the floor; rather, it is secured inside a vault, which creates another physical layer of security.

High-risk assets typically occupy their own segment, protected by another set of internal perimeter security devices. The security mechanisms may be firewalls or jump servers. Designers will create red (for low-security) and black (for high-security) zones. To move from a red to a black zone, in which high-priority databases reside, the user must go through a jump server. The latter first requires a Remote Desktop Protocol (RDP) session before accessing the database. This creates yet another layer of security in the network.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 9, Issue 3, March 2020

Proxy

An additional and valuable layer of protection that should be included in a comprehensive layering approach to security is the use of a network proxy or firewall proxy. A content filter at the network level is critical to the overall strategy. Proxies can filter out .exe or .bat files, which can greatly enhance the overall security package. Advanced filters can also filter based on application type and reputation. These filtering databases are typically cloud-based and can be fast to respond to zero-day outbreaks of malware. They can also be highly effective at dealing with ransomware.

An application proxy acts as a gateway between the end-user system and the Internet, essentially hiding and protecting the end point. The user system makes contact with the application proxy, while the proxy communicates, on behalf of the user, with the external server. The latter never has access to the internal network. Although proxy systems alone are not a solution to security, they add a pleasing complement to virus protection and several other layers of network defenses.

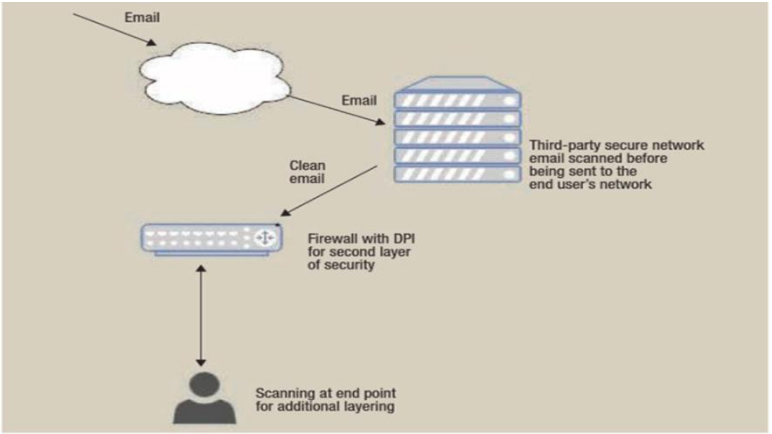
Third-Party Networks

With security designers so concerned with preventing breaches and virus outbreaks in their internal networks, the security industry has responded by offering solutions that prevent potential malware from ever entering the end user's environment. To complement the implementation of end-point security software and deep-packet scanning at the firewall level, many designers also use third-party networks to scan for threats before the traffic enters the end user's network.

An excellent example of this is email scanning in the cloud using a vendor network. Several vendors offer this service, including Barracuda and AppRiver. The design requires email sent to the end user to be diverted to the third-party network, where it is scanned for viruses, phishing, spam or many other combinations of filters. Any potential threats are removed before the clean email is sent to the end user's internal servers. These security solutions are extremely granular and very quick to respond to outbreaks.

An added benefit of this service is that traffic bound for the internal email server is reduced significantly. According to statistics, more than 69 percent of emails sent in 2013 were either spam or viruses. The number of spear-phishing email campaigns increased by 91 percent in 2013 over the year before, indicating that attackers had become more sophisticated in their assaults. They are learning about the end users and targeting specific individuals deemed to be high-value targets.10 With that type of statistic, the added layer of passing the Internet traffic through a third-party network where the traffic can be scanned for threats is of high value in a layered-security approach (Figure below).

Third-Party Network Layering



ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 9, Issue 3, March 2020

Physical Security

Although the need for physical security may seem obvious, it can all too easily be overlooked. It makes no sense to have a layered approach to network security and neglect the physical aspect. Physical security is not merely a layer of network security; it needs to be layered in its own right. For example, one key that allows access to the server room, or one camera that records entry to the building, is not sufficient. Access to the building should be restricted and monitored, just like the network infrastructure. If someone compromises the network from the outside, the organization's mechanisms should alert employees and allow them to establish what information was compromised and for how long.

Physical security should serve the same purpose: If someone compromises the physical security, resources should be in place to tell who breached the defenses, when and where. This is done by deploying security guards where possible and having keyed and logged access to the building, including separate access to sensitive areas such as the data center. Access to the building should be recorded via a camera system, while a separate system should monitor access to sensitive areas.

These components, just like network logging, should be reviewed on a regular basis. It is not advantageous to have cameras in place if no one is reviewing them, nor to have electronic card access if the logs are not evaluated. Alerts should also be configured to rouse security personnel regarding any failed attempts to access the building or sensitive areas. In sum, physical security is a key component of a layered security implementation.

