GKS SECURITY CONSULTING

ENPM 686: Information Assurance

Final Project Paper

Final Project Paper. By: Garleya Shimbura, Khushali Dalal and Sanusi Drammeh

5/15/2017

Disclaimer: There were some assumptions made in this paper. The names of companies are not real. They are just used for the purposes of this assignments and some of the claims of being registered under the University of Maryland is also not real.

Contents

1. INTRODUCTION

1.1. About KGS Consulting Company

KGS Security Consulting is a firm that was first established in spring 2017. Personnel of KGS has vast amount of experience in Cybersecurity; ranging from various areas like software, networks, systems, policies, legislation, and e-commerce.

KGS personnel have completed various security assignments around the globe, mainly in Africa and Asia. KGS provide the best solutions that companies would need, especially those that have become victims of cyber-attacks. KGS has the team to bring your security concerns to a concrete solution.

KGS are a registered company under the University of Maryland, A. James Clark School of Engineering department with certification license from the Office of Advance Engineering Education.

State Research Institute recently consulted KGS to provide security solutions in order to boost their productivity and operations.

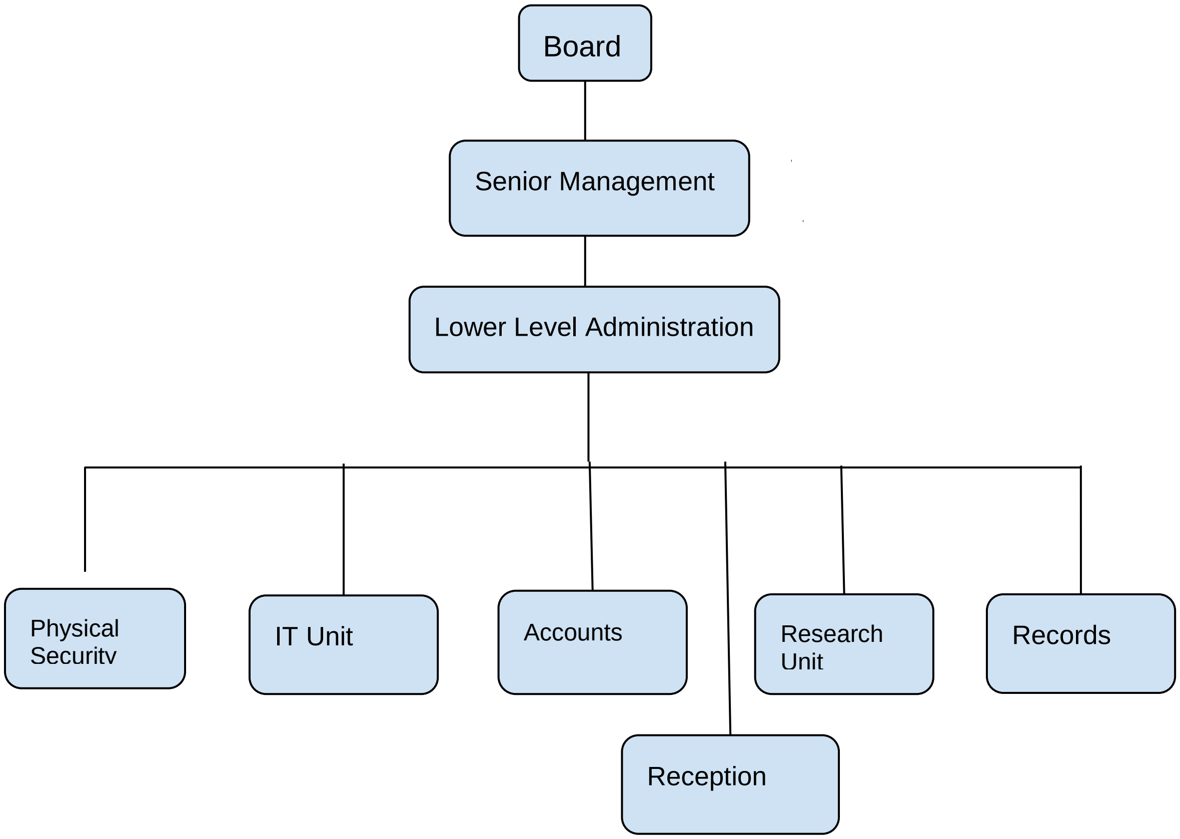
1.2. Objectives

Analysis and improvement of State Research Institute's overall system security and operations.

1.3. About State Research Institute (SRI)

The State Research Institute is one of the world's premier research institutions. SRI conducts groundbreaking research on some of the biggest challenges facing our global community, including cyber security and terrorism, bioengineering, public health equity, food safety and climate change. SRI strive to discover new knowledge and put it to work through innovation and entrepreneurship, advancing economic development and transforming lives. SRI publishes research for clients and also uses them as a base for future analysis. There are more than 100 students studying currently, over 5 undergraduate majors, and 5 graduate programs in the institute. SRI comprises of 57 distinguished faculty members (including full-time and part-time) and 30 staff members in all.

The diagram below shows the SRI's Hierarchy:



2. METHODOLOGY

Our approach to solving SRI's IT security constraints would be to cover for any shortfalls identified under the Confidentiality, Integrity, and Availability (C.I.A) Triad.

We would do a situational analysis to understand the current state of SRI and its assets. This, we intend to start with a SWOT analysis, which would enable us to fairly gauge the needs of SRI. Considering the current budget, our approach is intended to be cost-effective, yet reliable to address SRI’s needs as well as safeguard its assets by utilizing the best security plans, processes and tools.

