I.J. Information Technology and Computer Science, **2013, 04, 55-67**
Published Online March 2013 in MECS (http://www.mecs-press.org/)
DOI: 10.5815/ijitcs.2013.04.07

A Proposed Model for Datacenter in -Depth Defense to Enhance Continual Security

[1] Dr **Nashaat el-Khameesy** & [2] **Hossam Abdel Rahman Mohamed**
[1] Prof. and Head of Computers & Information systems Chair, Sadat Academy
[2] Computer & Information System Dept - Sadat Academy
Computer & Information System Dept - Sadat Academy for management Science –Maady-Cairo-Egypt
[1] Wessasalsol@gmail.com & [2] Hrahman@Transit.com.eg, HAbdel@Enr.gov.eg

***Abstract*—** Defense in Depth is practical strategy for achieving Information Assurance in today's highly datacenter environments. It is a "best practices" strategy in that it relies on the intelligent application of techniques and technologies that exist today. The strategy recommends a balance between the protection capability and cost, performance, and operational considerations. This paper provides an overview of the major elements of the strategy and provides links to resources that provide additional insight. Companies need to address the security challenges of datacenter using a comprehensive defense-in-depth strategy. No single security solution will keep a determined thief from the goal of compromising the hardware or software given enough time and resources. Applying multiple layers of system security will slow the progress made by a thief, and hopefully, force the thief to abandon the pursuit, at the least, resale of the stolen property, and at worst, of confidential corporate data. The Defense in depth is the concept of protecting a Datacenter with a series of defensive mechanisms such that if one mechanism fails, another will already be in place to thwart an attack. In this paper, the main focus is given to highlight the security aspects of data center from perspectives of threats and attacks from one side and approaches for solutions from the other side. The paper also proposes an effective and flexible distributed scheme with two salient features. Our scheme achieves the integration of continual security improvement and Security Risk localization. This paper deals with the implementation of defense in depth at a strategic, principle-based level and provides additional guidance on specific sets of controls that may be applicable to support an organization's defense in depth initiatives. The paper will present in Section (1) the Defense in depth concept, Section (2) Threats, Adversaries, Motivations, Classes of Attack and Vulnerability Analysis, Section (3) Information Security Assurance, Defense in Multiple Places, Layered Defenses, Security Robustness, Section (4) Design Goals and finally proposed solution and provide The IT Security Role & Functional Matrix

***Index Terms*—** Defense in Depth, Information Security, Threats, Attack, Risk Management, Datacenter Continuity

I. Introduction

Defense in depth promotes the idea that a layered approach to datacenter security makes for a formidable challenge for attackers to circumvent and/or compromise networks and their systems. The general principle is to have several layers of defense, sometimes overlapping, to provide the broadest and most complete coverage of the datacenter. [1] This would be accomplished utilizing diverse methods and technologies that integrate into a comprehensive representation of the datacenter. Defense in depth follows the premise that there is no single solution to network security that makes a datacenter completely secure. Instead, there is the more practical and effective practice of establishing several layers of security so that an intruder would have to navigate and compromise several layers of devices and policies in order to actually and fully compromises a datacenter without being noticed. Also, the intruder would find fewer opportunities and vantage points to successfully attack the network because of the distributed approach of defense in depth. [2] Defense in depth attempts to unify many approaches to security under an integrated umbrella of protection and awareness. The more layers, to a degree, the stronger the security and the more diversity the more comprehensive the protection. [3] An example to illustrate the defense in depth approach might be to establish a border router with access lists in order to enforce ingress and egress policy, also known as perimeter defense. To compliment this, a firewall might be put in place to provide network address translation, proxy filtering and more finite ingress/egress policy. From here, there may be a network intrusion detection system with one or more sensors monitoring traffic internally and looking for anomalies. Adding to this, host intrusion detection systems may be in place on critical servers and workstations in order to maintain and validate their integrity. [4] Virus detection compliments this by adding protection against malicious payload that gets carried in

via email, possibly avoiding policy and initial intrusion detection. A Syslog server could be established to provide centralized or redundant alerting of infrastructure devices as well as historical data that is easily backed up. Finally, a network management station can provide traffic analysis and network stability reporting for preventative actions as well as analysis of the events and trends that led up to a previous incident. This robust approach to network security offers a full spectrum of coverage and awareness to security issues and anomalous network activity. It provides near real time awareness to potential or active problems and security breaches while being meshed within the total infrastructure. Weaknesses and faults in the network devices can be recognized and addressed to prevent future compromise. The result is a very wide range in the types of protection, which are layered around each other to provide a broad depth of protection, prevention and awareness. [5]

II. Threats, Adversaries, Motivations, Classes of Attack

To effectively resist attacks against its information and information systems, an organization needs to characterize its adversaries, their potential motivations, and their classes of attack. Potential adversaries might include: Criminal Elements, Hackers, or Corporate Competitors. [6] Their motivations may include: intelligence gathering, theft of intellectual property, denial of service, embarrassment, or just pride in exploiting a notable target. Their classes of attack may include: passive monitoring of communications, active network attacks, close-in attacks, exploitation of insiders, and attacks through the industry providers of one's Information Technology resources. It's also important to resist detrimental effects from non-malicious events such as fire, flood, power outages and user error.