Authentication

Authentication is the process of proving that people are who they say they are. This procedure is at the core of every security system in use today. As discussed in this article, these systems have layers of protection to keep people who are not meant to be there, or to have access, out of the network and away from data. These processes cover the back doors and prevent the infiltration of malware. Authentication is the process of allowing permitted access through the front door of a network. This operation must also be layered, just like other sections of the network. How is this accomplished? By using multifactor authentication (MFA). "The goal of MFA is to create a layered defense and make it more difficult for an unauthorized person to access a computer system or network." Every authentication system can be compromised and should not, particularly those with high-value assets (e.g., banks, power plants), rely on a single form of authentication.

Designers can use several options to achieve MFA. These can be broken down into three categories: something one knows (a password), something one has (a token number or code sent via email or text), or something one is (biometric). Security designers combine two or more of the three categories to create MFA. The procedure is effective only when two or more passwords are required. For example, a person accessing a financial database may be required to enter a password (something he/she knows), then enter the code from a smart card (something he/she has), and may still be required to scan a fingerprint or iris for access. Following this process allows for layered security during authentication.

User Education

With the increase in social engineering and zero-day attacks, user education plays a huge part in a layered security approach. The end user may be the final or first (depending on where the attack originates) line of defense. To ignore the user would be a massive mistake. With script kiddies becoming more prevalent, these amateurs can easily circumvent firewalls by sending mass emails in an attempt to persuade users to click on loaded links; the user must be aware of the risk. According to one expert:

A strong security architecture will be less effective if there is no process in place to make certain that the employees are aware of their rights and responsibilities. All too often, security professionals implement the 'perfect' security program and then forget to factor the customer into the formula.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 9, Issue 3, March 2020

Testing

The final step in any sound security design is the testing phase. Routine testing should be a matter of written policy and followed to the letter; network security officers should look at themselves as military personnel and be constantly prepared for an attack. Building defenses, setting alarms and monitoring is not enough—it is necessary to constantly test the defenses. Such testing must be performed both internally and externally, by internal staff and outside security experts. "Penetration testing is like having a mock firefight on a military base." White-hat hacking, penetration testing and vulnerability testing are crucial in a layered security approach to network defense.

IV. CONCLUSION

With the increase in data breaches and the resultant cost to organizations, the protection of networks and data is paramount. Firms cannot afford to turn a blind eye to network security. Organizations are increasing their security spending, and in many cases these additional resources are going to add layers of defensive mechanisms.

Security designers are using various approaches to layering defenses to thwart hackers and prevent data loss. They are implementing layers to prevent malware infections and head off hackers at the border, and increasing the complexity of network design to add additional passes through checkpoints for data access. Designers are also routing traffic through third-party security networks before entry into the trusted network to weed out threats before they ever enter the network.

Those in charge of physical security, meanwhile, are implementing layered security in their design and complementing network-based layered security. The process of MFA is quickly becoming de rigueur in the move to standardize the process of a layered defense. Security officers are educating their user base as well as using mechanisms to test the effectiveness of their programs.

Policy design and implementation are crucial in designing and implanting layered security. The security policy of modern networks is to mandate many layers of data scanning before entry and/or exit from the network. Although these methodologies will not prevent all data loss, with the concept of layered security becoming the norm, they will play a significant role in protecting the networks of today and tomorrow.

REFERENCES

[1]Perrin, C.; "Understanding Layered Security and Defense in Depth," TechRepublic, 18, 2008.
[2]Mohamed, T. S.; "Security of Multifactor Authentication Model to Improve Authentication Systems," Information and Knowledge Management, vol 4, Issue 6, 2014.
[3]Choi, Y. B.; C. Sershon; J. Briggs; C. Clukey; "Survey of Layered Defense, Defense in Depth and Testing of Network Security," International Journal of Computer and Information Technology, vol 3, Issue 5, 2014.
[4]McGuiness, T.; "Defense In Depth," SANS Institute, Vol.11, pp.525,2001.
[5]Williams, J.; "Practical Threat Management and Incident Response for the Small- to Medium-Sized Enterprises," SANS Institute, 2014.
[6]Musa, S.; "Five Steps to Take on Ransomware Using a Defense-in-Layers Approach," Government Technology, Vol. 14,2016.
[7]Roesler, J.; "Defense in Depth Layer Six: Application Security," Topics on Information Security, Vol.6.2013.
[8]Dominguez, J. A.; "An Overview of Defense in Depth at Each Layer of the TCP/IP Model," SANS Institute, 2002.
[9]Banathy, A.; G. Panozzo; A. Gordy; J. Senese; "A Layered Approach to Network Security," Industrial IP Advantage, Vol 3,2013.
[10]Federal Communications Commission, "Cyber Security Planning Guide," USA, p. 3, 2016.
[11]Symantec, Internet Security Threat Report Vol.19 2014.