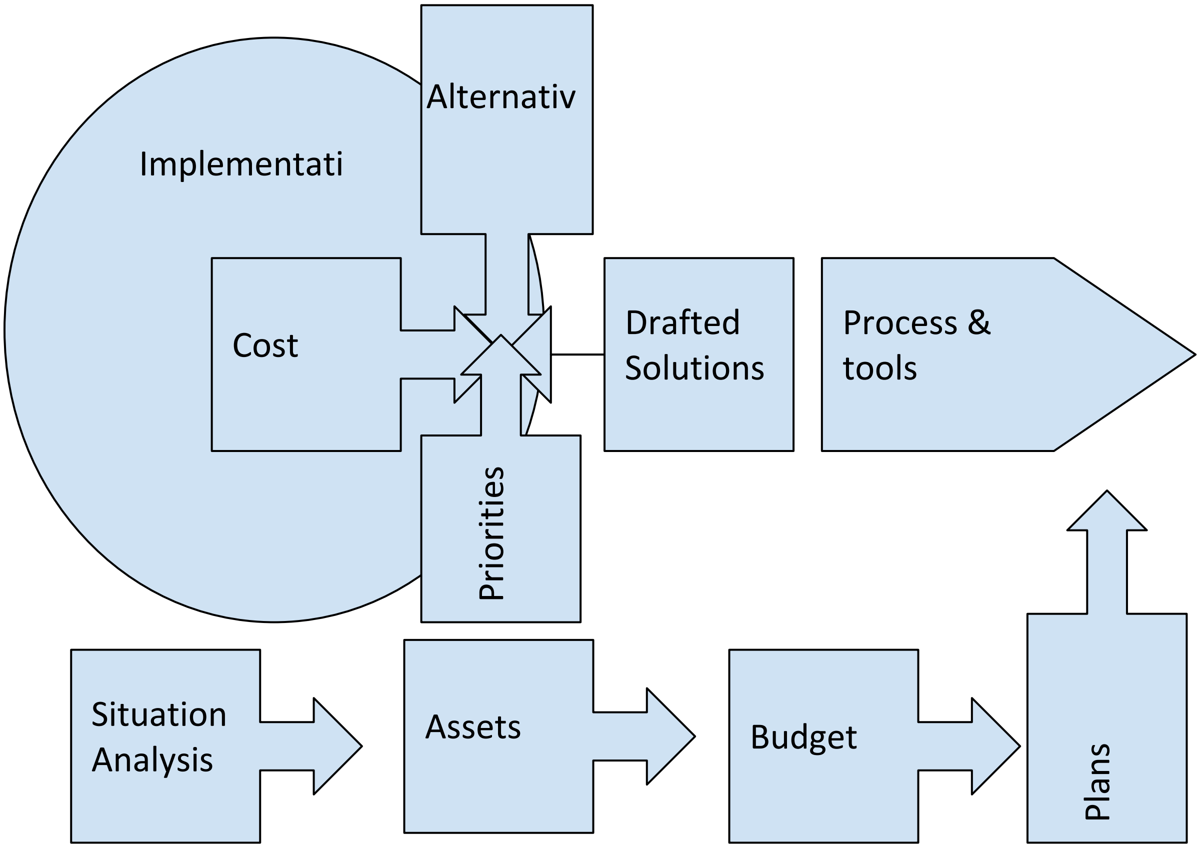
Secondly, after acquiring enough data, we would utilize this information to draft immediate solutions to solve SRI’s security issues.

Under a tight budget of $500,000, we would try to be as reasonable as possible to draw a considerate yet qualitative and constructive approach to our solution.

We would also have a list of all information and material needed for this assignment as well as their relative cost.

Then, we would prioritize our drafted solutions and reserve outstanding options as alternatives. We would also add to our cost a maintenance and contingency cost to cater in for unexpected issues along the way.

In brief, our approach outlines below:



3. SITUATIONAL ANALYSIS

3.1. Assets

After our analysis of the Assets of SRI, we have discovered that they have laid emphasis of Research Data. The institution's reputation came in second. The third was the employees. SRI seemed to have very competent people in Research and Data Analysis. Fourth, the systems that host their applications and resources interfaces their clients (such as their web server), Human Resource Management Systems, Customer Resource Management Systems and applications that warehouse their collected data for data mining purposes. This was followed by systems that transport them such as the networking devices. Lastly, the physical security. However, attention was not given too much on IT security even though they have prioritized IT equipment and services. A breakdown of the Assets and their priority is listed below:

No	Assets	Priority Level (10-50) 10: Lowest & 50: Highest
1.	Institution's Physical Premises	50
2.	Research Data	50
3.	Reputation	48
4.	Employees	45
5.	Database Systems	41
6.	Other Applications	41
7.	Hardware Systems	40
8.	Network Systems	39
9.	Physical security	30
10.	Institutions other physical resources (like cars, trucks, etc.)	20

3.1.1. User Information

All employees of SRI have registered information stored on the system. These include home addresses, emails, financial details and other personal information. This information is very important to the users and can be exploited in the wrong hands so has to be protected at all costs.

3.1.2. Research Data

Data is collected from various industries all over the world and used to generate meaningful information that is then the research papers. Some of this statistical data could be confidential and not meant for general viewing so has to be protected. The work done to actually gather this data could be very high and it being leaked and used by other people is both not fair and safe.

3.1.3. Research papers

Research data is converted into research papers by means of analysis and hard work by the employees. These papers are then published and sold for some profit or used privately by the State. These have to be prevented from getting into the wrong hands and also ensure that the company does not suffer financial loss by having their publications leaked to the general public.

3.1.4. Customer information

Some research papers are created for clients who pay the company for its services. This research could be pivotal in a company making a breakthrough or gaining an advantage over its competitors so this needs to be kept private in order not to give anything away. The customers would also normally want their information to be kept securely and privately so it has to be protected at all costs.

3.1.5. Hardware systems

The computers and other electronic devices need to be kept safe as they are expensive and also contain information on the hard drives. This implies that the security and state of these devices are very important

3.1.6. Network system

This is very important because this is the means by which everything is connected. Communication takes place over the network, and vital data is passed over so the integrity of this network has to be kept and maintained at all times.