The following is brief listings of some major drivers to implementing security for datacenter from perspectives of challenging threats and attacks:

- Motivated professionals have advanced knowledge and computing skills. They pose a very high risk to an organization because they also have motivations (political, financial and personal) that drive their behaviors. These adversaries study all public domain information about an organization and conduct reconnaissance studies when possible. [7] Because they are motivated and targeted in their attacks, they continue attempting to penetrate an organization's information infrastructure until they have successfully achieved their goals.
- Perimeter defense strategies focus on protection from external threats. With the number of security attacks on the rise, relying on perimeter defense alone is not sufficient to protect enterprise data, and a single security breach can cripple a business [8]
- The number of internal attacks is on the rise thereby threatening NAS/SAN deployments that are part of the "trusted" corporate networks. Reports such as the CSI/FBI's annual Computer Crime & Security Survey help quantify the significant threat caused by data theft [9]
- The data stored in the cloud may be updated by the users, including insertion, deletion, modification, appending, reordering, etc.
- Individual user's data is redundantly stored in multiple physical locations to further reduce the data integrity threats.
- Newbie's, attempt to use tools and techniques that are well documented through publicly available publications and web sites. They tend to attack a wide array of organizations without a specific motive or intention beyond testing their capabilities and gaining access. They have only basic knowledge of attack techniques and concepts and can typically be defended against by using basic protection techniques. [10]
- Script kiddies, similar to newbie, attempt to use tools and techniques that are well documented through publications and public web sites. [11] These adversaries try to expand their knowledge and gain inside information about exploits and vulnerabilities through personal research and hacker community interaction to enhance the existing tools and create their own basic tools.
- Spooks/government agents/terrorists have extensive technology capabilities and intelligence resources. [12] These attackers have significant financial and technology resources to draw from, as well as in-depth knowledge of an organization's information infrastructure. They most likely use blended attack methods, including physical and technological means for attack and reconnaissance activities.

III. Threat and Vulnerability Analysis

Threat and vulnerability analysis is an exercise that models a particular solution or business process against attack scenarios and known vulnerabilities to evaluate its resiliency or capability to repel attacks. It utilizes intelligence capabilities such as technical knowledge, behavioral science and business logic to model attack scenarios, the likelihood of such attacks and the potential business impact if the attack were successful. [13]

Threat analysis activities require specific information. First, information must be gathered on the business process or solution to be analyzed, as well as the physical and logical data elements associated with it. Typically, this information is gathered from the business process owner and by utilizing the asset inventory. It is important to define the scope and

boundaries of the business process solution; otherwise, the threat analysis can become incomprehensible to the organization and challenging to complete. [14]

Some key additional considerations include the value of the solution or business process to the organization, the regulatory and/or legal constraints, and the impact on third-party activities. This information must be gathered through independent discussions with senior managers, consultations with regulators and interactions with third parties. Additional information can be gathered by examining the organization's business continuity and disaster recovery plans, which should include this type of information for the critical business processes of the organization.

IV. Information Security Assurance [15], [16], [17], [18]

Information Security Assurance is achieved when information and information systems are protected against such attacks through the application of security services such as: Availability, Integrity, Authentication, Confidentiality, and Non-Repudiation. The application of these services should be based on the Protect, Detect, and React paradigm. This means that in addition to incorporating protection mechanisms, organizations need to expect attacks and include attack detection tools and procedures that allow them to react to and recover from these attacks. An important principle of the Defense in Depth strategy is that achieving Information Assurance requires a balanced focus on three primary elements: People, Technology and Operations.

4.1 People

Achieving Information Security Assurance begins with a senior level management commitment (typically at the Chief Information Officer level) based on a clear understanding of the perceived threat. This must be followed through with effective Information Assurance policies and procedures, assignment of roles and responsibilities, commitment of resources, training of critical personnel (e.g. users and system administrators), and personal accountability. This includes the establishment of physical security and personnel security measures to control and monitor access to facilities and critical elements of the Information Technology environment. [19]

4.2 Technology

Technologies Today, a wide range of technologies are available for providing Information Assurance services and for detecting intrusions. To insure that the right technologies are procured and deployed, an organization should establish effective policy and processes for technology acquisition. These should include: security policy, Information Assurance principles, system level Information Assurance architectures and standards, criteria for needed Information Assurance products, acquisition of products that have been validated by a reputable third party, configuration guidance, and processes for assessing the risk of the integrated systems. The Defense in Depth strategy recommends several Information Assurance principles. These include:

4.2.1 Defense in Multiple Places

Given that adversaries can attack a target from multiple points using either insiders or outsiders, an organization needs to deploy protection mechanisms at multiple locations to resist all classes of attacks. As a minimum, these defensive "focus areas" should include:

A) Defend the Networks and Infrastructure

Protect the local and wide area communications networks (e.g. from Denial of Service Attacks) and Provide confidentiality and integrity protection for data transmitted over these networks (e.g. use encryption and traffic flow security measures to resist passive monitoring)

B) Defend the Enclave Boundaries

(e.g. deploy Firewalls and Intrusion Detection to resist active network attacks).

C) Defend the Computing Environment

(e.g. provide access controls on hosts and servers to resist insider, close-in, and distribution attacks).

4.2.2 Layered Defenses

Even the best available Information Assurance products have inherent weaknesses. So, it is only a matter of time before an adversary will find an exploitable vulnerability.

Table 1: Layered Defenses

Class of Attack	First Line of Defense	Second Line of Defense
Passive	Link& Network Layer Encryption and Traffic Flow Security	Security Enabled Applications
Active	Defend the Enclave Boundaries	Defend the Computing Environment
Insider	Physical and personnel Security	Authenticated Access Controls, Audit
Close-In	Physical and personnel Security	Technical Surveillance Countermeasures
Distribution	Trusted Software Development and Distribution	Run Time Integrity Controls

An effective countermeasure is to deploy multiple defense mechanisms between the adversary and his target. Each of these mechanisms must present unique obstacles to the adversary. Further, each should include both "protection" and "detection" measures. These help to increase risk (of detection) for the adversary while reducing his chances of success or making successful penetrations unaffordable. Deploying nested Firewalls (each coupled with Intrusion Detection) at outer and inner network boundaries is an example of a layered defense. The inner Firewalls may support more granular access control and data filtering. [20]

4.2.3 Security Robustness

Specify the security robustness (strength and assurance) of each Information Assurance component as a function of the value of what's it is protecting and the threat at the point of application. For example, it's often more effective and operationally suitable to deploy stronger mechanisms at the network boundaries than at the user desktop.

4.2.4 Intrusions Detection

Deploy infrastructures to detect intrusions and to analyze and correlate the results and react accordingly. These infrastructures should help the "Operations" staff to answer questions such as: Am I under attack? Who is the source? What is the target? Who else is under attack? What are my options? and Deploy robust key management and public key infrastructures that support all of the incorporated Information Assurance technologies and that are highly resistant to attack. This latter point recognizes that these infrastructures are lucrative targets. [21]

4.3 Operations [22]

The operations leg focuses on all the activities required to sustain an organization's security posture on a day to day basis. These include:

- Maintaining visible and up to date system security policy
- Certifying and accrediting changes to the Information Technology baseline. The C&A processes should provide the data to support "Risk Management" based decisions. These processes should also acknowledge that a "risk accepted by one is a risk shared by many" in an interconnected environment.
- Managing the security posture of the Information Assurance technology (e.g. installing security patches and virus updates, maintaining access control lists)
- Providing key management services and protecting this lucrative infrastructure
- Performing system security assessments (e.g. vulnerability scanners, RED teams) to assess the continued "Security Readiness"
- Monitoring and reacting to current threats
- Attack sensing, warning, and response
- Recovery and reconstitution

V. Design Goals

The policy layer is probably the most overlooked and misunderstood aspect of information security. Security policies should be the foundation of every Defense in Depth plan. One of the main purposes of security policies is to educate all users of their obligation to the protection of the technologies and business information. Security policies help protect both business information and employees; we aim to design efficient mechanisms to resist attacks of data center and business Continuity verification and achieve the following goals:

5.1 Design Data Security

Refers to application of the principles, policies, and procedures necessary to ensure the confidentiality, integrity, availability, and privacy of data in all forms of media (electronic and hardcopy) throughout the data life cycle. [23]

- Develop data security policies using datacenter security standards, guidelines, and requirements that include privacy, access, retention, disposal, incident management, disaster recovery, and configuration
- Identify and document the appropriate level of protection for data storage in datacenter.
- Specify data and information classification, sensitivity, and need-to-know requirements by information type
- Create authentication and authorization system for users to gain access to data by assigned privileges and permissions
- Develop acceptable use procedures in support of the data security policy
- Develop sensitive data collection and management procedures in accordance with standards, procedures, directives, policies, regulations, and laws (statutes)
- Identify an appropriate set of information security controls based on the perceived risk of compromise to the data
- Develop security testing procedures.

5.2 Design Personnel Security

Refers to methods and controls used to ensure that an organization's selection and application of human resources (both employee and contractor) are controlled

to promote security, Personnel security controls are used to prevent and detect employee-caused security breaches such as theft, fraud, misuse of information, and noncompliance. These controls include organization/functional design elements such as separation of duties, job rotation, and classification. [24]

- Establish personnel security processes and procedures for individual job roles
- Establish procedures for coordinating with other organizations to ensure that common processes are aligned
- Establish personnel security rules and procedures to which external suppliers (e.g., vendors, contractors) must conform.

5.3 Design Datacenter Network and Telecommunications Security

Refers to application of the principles, policies, and procedures involved in ensuring the security of basic network and telecommunications services and data, and in maintaining the hardware layer on which it resides. Examples of these practices include perimeter defense strategies, defense-in-depth strategies, and data encryption techniques. [25]

- Develop Datacenter network and host-based security policies in accordance with standards, procedures, directives, policies, regulations, and laws (statutes)
- Specify Datacenter strategic security plans for Datacenter network telecommunications in accordance with established policy, to meet Datacenter security goals
- Develop Datacenter network and telecommunications security operations and maintenance Datacenter standard operating procedures
- Develop effective network domain security controls in accordance with enterprise, Datacenter network and host-based policies
- Develop Datacenter network security performance reports
- Develop Datacenter network security and telecommunication audit processes, guidelines, and procedures.

5.4 Design IT Security Training and Awareness

Refers to the principles, practices, and methods required to raise employee awareness about basic information security and train individuals with information security roles to increase their knowledge, skills, and abilities. [26]

- Develop the security awareness and training policy for the IT security training and awareness program
- Define the goals and objectives of the IT security awareness and training program
- Work with appropriate security SMEs to ensure completeness and accuracy of the security training and awareness program
- Establish a tracking and reporting strategy for IT security training and awareness
- Establish a change management process to ensure currency and accuracy of training and awareness materials
- Develop a workforce development, training, and awareness program plan.