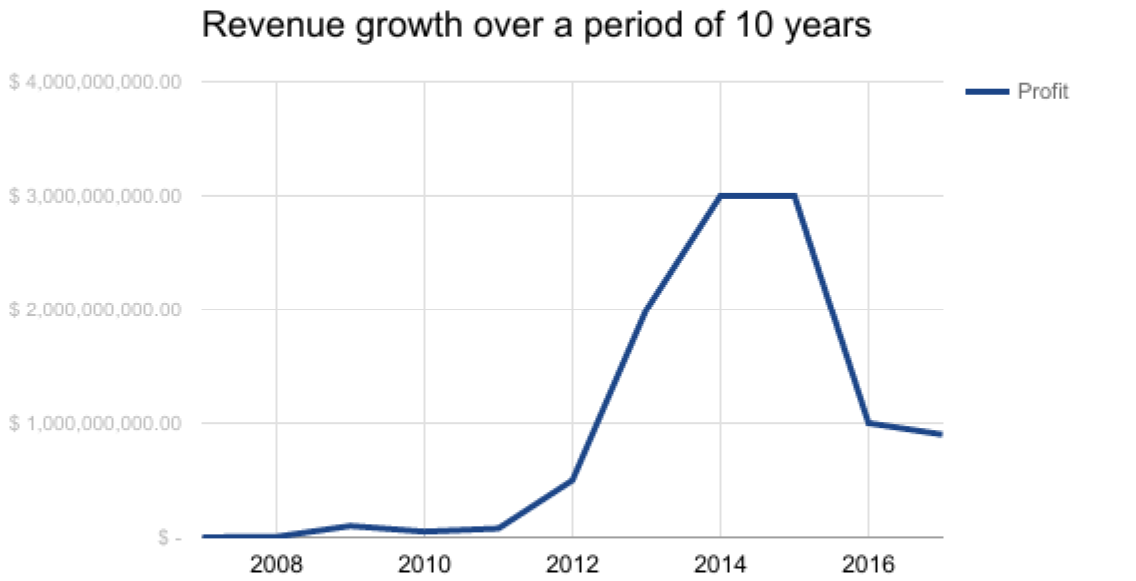
3.2. SWOT ANALYSIS

3.2.1. Strengths

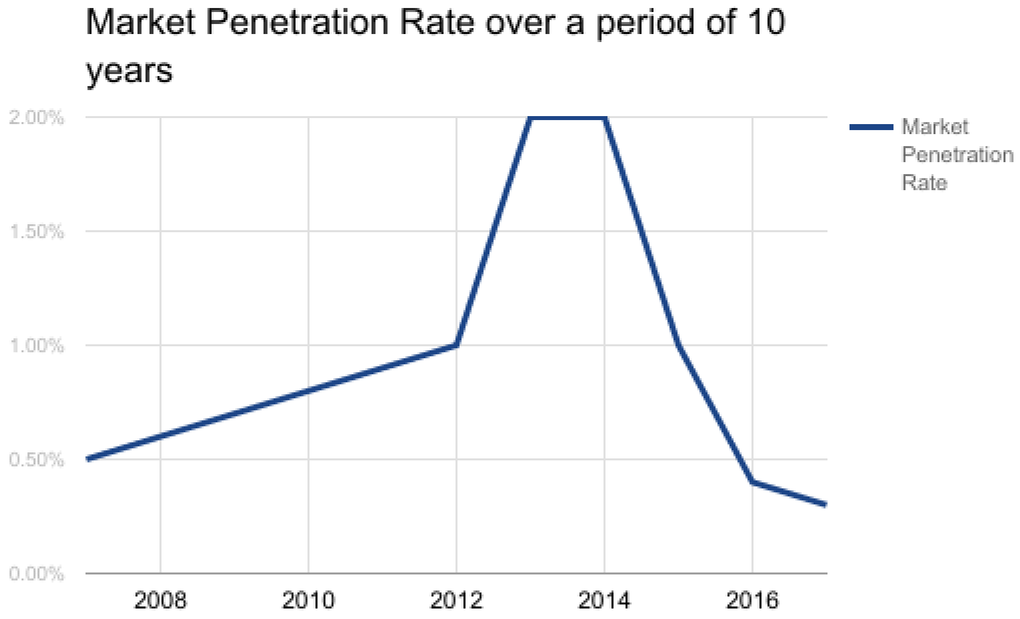
SRI, from a security standpoint, have more weaknesses and threats as opposed to its strengths right now. However, the fewer strengths it has would help us in trimming down our solutions and concentrate on areas that are affected. This would help us avoid some wasteful spending on redundant items and thereby conserve the resources of SRI.

The few strengths SRI poses is the human capacity in Data Analytics, Marketing, and a strong leadership, even though their familiarity with security issues is deficient. Another area of Strength the company has is in their financial muscle. SRI in the past decade SRI was able to generate 10 Billion dollars in revenue. And in that process, they have boosted their market niche to up to 10.20% from previous years.

Please see the below graphs for more details



Graph 1.0



Graph 2.0

As it could be observed from the statistics collected the revenue generated by the company over the years has helped the company to survive. But as the graph shows there was a steadily decline from 2016 to 2017 due to an increased attack on company assets like web servers that was brought down mostly between 2016 to 2017. So it affected the revenue generation of the company. Please see section 2.2 for more details.

3.2.2. Weaknesses

SRI's has inadequate security in various areas of its institution. Among them are policies, human resources, application systems, hardware systems, network systems, operations, physical security and backup.

- **Policies**

The first thing we assessed of SRI's current security state was its security policy. Unfortunately, the institution has a very weak security policy which neglects many important assets of the organization. It has not defined the organization's assets. The one it has highlighted was mostly centered on password policy and shutting down unattended workstations.

The first password policy started with the fundamentals. That passwords should not be less than 8 characters and that it should contain numbers, lowercase, uppercase and special characters. However after multiples complaints from employees pertaining to issues of password complexities managed revised their password policies without prior consultation of security experts. Now this policy has only maintained 8 characters minimum length and has scrubbed away all former requirements.

For Access Control, the policy has covered it. However, in practice what was discovered about SRI is a Discretionary Access Control (DAC), which is crucial subject to the owner of a particular resource on the system.

- **Human resource**

After completing a fact-finding mission on SRI's human resource capacity pertaining to critical information technologies, we discovered that they had only 1 IT personnel whose main job was to provide desktop support for employees. We evaluated his competencies and skills-set and discovered he had only 2 years working experience with SRI with no prior experience with another institution. The experience he had was only centered with Windows systems and the Company does have 100 Linux systems for the Research unit.

We also realized that the institution's workload was enormous on him as he had to multi-task on different assignments which he cannot effectively deliver alone. This has led the SRI to outsource most of its security demands to third party vendors. The vendors would normally charge insurmountable fees for basic troubleshooting as well as the development of applications of SRI's CRMS.