5.5 Design Datacenter Security Risk Management

Refers to the policies, processes, procedures, and technologies used by an organization to create a balanced approach to identifying and assessing risks to information assets, personnel, facilities, and equipment, and to manage mitigation strategies that achieve the security needed at an affordable cost2[27]

- Specify Datacenter risk-based information security requirements and a Datacenter security concept of operations
- Develop Datacenter policies, processes, and procedures for identifying, assessing, and mitigating risks to information assets, personnel, facilities, and Datacenter equipment
- Develop Datacenter processes and procedures for determining the costs and benefits of risk mitigation strategies
- Develop Datacenter procedures for documenting the decision to apply mitigation strategies or acceptance of risk
- Develop and maintain Datacenter risk-based security policies, plans, and procedures based on security requirements and in accordance with standards, procedures, directives, policies, regulations, and laws (statutes).

5.6 Design Datacenter Continuity

Refers to application of the principles, policies, and procedures used to ensure that an enterprise continues to perform essential business functions after the occurrence of a wide range of potential catastrophic events [28]

- Develop an Datacenter continuity of operations plan and related procedures
- Develop and maintain Datacenter continuity of operations documentation, such as contingency, business continuity, business recovery, disaster recovery, and incident handling plans

- Develop a comprehensive test, training, and exercise program to evaluate and validate the readiness of Datacenter continuity of operations plans, procedures, and execution
- Prepare internal and external continuity of Datacenter operations communications procedures and guidelines.

5.7 Design Datacenter Operations and Maintenance

Refers to the ongoing application of principles, policies, and procedures to maintain, monitor, control, and protect IT infrastructure and the information residing on it during the operations phase of an IT system or application in production. Individuals with this role perform a variety of data collection, analysis, reporting and briefing activities associated with security operations and maintenance to ensure that the organizational security policies are followed as intended. [29]

- Develop Datacenter security administration processes and procedures in accordance with standards, procedures, directives, policies, regulations, and laws (statutes)
- Develop personnel, application, middleware, operating system, hardware, network, facility, and egress security controls
- Develop Datacenter security monitoring, test scripts, test criteria, and testing procedures
- Develop Datacenter security administration change management procedures to ensure that security policies and controls remain effective following a change
- Define IT security performance measures
- Develop a Datacenter continuous monitoring process
- Maintain the daily/weekly/monthly process of backing up Datacenter to be stored both on- and off-site in the event that a restoration should become necessary
- Develop a Datacenter plan to measure the effectiveness of security controls, processes, policies and procedures.

5.8 Design Datacenter Incident Management

Refers to knowledge and understanding of the process to prepare and prevent, detect, contain, eradicate, and recover, and the ability to apply lessons learned from incidents impacting the mission of an organization. [30]

- Develop the Datacenter incident management policy, based on standards and procedures for the organization
- Identify Datacenter services that the incident response team should provide
- Create Datacenter incident response plans in accordance with Datacenter security policies and organizational goals
- Develop Datacenter procedures for performing incident handling and reporting
- Create Datacenter incident response exercises and penetration testing activities
- Develop Datacenter specific processes for collecting and protecting forensic evidence during incident response
- Specify Datacenter incident response staffing and training requirements
- Establish the Datacenter incident management measurement program.

VI. Proposed Solution

Datacenter security Assurance is achieved when information and information systems are protected against such attacks through the application of security services such as: Availability, Integrity, Authentication, Confidentiality, and Non-Repudiation. The application of these services should be based on the Protect, Detect, and React paradigm. This means that in addition to incorporating protection mechanisms, organizations need to expect attacks and include attack detection tools and procedures that allow them to react to and recover from these attacks. This proposal is based on three main functions perspectives of Managing Solution, Implement and Evaluate

Manage Solution: Functions that encompass overseeing a program or technical aspect of a security program at a high level, and ensuring currency with changing risk and threat environments.

Implement: Functions that encompass putting programs, processes, or policies into action within an organization.

Evaluate: Functions that encompass assessing the effectiveness of a program, policy, process, or security service in achieving its objectives. [31]

6.1 Manage Solution

6.1.1 Managing Data Security [32]

- Ensure that data classification in Datacenter and data management policies and guidance are issued and updated
- Specify Datacenter policy and coordinate review and approval

- Ensure compliance with data security policies and relevant legal and regulatory requirements for datacenter
- Ensure appropriate Datacenter changes and improvement actions are implemented as required. Maintain confidentiality controls and processes in accordance with standards, procedures, directives, policies, regulations, and laws (statutes).

6.1.2 Managing Personnel Security

- Coordinate with IT security, physical security, operations security, and other organizational managers to ensure a coherent, coordinated, and holistic approach to security across the organization
- Ensure personnel security compliance with standards, procedures, directives, policies, regulations, and laws (statutes)
- Acquire and manage the necessary resources, including financial resources, to maintain effective personnelsecurity
- Establish objectives for personnel security to ensure alignment with overall security goals for the enterprise
- Ensure compliance through periodic audits of methods and controls
- Ensure personnel security is a component of enterprise continuity of operations
- Direct ongoing operations of the personnel security program
- Ensure that appropriate changes and improvement actions are implemented as required Ensure personnel security compliance with standards, procedures, directives, policies, regulations, and laws (statutes).

6.1.3 Managing Datacenter Network and Telecommunications Security [33]

- Establish a Datacenter network and telecommunications security program in line with enterprise goals and policies
- Manage the necessary resources, including financial resources, to establish and maintain an effective Datacenter network and telecommunications security program
- Direct Datacenter network and telecommunications security personnel
- Define the scope of a Datacenter network and telecommunications security program
- Establish communications between a Datacenter network and telecommunications security team and related security teams (e.g., technical support, security administration, incident response)
- Establish a Datacenter network and telecommunications performance measurement and monitoring program
- Ensure enterprise compliance with applicable network-based standards, procedures, directives, policies, regulations, and laws (statutes)
- Ensure that network-based audits and management reviews are conducted to implement process improvement
- Ensure that appropriate changes and improvement actions are implemented as required.

6.1.4 Managing IT Security Training and Awareness

- Identify business requirements and establish Datacenter-wide policy for the IT security awareness and training program
- Acquire and manage necessary resources, including financial resources, to support the IT awareness and training program
- Set operational performance measures for training and delivery, and ensure that they are met
- Ensure the organization complies with IT security awareness and training standards and requirements
- Ensure that appropriate changes and improvement actions are implemented as required.
- Ensure that information security personnel are receiving the appropriate level and type of training

6.1.5 Datacenter Security Risk Management

- Establish a IT security risk management program based on enterprise business goals and Datacenter objectives
- Establish the Datacenter risk assessment process
- Advise senior management on the impact during the decision making process by helping them understand and evaluate the impact of Datacenter security risks on business goals, objectives, plans, programs, and actions
- Acquire and manage the resources, including financial resources, necessary to conduct an effective risk management program
- Make determination on acceptance of Datacenter residual risk
- Ensure that appropriate Datacenter changes and improvement actions are implemented as required.

6.1.6 Managing Datacenter Continuity [34]

- Coordinate with corporate stakeholders to establish the Datacenter and enterprise continuity of operations program
- Acquire necessary resources, including financial resources, to conduct an effective enterprise continuity of Datacenter operations program
- Define the Datacenter Security continuity of Datacenter operational structure and staffing model
- Define emergency delegations of authority and orders of succession for key positions
- Direct contingency planning, operations, and programs to manage risk
- Define the scope of the Datacenter continuity of operations program to address Datacenter Security continuity, Datacenter recovery, contingency planning, and disaster recovery/related activities
- Identify and prioritize critical business functions
- Ensure that appropriate changes and improvement actions are implemented as required

6.1.7 Managing Datacenter Operations and Maintenance [35]

- Establish Datacenter security administration program goals and objectives
- Monitor the Datacenter security administration program budget
- Direct security administration personnel
- Address Datacenter security administration program risks
- Define the scope of the Datacenter security administration program
- Establish communications between the security administration team and other security related personnel (e.g., technical support, incident management)
- Integrate security administration team activities with other security-related team activities (e.g., technical support, incident management, security engineering)
- Acquire necessary resources, including financial resources, to execute the security administration program
- Ensure operational compliance with applicable standards, procedures, directives, policies, regulations, and laws (statutes)
- Collaborate with technical support, incident management, and security engineering teams to develop, implement, control, and manage new security administration technologies

6.1.8 Datacenter Incident Management [36]

- Coordinate with stakeholders to establish the incident management program
- Establish relationships between the incident response team and other groups, both internal (e.g., legal department) and external (e.g., law enforcement agencies, vendors, and public relations professionals)
- Acquire and manage resources, including financial resources, for incident management functions
- Ensure coordination between the incident response team and the security administration and technical support teams
- Apply lessons learned from information security incidents to improve incident management processes and procedures
- Ensure that appropriate changes and improvement actions are implemented as required
- Establish an incident management measurement program.

6.2 Implementation and Evaluation

Table 2: Implementation and Evaluation (6.2.1)

6.2.1 Data Security	
Implementation	**Evaluation**
• Perform the data access management process according to established guidelines • Apply and verify data security access controls, privileges, and associated profiles • Implement media control procedures, and continuously monitor for compliance • Implement and verify data security access controls, and assign privileges • Address alleged violations of data security and privacy breaches	• Assess the effectiveness of enterprise data security policies, processes, and procedures against established standards, guidelines, and requirements, and suggest changes where appropriate • Evaluate the effectiveness of solutions implemented to provide the required protection of data • Review alleged violations of data security and privacy breaches • Identify improvement actions required to maintain the appropriate level of data protection.

Table 2: Implementation and Evaluation (6.2.2)

6.2.2 Personnel Security	
Implementation	**Evaluation**
• Coordinate within the personnel security office, or with Human Resources, to ensure that position sensitivity is established prior to the interview process, and that appropriate background screening and suitability requirements are identified for each position • Coordinate within the personnel security office, or with Human Resources, to ensure background investigations are processed based on level of trust and position sensitivity • Review, analyze, and adjudicate reports of investigations, personnel files, and other records to determine whether to grant, deny, revoke, suspend, or restrict clearances consistent with organizational requirements, national security, and/or suitability issues • Coordinate with physical security and IT security operations personnel to ensure that employee access to physical facilities, media, and IT systems/networks is modified or terminated upon reassignment, change of duties, resignation, or termination	• Review effectiveness of the personnel security program, and recommend changes that will improve internal practices and/or security organization-wide • Assess the relationships between personnel security procedures and organization-wide security needs, and make recommendations for improvement • Periodically review the personnel security program for compliance with standards, procedures, directives, policies, regulations, and laws (statutes) • Exercise oversight of personnel security program appeals procedures to verify that the rights of individuals are being protected according to law.