The table below shows the evaluation data collected in the area of information Security human resource and their capacity:

Table 1.0

No.	**Employee ID**	**Unit**	**Certifications Completed**	**Level of Experience in the field**	**Annual Salary**	**Workload**
1.	11221122	IT	MCSA	2 years	$ 30,000	All areas of IT
2.	11331133	Guard	Security Service	5 years	$35,000	Physical Security
3.	11331135	Guard	Security Service level 2	8 years	$45,000	Physical Security
4.	11331136	Guard	Security Level 3	10 years	$60,000	Physical Security
5.	11331137	Guard	Security Level 2	6 years	$45,000	Physical Security

From an organization that deals with sanitizing research data from various vital sectors, it evident that it understaffed in the Information Security domain. The only other security mechanisms they have from a human resource perspective is the security guards that ensure the physical security of the premises. Even though they have several surveillance cameras in the entire office. The data that is considered to be one of the company's vital assets can still be stolen virtually without the knowledge of the security guards.

Out of the five security personnel, as shown in table 1.0, only 1 is IT. The rest are guards. The second table below will show an assessment or feedback from management appraisals as to their effectiveness. It also shows how many times they have been promoted.

Table 2.0

No.	**Employee ID**	**Unit**	**Effectiveness (1-5) 1-lowest; 5 (highest)**	**Number of promotions**
1.	11221122	IT	2	None
2.	11331133	Guard	3	1
3.	11331135	Guard	4	1
4.	11331136	Guard	4	2
5.	11331137	Guard	2	None

Analyzing the data above it is evident that the effectiveness of the IT personnel is low and based on our investigations his involvement in different areas without prior experience might have impacted his performance.

- **Application Systems**

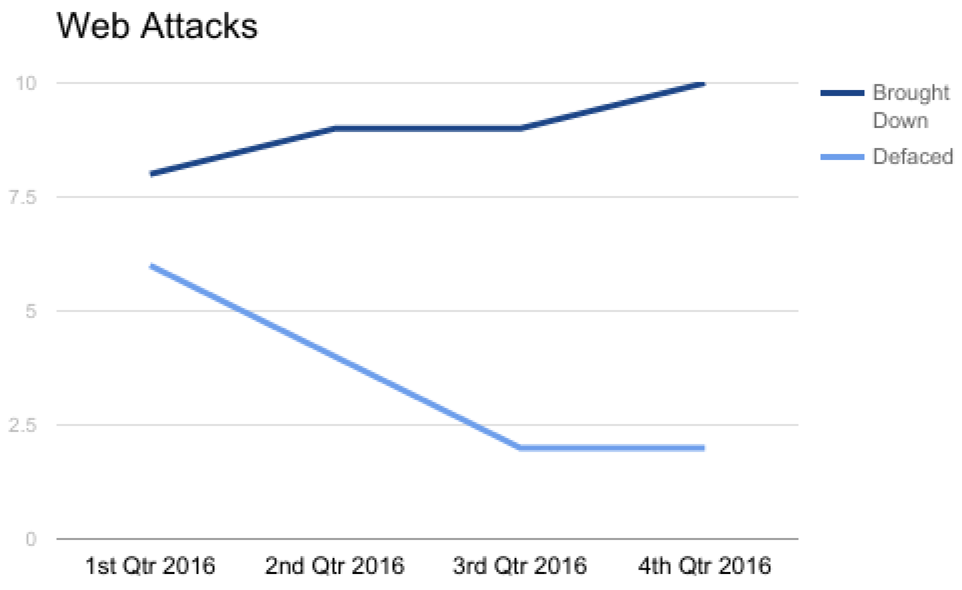
SRI is using Oracle's Human Capital Management System as their human resource tool. The company runs this expensive database application to keep employee data and help track and manage employee welfare as well as track other employee performance indicators.

Through our findings, we discovered that this application was being hosted on a windows 2003 R2 server which was last patched 2 years ago. We discovered that the Windows server was functioning multiple roles at the same time. It was the Web server, the DNS server, Active Directory, Application server as well as the File Server. The server was overloaded and also connected to the internet.

The server also had terminal services enabled on it like Remote Desktop connections (RDP) which are being used by employees to remotely log in to the server to complete certain tasks remotely. This remote connection is using the global internet and has no secure tunnel encryption or tunneling mechanisms set.

Also, the telnet, FTP which sends data in plain text were actively being utilized by employees. Other protocols and services were also left open such as SNMP, POP, RDP, IMAP etc. These open ports can be exploited by hackers to infiltrate the system.

The web server intended to be used for clients is running HTTP and there is no secure transaction present. Previous attacks have been reported by customers and the website has been brought down and defaced 50 times for the past 1 year.



Our analysis also discovered that all the 50 windows systems in the Administration unit, mainly used by senior management had pirated antiviruses installed which are mostly infested with malware or Trojan backdoors. We found only one valid anti-virus which was a Kaspersky 2016. However, the anti-virus's license expired 4 months ago and it was last updated 5 months ago. The antivirus installed on the server last conducted a full scan 6 months ago.

Analysis of the password policies set on the server showed that the default password policies of windows 2003 Active Directory were disabled, simply because employees complained of the inconvenience of entering complex passwords because of the difficulty to remember it. This had led to management allowing them to use passwords of their choice.

The table below shows the data collected on the types of applications and their respective issues:

No.	Application	Date of installation	Status	Security
1.	Windows Server 2003 R2	01/10/2008	Valid	Unpatched for 2 years
2.	Oracle HCM	03/15/2010	Valid	Not secured. Running with multiple applications on a single server.
3.	DNS, FTP, RDP, TELNET	02/10/2008	Valid	Unsecured ports left open
4	Web Server Joomla CMS 3.2	03/11/2008	Valid	Not secured. Legacy CMS version.
5	Anti-viruses (Kaspersky 2016)	10/20/2016	Expired	Not active
6	Antiviruses (pirated)	08/10/2016	Pirated	Not secured. Embedded with malware

We discovered that there was no Secure Socket Layer (SSL/TLS) settings on the Web server to encrypt web transaction of clients.

- **Hardware**

Our research has found that the security hardware of SRI is mostly old and outdated. This includes all the workstations and server. The Company has 100 Linux computers that are used by the Research unit and 50 windows computers used by the Administration unit.

The hardware is as old as 1990 and a few as new as 2015. Most of them are legacy, not optimized and therefore fall short of the requirements for new security software installation or upgrades.

There is also one Cisco legacy stateless packet filter firewall that is the only tool the organization relies on to protect it from threats coming from the internet.

The following table shows the list of hardware material found:

No.	Hardware	Specification	Release/Manufacture Date	Qty.
1.	Dell OptiPlex 7010 (Windows 2003 Server R2)	Graphics: Intel GPU Processor speed: 3.1 GHz Installed memory: 8 GB RAM Drive Capacity: 1 TB	November 2013	1
2.	Cisco PIX Stateless packet filter firewall	20 Mbps of firewall throughput	2009	1
3.	Dell OptiPlex 350 (Linux Ubuntu 14.0.4 LTS) workstations	4GB memory 160 GB HDD Intel Celeron 2.50ghz	2009	100
4.	Dell OptiPlex 350 (Windows) workstations	4GB memory 160 GB HDD Intel Celeron 2.50ghz	2009	49
5.	CCTV Camera	300ft long range night vision HD	2014	3

- **Network Systems**

As listed in the above table the network system includes the stateless filter firewall also an 1800 series Cisco router that was provided by the Internet Service Provider. There is no internal networking to a large extent such as segmentation or separation of the Administration network from the Research network, which could lead to data being leaked to unauthorized personnel from both domains.

The other networking devices available were generic network switches that are not intellect and unmanageable to optimize the network. There was also no Intrusion Detection or Prevention systems to detect or respond to attacks. There are no honeypots as well to learn from attack trends in order to help in decision making for future security interventions.

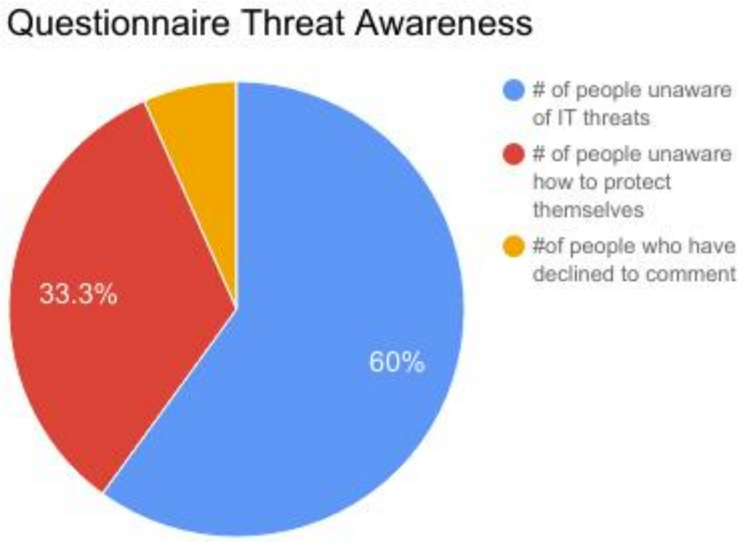
The list of networking devices is indicated in the table below:

No.	**Network Devices**	**Specification**	**Manufactured date**	**Qty.**
1	Cisco PIX Stateless packet filter firewall	20 Mbps of throughput	2009	1
3	3 Com Generic Switch	24 ports 100/1000 Mbps	2008	3
1	Cisco 1814 Router	IOS legacy	1998	1

- **Operations**

The daily operations of SRI are heavily dependent on data collection and analysis. This process has to go through tedious processes of sanitization and accuracy. Therefore availability is paramount as well as integrity and confidentiality of the data being processed. It is indeed best practice to introduce job rotation and switch roles of data analyst from one unit to another in order to prevent collisions and insider threats. The IT policy of SRI has not covered any aspects on this. Policies like forced leaves, system integrity check for modifications to critical data. Some of the employees are not aware that IT security threats occur or have an impact on business. Most of them though, do not know how to protect themselves against such attacks.

The chart below shows a respondent to a questionnaire given to employees.



- **Backup**

The only backup procedure that the organization relies on is a manual backup with tapes. This is done at irregular intervals and it is not automated. The tapes that are backed up are also stored in onsite. There is no vault system in place to support replication to offsite backup capabilities.

There is an absence of a Disaster Recovery Plan, which is usually activated once a disaster strikes an institution in order to recover from any loss it incurs.

3.2.3.Opportunities

Financial Muscle

From our analysis of SRI's financial muscle, we believe that this is an advantage the institution can leverage upon to provide the best security solutions in order to avoid future declines in revenue generation. Because of the majority of employees not being aware of security threats, and the minimal attacks that took place from previous years, there was some form of complacency from senior management. IT Security was never in the past considered a priority.

3.2.4.Threats

Using the STRIDE model, we were able to give an overview of the system and identify the threats and their points of entry.

3.2.4.1 Host-based (System Users)

As seen from the model, users (primary and admin) connect to the web server to make use of the system. These users are susceptible to Spoofing and Repudiation related attacks. However, they interact with the web server and the databases which come up with their own set of attacks. These attacks affected the users' use of the system and these attacks include

- **Poor web server authentication**

Pages on the web were not set up with proper security measures. Due to this, web pages were hijacked and the users connected to the system were interacting with the attackers' uploaded sites. Information was given out and this was not realized until a later date.

- **No server logs**

Server logs record the information taking place during a session and provides good information regarding system activities. These logs were absent in the system and this resulted in not being to prove if actions were taken or not so server activities could not be monitored or verified.

- **Leak of User credentials (Eavesdropping)**

The SRI building does not have any form of restriction to who accesses the building. Visitors could enter into the work area and listen in on conversations and watch closely and pick up sensitive data that should not be available to the public.

- **Phishing emails and Ransomware**

Also due to the improper setup of the web server and lack of awareness of users to the latest security trends, users fell for phishing emails and either gave out sensitive information or downloaded ransomware onto the systems which distributed via the web server and compromised the other connected systems on the network

- **Insider threats**

Of all the threats, this could be considered the most dangerous. No form of security can prevent the situation where a user willing fully gives out information that is either sensitive or could be used to carry out further attacks. Either due to frustration or a promise of a bribe, users decide to give attackers information without a care of those affected or hence the systems get easily compromised.