Table 2: Implementation and Evaluation (6.2.3)

6.2.3 Datacenter Network and Telecommunications Security	
Implementation	**Evaluation**
• Prevent and detect intrusions, and protect against malware • Perform audit tracking and reporting • Apply and manage effective network domain security controls in accordance with enterprise, network, and host-based policies • Test strategic network security technologies for effectiveness • Monitor and assess network security vulnerabilities and threats using various technical and non-technical data • Mitigate network security vulnerabilities in response to problems identified in vulnerability reports • Provide real-time network intrusion response • Defend network communications from tampering and/or eavesdropping	• Perform a network security evaluation, calculate risks to the enterprise, and recommend remediation activities • Ensure that appropriate solutions to eliminate or otherwise mitigate identified vulnerabilities are implemented effectively • Assess fulfillment of functional requirements by arranging independent verification and validation of the network • Analyze data and report results • Ensure that anti-malware systems are operating correctly • Compile data into measures for analysis and reporting. • Ensure that messages are confidential and free from tampering and repudiation

Table 2: Implementation and Evaluation (6.2.4)

6.2.4 IT Security Training and Awareness	
Implementation	**Evaluation**
• Perform a needs assessment to determine skill gaps and identify critical needs based on mission requirements • Develop new or identify existing awareness and training materials that are appropriate and timely for intended audiences • Deliver awareness and training to intended audiences based on identified needs • Update awareness and training materials when necessary • Communicate management's commitment, and the importance of the IT security awareness and training program, to the workforce.	• Assess and evaluate the IT security awareness and training program for compliance with corporate policies, regulations, and laws (statutes), and measure program and employee performance against objectives • Review IT security awareness and training program materials and recommend improvements • Assess the awareness and training program to ensure that it meets not only the organization's stakeholder needs, but that it is effective and covers current IT security issues and legal requirements • Collect, analyze, and report performance measures.

Table 2: Implementation and Evaluation (6.2.5)

6.2.5 Datacenter Security Risk Management	
Implementation	**Evaluation**
• Apply controls in support of the risk management program • Provide input to policies, plans, procedures, and technologies to balance the level of risk associated with benefits provided by mitigating controls • Implement threat and vulnerability assessments to identify security risks, and regularly update applicable security controls • Identify risk/functionality tradeoffs, and work with stakeholders to ensure that risk management implementation is consistent with desired organizational risk posture.	• Assess effectiveness of the risk management program, and implement changes where required • Review the performance of, and provide recommendations for, risk management (e.g., security controls, policies/procedures that make up risk management program) tools and techniques • Assess residual risk in the information infrastructure used by the organization • Assess the results of threat and vulnerability assessments to identify security risks, and regularly update applicable security controls • Identify changes to risk management policies and processes that will enable them to remain current with the emerging risk and threat environment.

Table 2: Implementation and Evaluation (6.2.6)

6.2.6 Datacenter Continuity	
Implementation	**Evaluation**
• Execute enterprise continuity of operations and related contingency plans and procedures • Control access to information assets during an incident in accordance with organizational policy. • Establish an enterprise continuity of operations performance measurement program • Apply lessons learned from test, training and exercise, and crisis events.	• Review test, training, and exercise results to determine areas for process improvement, and recommend changes as appropriate • Assess the effectiveness of the enterprise continuity program, processes, and procedures, and make recommendations for improvement • Continuously validate the organization against additional mandates, as developed, to ensure full compliance • Collect and report performance measures and identify improvement actions • Execute crisis management tests, training, and exercises.

Table 2: Implementation and Evaluation (6.2.7)

6.2.7 Datacenter Operations and Maintenance	
Implementation	**Evaluation**
• Perform security administration processes and procedures in accordance with standards, procedures, directives, policies, regulations, and laws (statutes) • Establish a secure computing environment by applying, monitoring, controlling, and managing unauthorized changes in system configuration, software, and hardware • Ensure that information systems are assessed regularly for vulnerabilities, and that appropriate solutions to eliminate or otherwise mitigate identified vulnerabilities are implemented • Perform security performance testing and reporting, and recommend security solutions in accordance with standards, procedures, directives, policies, regulations, and laws (statutes) • Perform security administration changes and validation testing • Identify, control, and track all IT configuration items through the continuous monitoring process • Establish and maintain controls and surveillance routines to monitor and control conformance to all applicable information security laws (statutes) and regulations	• Review strategic security technologies • Review performance and correctness of applied security controls in accordance with standards, procedures, directives, policies, regulations, and laws (statutes), and apply corrections as required • Assess the performance of security administration measurement technologies • Assess system and network vulnerabilities • Assess compliance with standards, procedures, directives, policies, regulations, and laws (statutes) • Identify improvement actions based on reviews, assessments, and other data sources • Collect IT security performance measures to ensure optimal system performance. • Monitor vendor agreements and Service Level Agreements (SLA) to ensure that contract and performance measures are achieved • Ensure that IT systems operations and maintenance enables day-to-day business functions

Table 2: Implementation and Evaluation (6.2.8)

6.2.8 Datacenter Incident Management	
Implementation	**Evaluation**
• Apply response actions in reaction to security incidents, in accordance with established policies, plans, and procedures • Respond to and report incidents • Assist in collecting, processing, and preserving evidence according to standards, procedures, directives, policies, regulations, and laws (statutes) • Monitor network and information systems for intrusions • Execute incident response plans • Execute penetration testing activities and incidence response exercises • Ensure lessons learned from incidents are collected in a timely manner, and are incorporated into plan reviews • Coordinate, integrate, and lead team responses with internal and external groups according to applicable policies and procedures.	• Assess the efficiency and effectiveness of incident response program activities, and make improvement recommendations • Examine the effectiveness of penetration testing and incident response tests, training, and exercises • Assess the effectiveness of communications between the incident response team and related internal and external organizations, and implement changes where appropriate • Identify incident management improvement actions based on assessments of the effectiveness of incident management procedures. • Collect, analyze, and report incident management measures

IT Security Role and Functional Matrix

The IT Security Role, Competency, and Functional Matrix provide a visual representation of the linkage between roles, competency areas, and functions. In this section, IT security roles are broadly grouped into Executive, Functional, and Corollary categories.

Table 3: The Functional Matrix of IT Security Role

IT Security Functional Manage M Design D Implementation I Evaluate E		IT Security Roles																	
		Executive						Functional						Corollary					
		Chief Information Officer		Information Security Officer		IT Security Compliance Officer		Digital Forensics Professional		IT Systems Operations and Maintenance Professional		IT Security Professional		IT Security Engineer		Physical Security Professional		Privacy Professional	
IT Security Competency Areas	Managing Data Security	M		M	D							M	D		D				D
					E		E			I	E		E		E				E
	Personnel Security	M		M								D							D
							E					E				E	I		
	Datacenter Network and Telecommunications Security								D	M	D				D				
							E	I		I	E			I					
	IT Security Training and Awareness	M		M									D						D
					E		E					I	E						E
	Datacenter Security Risk Management	M		M	D								D					M	D
			E		E	I	E	I		I		I	E	I				I	E
	Datacenter Continuity	M		M							D						D		
					E		E			I			E			I			
	Datacenter Operations and Maintenance								D	M	D				D				
							E	I	E	I	E			I					
	Datacenter Incident Management	M		M	D						D		D					M	D
					E		E	I		I	E		E			I		I	E

VII. Conclusion

As we present in this paper the Defense in Depth is the most efficient and practical way to build an Information Security Plan, but it is not all there is to information security. Defense in Depth is the framework and/or foundation for your Information Security needs. We all know perfect security is a myth

and cannot be achieved, but with Defense in Depth strategies there is much that can be done to minimize risk. Stay the course; we're all in this together. As described by this paper, many security technologies only needs to be one step stronger than the thief is willing to pursue. Having a defense-in-depth strategy will provide many layers of security and will ensure that your defenses are strong enough to protect your datacenter. The Defense in depth is process not a product. It's a proactive approach to thinking about security from the inside out. Certain architectural approaches such as centralized security overlays lend themselves well to solve today interior security problems. Security continues to be an ongoing process and constant vigilance and user awareness play equally important roles in building the best security posture for Datacenter.

Acknowledgments

I would like to express our gratitude to Prof. DR/ Nashaat El- Khameesy & Prof. DR / Sayed Abdel-Wahab - Computers & Information systems Dept- Sadat Academy, The authors thankfully acknowledge the support provided by Trans IT Datacenter Operation Team

References

[1] Smith, C. L. /Understanding concepts in the defense in depth strategy, Paper presented at the IEEE 37th Annual International Carnahan Conference on Security Technology-14-16 October 2003

[2] Bass, T., & Robichaux, R. / Defense-in-depth revisited: qualitative risk analysis methodology for complex network-centric operations. Paper presented at the IEEE Military Communications Conference (2001)

[3] Bakolas, E., Saleh, J. H. "Augmenting defense-in-depth with the concepts of observability and diagnosability from Control Theory and Discrete Event Systems." Reliability Engineering and System Safety,, pp. 184–193, Vol. 96, Issue 1, 2011

[4] Souppaya, Murugiah, Kent, Karen, NIST SP 800-92, Guide to Computer Security Log Management, 2006, http://csrc.nist.gov/publications/PubsSPs.html.

[5] Peterson, Dale, Intrusion Detection and Cyber Security Monitoring of SCADA and DCS Networks, ISA, 2004, http://whitepapers.techrepublic.com.com/whitepaper.aspx?&docid=126355&promo=100511.

[6] CCSP Secure Intrusion Detection and SAFE Implementation, United States, Library of Congress ISBN: 0-7821-4422-5 © 2004 SYBEX Inc

[7] Suarez, G. / Challenges affecting a defense-in-depth security architected network by allowing operations of wireless access points (WAPs). Paper presented at the Symposium on Application and the Internet Workshops, Orlando, Florida , 27-31 January 2003

[8] Workman, M / Gaining Access with Social Engineering: An Empirical Study of the Threat, Information Systems Security, 16(6), pp. 315-331,(2007)

[9] Nashaat el-Khameesy,Hossam Abdel Rahman/ A Proposed Model for Enhancing Data Storage Security in Cloud Computing Systems, Journal of Emerging Trends in Computing and Information Sciences,VOL. 3, NO. 6, June 2012

[10] Debar, H. and Viinikka, J/ Security Information Management as an Outsourced Service, Computer Security, 14(5), pp. 416-434 (2006)

[11] Scarfone, Karen, and Mell, Peter, NIST SP 800-94, Guide to Intrusion Detection and Prevention Systems (IDPS), 2007, http://csrc.nist.gov/publications/PubsSPs.html.

[12] Byoungkoo Kim, Seungyong Yoon, and Jintae Oh, "Multihash based Pattern Matching Mechanism for High-Performance Intrusion Detection", International Journal of Computers Issue 1, Volume 3, 2009.