3.2.4.2 Network-Based

The setup of SRI's network is also a cause of the risks to its security. Network weaknesses without involving the user are carried out and this renders the system under control of the attacker where he is free to carry out a variety of attacks. These include

- **Man in the Middle attacks**

Improper set up of the web by means of no detection systems, no encryption and a lot of open services creates an avenue for attackers to perform Man in the Middle attacks. An attacker is able to redirect traffic between two clients or the client and server. With this, he can intercept messages in plain text as well as login credentials via listening on the FTP port and other services. The acquired data can then be published which translates to information disclosure and this data is the most important facet of SRI.

- **SQL Injection**

In this attack, an attacker takes advantage of database scripts and is able to formulate input strings that interact directly with the database. These commands resemble the scripts used to write databases so could be used to perform actions on the database like adding and dropping of tables. This could create a denial of service situation because by dropping a table, the user is denied the availability of the contents of that service. By adding information to a table, a user then accesses false data and works with it which results in the generation of wrong research publications and data.

- **Buffer overflow attacks**

This also falls under the improper coding of scripts. An attacker is able to input data that exceeds the length of a buffer and is able to access points in memory that he should not access to. The input could contain malicious code that runs on these memory locations and either crashing the system, providing remote access or the running of malware on the network.

- **Denial of Service**

The network was not designed to tolerate heavy load simultaneously. This, in turn, causes the system to crash or freeze when multiple requests are made at the same time. The users then have to wait for a system reboot by which time a lot of time may have passed or certain activities being performed may have to be started again. Infected systems with Trojans can also cause a denial of service when they are in communication with the system and the Trojans increase the load on that particular system or network thereby causing a crash.

3.2.4.3. Policy issues

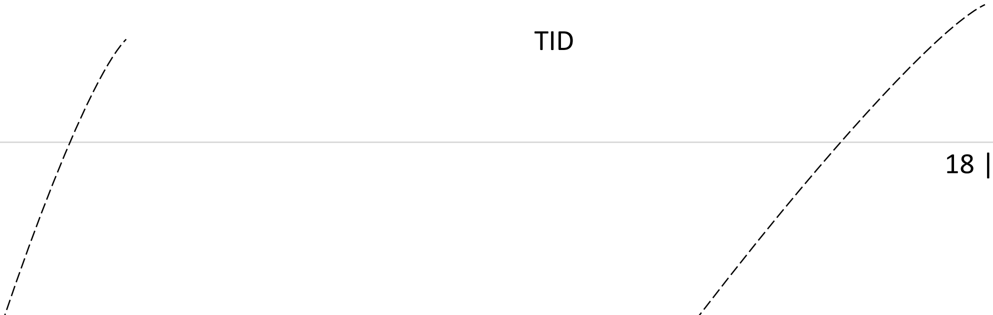
Exploited threats could also be attributed to poor security policies set up to ensure that the security of the system is intact. These policies form the background of how security is enforced and access is controlled. If not properly implemented, security and system operations could be affected. The policies being used at SRI are very weak and are either poorly thought out or nonexistent. These are:

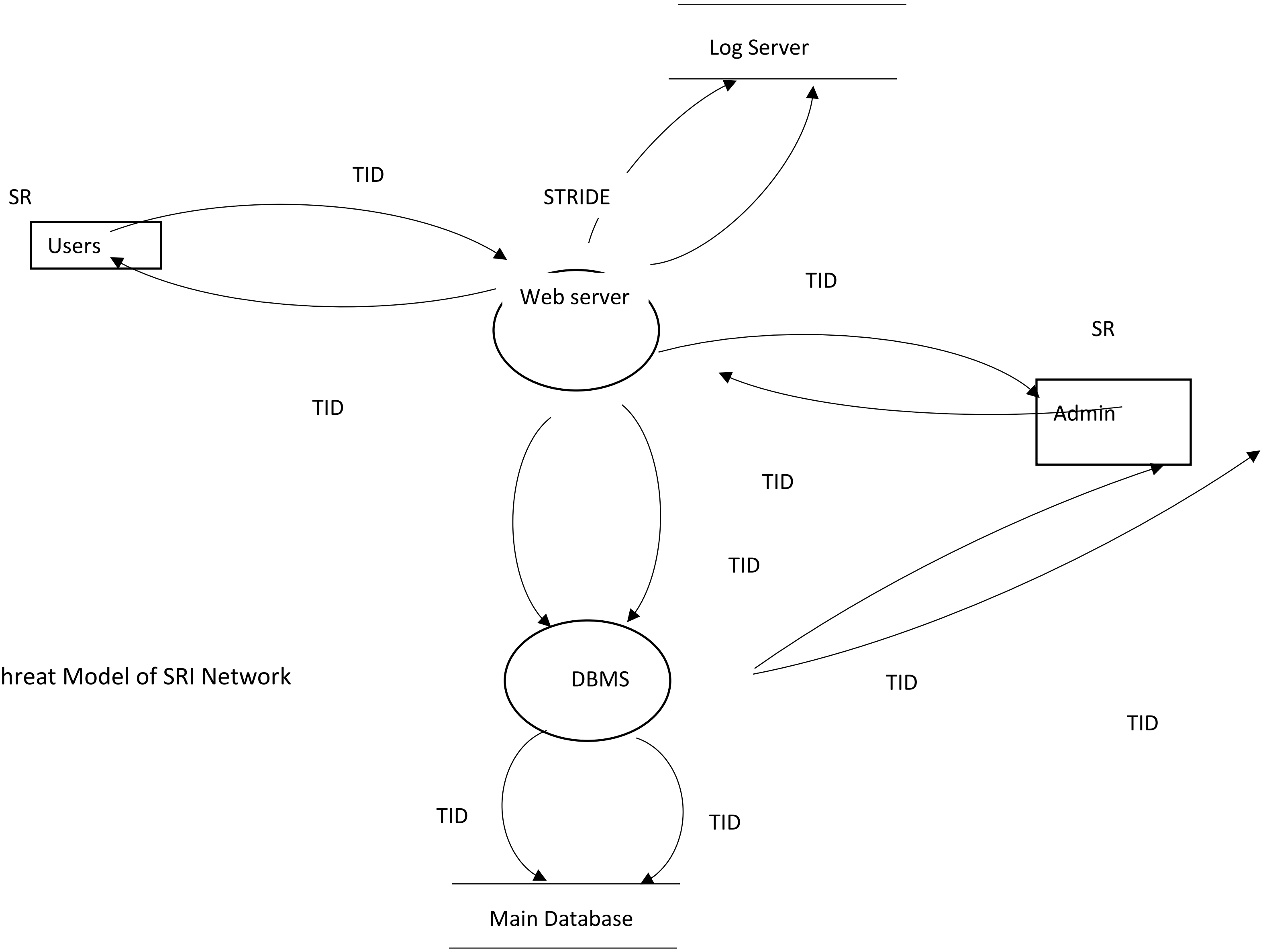
- **Weak Password Policies**

Users require passwords to log into the network and access their data. Users have multiple accounts over the internet (email, social media, fantasy leagues, etc.) and may be difficult to remember so end up setting easy or common passwords (words with meaning). These type of passwords are weak to brute force attacks because they constitute easy to remember strings or slight variations of words. By ensuring that a user has his password easy to remember, the lack of complexity makes systems more prone to attacks by external and unauthorized individuals.

- **Weak Access Control policies**

Access Controls define which user has access to a particular file or function in a system. These policies identify who has the rights to perform core functions (execute, read and write) to a file so that they can be controlled and monitored. SRI did not set this up and these caused issues whereby files were edited by people of not high enough security clearance or required expertise which resulted in errors in compilation of data.



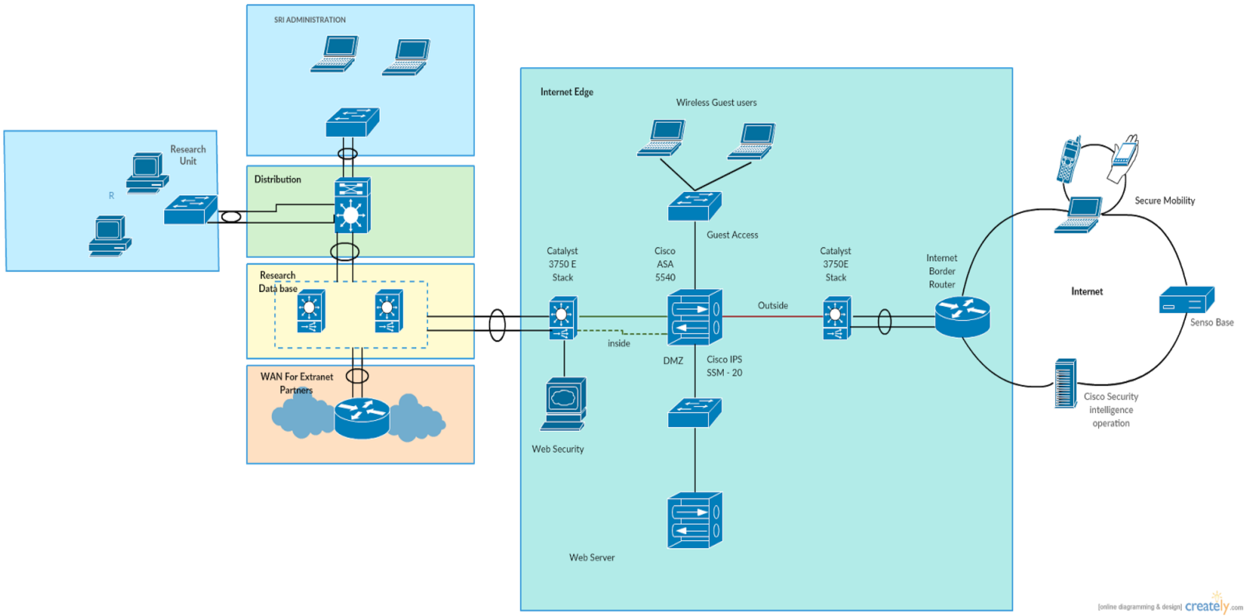


Threat Model of SRI Network

4. SOLUTIONS

As highlighted in our methodology, we intend to draft solutions to the above information security issues discovered within SRI.

The diagram below illustrates our proposed solution



Overview of proposed Network setup

4.1. **Policies**

For the Information Security policies, we would draft policies that are in line with international best practices.

4.1.1. Password Policy

Password complexity would be included. The minimum password length would stay the same for 8 characters long. However, for the research unit, the minimum password length would be increased to 12 with a combination of lowercase, uppercase, numbers, and special characters. Password age would also be enforced throughout SRI. And that password reset request would be done over a secured VPN connection and over the counter. Account lockout policy would also be enforced to prevent brute force attacks.

4.1.2. Standard Compliance

Our plan is to comply with The State Information Technology Security Policy and Standards (SITSPS) of Maryland. We would also comply with the HIPSA ACT to ensure that data collected from health sectors so as to ensure individuals' privacy is protected and not disclosed. FISA Act would also be considered.

4.1.3. Analysis Paralysis

Our drafted policy would also avoid including the tedious bureaucratic process that could hamper progress whilst not being negligent of potential security risk. IT engineers would be given some level of freedom so as to promptly act to address any imminent threat without any prior approval from management.

4.2. Physical Premises

We plan to deploy additional surveillance cameras at strategic points especially to the server room, research unit, and the IT unit. Another one will be deployed at the Administration unit as well. This measure is intended to keep an eye on the activities that take place in these rooms.

4.3. Access Control

We intend to protect Research data by introducing Mandatory Access Control so that employees are only able to access what has been assigned to them. This will help curb issues of excessive privileges. We would also couple this with the HRU model so as to avoid making it a static system. Whereby, Access rights (R) can be granted to a set of subjects (S) such that subject (s1) can have access to an object (o1). This would provide some form of flexibility should in case of management redefines data assignment policies.

SRI would get a Role-Based Access Control Model that will define who does what under what privileges. In the interest of protecting all assets we would first draw up a work plan to help us achieve our goal in the short, but most effective possible time.

4.4. Human Resource Capacity

4.4.1. General employees

We intend to conduct user awareness training for SRI employees in order raise awareness of Information security threats and also acquainting them how to protect themselves.