[13] CCSP Secure Intrusion Detection and SAFE Implementation, United States, Library of Congress ISBN: 0-7821-4422-5 © 2004 SYBEX Inc

[14] Saira Beg, Umair Naru, Mahmood Ashraf , Sajjad Mohsin/ Feasibility of Intrusion Detection System with High Performance Computing: A Survey,International Journal for Advances in Computer Science, Volume 1, Issue 1-December 2010

[15] ISO/IEC, "Information technology – security techniques – information security management systems – requirements," ISO/IEC 27001:2005(E), October 15, 2005.

[16] ISO/IEC, "Information technology – security techniques – code of practice for information security management," ISO/IEC 27002:2005(E), June 15, 2005

[17] ISO/IEC, "Information technology – security techniques – ISM guidelines for e-government services," ISO/IEC NP 27012, November 8, 2008

[18] Chien-Cheng Huang,Kwo-Jean Farn,Frank Yeong-Sung Lin/ A Study on Information Security Management with Personal Data Protection, 2011

IEEE 17th International Conference on Parallel and Distributed Systems

[19] Dhillon, G. and Torkzadeh, G/ Value-focused assessment of information System Security in Organizations, Information Systems Journal, 16(3), pp. 293-314 (2006)

[20] Federal Information Security Management Act of 2002, Section 301: Information Security, http://csrc.nist.gov/drivers/documents/FISMA-final.pdf.

[21] Harley Kozushko, "Intrusion Detection: Host-Based and Network-Based Intrusion Detection Systems", 2003

[22] http://infohost.nmt.edu/~sfs/Students/HarleyKozushko/Papers/IntrusionDetectionPaper.pdf

[23] Alma Whitten/Making Security Usable, School of Computer Science, Carnegie Mellon University, 5000 Forbes Avenue Pittsburgh, PA 15213-3890

[24] Koskosas, I.V., Charitoudi, G. and Louta, M/ The Role of Culture to Information Systems Security Management: A Goal Setting Perspective, Journal of Leadership Studies, 2(1), pp. 7-36 (2008)

[25] Albrechtsen, E/ A Qualitative Study of Users' View on Information Security, Computer and Security, 26(4), pp. 276-289 (2007)

[26] CCSP Secure PIX and Secure VPN Study Guide SYBEX Inc, United States, Library of Congress ISBN: 0-7821-4422-5 © 2004 SYBEX Inc

[27] Wilson, Mark, and Hash, Joan, NIST SP 800-50, Building an Information Technology Security Awareness and Training Program, 2003, http://csrc.nist.gov/publications/PubsSPs.html.

[28] Ross, Ron, et al., NIST SP 800-37, Revision 1, Guide for Applying the Risk Management Framework to Federal Information Systems, 2010, http://csrc.nist.gov/publications/PubsSPs.html and Ross, Ron, et al., NIST SP 800-39, Managing Information Security Risk, 2011, http://csrc.nist.gov/publications/PubsSPs.html.

[29] Siponen, M., Pahnila, S. and Mahmood, A. Employees' Adherence to Information Security Policies: An Empirical Study, in IFIP International Federation for Information Processing, Vol. 232, New Approaches for Security, Privacy and Trust in Complex Environments, eds. Venter, H., Eloff, M., Labuschagne, L. Eloff, J.von Solms, R., (Boston: Springer), pp. 133-144, (2007)

[30] Von Solms, R. and Von Solms, S.H / Information Security Governance: A Model based on the Direct- Control Cycle, Computers and Security, 25(6), pp. 408- 412 (2006)

[31] Grance, Tim, et al., NIST SP 800-61, Computer Security Incident Handling Guide, 2004, http://csrc.nist.gov/publications/PubsSPs.html.

[32] Ioannis V. Koskosas, Nikolaos Asimopoulos /Information System Security Goals, International Journal of Advanced Science and Technology Vol. 27, February, 2011

[33] Paul Rubel, Michael Ihde, Steven Harp, Charles Payne/ Generating policies for defense in depth Computer Security Applications Conference, 21st Annual, 10 pp. – 514, 9 Dec. 2005

[34] Christopher J. May, Josh Hammerstein, Jeff Mattson, and Kristopher Rush /Defense in Depth: Foundations for Secure and Resilient IT Enterprises, The Software Engineering Institute is a federally funded research and development center sponsored by the U.S. Department of Defense. ©2006 Carnegie Mellon University-September 2006

[35] Jay Ramachandran , Designing Security Architecture Solutions -Copyright © 2002 John Wiley & Sons, Inc. 605 Third Avenue, New York

[36] Duijm, N. J. "Safety-barriers diagrams as a safety management tool." Reliability Engineering and System Safety, Vol. 94, No. 2, 2009, pp. 332–341.

[37] Koskosas, I.V/ Goal Setting and Trust in a Security Management Context, Information Security Journal: A Global Perspective, 17(3), pp. 151-161 (2008)

Authors' Profiles

Dr Nashaat el-Khameesy: Prof. and Head of Computers & Information Systems, Chair, Sadat Academy, Maady, Cairo, Egypt

Hossam Abdel Rahman: Post-graduate student for degree of Master of Computer Science & Information System - Sadat Academy, Cairo , Egypt, He is currently position Data Center Operation Team leader at Trans IT Company –ENR, Ministry of Transportation

How to cite this paper: Nashaat el-Khameesy, Hossam Abdel Rahman Mohamed,"A Proposed Model for Datacenter in -Depth Defense to Enhance Continual Security(Applied Study to ENR Datacenter – Egyptian National Railways)", International Journal of Information Technology and Computer Science(IJITCS), vol.5, no.4, pp.55-67, 2013.DOI: 10.5815/ijitcs.2013.04.07