4.4.2. IT Employees

Training for IT employees would be conducted through professional certifications and secondment assignments to cyber security industries. This would be very useful to help them learn about real word industrial best practice.

Under the budget allocated for this assignment, an extra employee is required. Mainly, a Network Security Administrator. Requirements for this role would involve: at least 5 years' experience working for a Cybersecurity company, certifications in acquired in CISSP, CEHv9, C, C++, and other familiar languages. Network certifications would also be required such as CCNA RS, CCNP RS, and CCNA & CCNP Security. At least a Bachelor's degree in Computer Science, Information Security or equivalent. The user should have familiar experience working with Windows and Linux systems.

4.5. Applications

4.5.1. Antiviruses

Corporate antivirus software would be procured and installed on all new systems including servers. This ensures computers are protected with the most up to date implementations.

4.5.2. SSL certificates

We would procure Enterprise SSL certificates from recognized Certification Authorities (like VeriSign, DigiCert, etc.).This ensures that networks are encrypted and the sensitive data being passed across the network cannot be accessed by external entities.

4.5.3. Operating Systems

All operating Systems would be upgraded after procuring new hardware. Licenses for existing software will also be upgraded. Including those of Database software.

4.5.4. Intrusion Detection and Preventions Systems

Intrusion Detection and Prevention applications would be procured to detect and respond to attacks.

4.5.5. Proxy Servers

Application level proxies would also be used to do some content filtering for internal users.

4.5.6. AAA

Authentication Authorization and Accounting would be enforced in all services mainly using 801.2x standards - relying mostly on RADIUS authentication.

4.5.7. Closing Unused Ports

All service or open ports on systems which are not used would be closed. And those that are not secure would be abandoned and their secure version used. FTP, HTTP, TELNET, would be disabled. HTTPS, SSH, SFTP would be introduced. This prevents remote access to the company's system by attackers.

4.5.8. Port Security

We would also configure port security on VLAN switches to prevent CAM table attacks, MAC address spoofing etc.

4.6. Hardware Systems

4.6.1. Servers

All computer hardware systems would be replaced and modern ones introduced. We would disintegrate server roles to multiple computers to load balance and also to prevent a single point of failure. This would entail separating the web server from the production server, where we have our Research database. We would also separate the Oracle HCM and placed it on a different server accessible internally. However, due to budget limitations, we would allow the Oracle HCM to be on the same server as the active directory. We would install Linux on one of the newly procured servers to act as our DNS. The Web server (also on Linux) would be positioned in a DMZ, making it separate from the internal network. It will also be hardened to make it difficult for hackers to crack.

4.6.2. Firewall systems

We would procure Stateful packet filter firewalls as opposed to stateless. We intend to place one of these firewalls at the perimeter network and one between the Research database and the outer internal network. The firewall will be configured as a zone-based. Inside, Outside and DMZ zones. This would regulate the content that is allowed within the network so restrictions can be set to avoid harmful access to the system.

4.6.3. Switches

We would introduce network segmentation to segment all units on their own VLANs. The layer 3 switches would come in handy here. However, we would allow VLAN trunking wherever necessary.

4.6.4. Honeypots

We would configure one extra server as a hybrid honeypot in order to learn from common threats target to the institution. The information collected from these systems would be provided to management as a quarterly report. This would help SRI to fix any vulnerability in their systems or even act swiftly to prevent future attacks.

4.6.5. Data center

All Servers, network devices, Intrusion Detection System (IDS), and Intrusion Prevention System (IPS) would be placed in a special dedicated room. Basically, a data center which would only be accessible to authorized personnel. The data center would have a fingerprint biometric access control system fixed to its entry.

4.6.6. Offsite Backup

In order to ensure availability backup is an integral part of information security. That is the reason we are proposing an at least one offsite backup facility or a disaster recovery site in the event SRI faces any unexpected disaster, the backup facility would be used to recover from it. In this, we would recommend a VAULT system that can deal with automated backup through a leased high-speed Fiber connectivity.

4.7. Redundancy for Availability

Also, we intend to use multi-homing technologies to ensure that our web server does not incur connectivity lost.

4.8. Evaluation Frameworks

In other to ensure sustainability of our security implementation, we would propose that SRI hires a third party company to conduct an evaluation using standard evaluation frameworks as the tool to measure progress. The Trusted Computing Standard Evaluation Criteria (TCSEC) (the Orange Book) and the Common Criteria would be utilized quarterly once the project is complete to report to senior management.

5. COST

The cost associated with setting up this proposed design has been divided into four categories. These are

1. Hardware
2. Software
3. Services
4. Maintenance and Contingencies

5.1. Hardware Cost

Item	**Quantity**	**Cost**
2960X cisco switch	3	$2500
2921 Cisco router	1	$1200
Web Server	2	$3500
Fingerprint Biometric scanners	1	$1000
Total		$16,700

5.2. Software Cost

Item	Quantity	Cost
Hybrid honeypot	1	$3500
Cisco WS381 IDS Catalyst 6000	1	$10000
Cisco 4200 series IPS	1	$10000
Windows 10 OS	50	$200
McAfee Antivirus	50	$45
Firewall	2	$10000
Total		$55,750

5.3. Service Cost

Item	Quantity	Cost
Consultancy Services	1	$50000
Evaluation Framework	4	$15000
Network Administrator	1	$80000
User awareness training	187	$1000
Training of Network Admin	1	$5000
Total		$382,000

Grand Total:	**$454,450**
Maintenance cost:	**$45,550**

We have included all the 100 students, 57 faculty members and 30 staff members in the awareness training as, social engineering is one of the biggest vulnerabilities in the world. No matter how many firewalls or how any IDS we install if any single person intentionally or unintentionally compromises data then that is the biggest threat to SRI. The remaining cost we have decided to keep for maintenance in order to foster SRI’s needs and requirement in the near future.

6. PRIORITIES

With the limited budget allocated to this assignment, we intend to prioritize the immediate security needs of SRI. We, therefore, divided this task into two parts, immediate needs (PLAN A) and alternatives (PLAN B). Alternatives will be considered if this proposal is convinced SRI's senior management is adding more budget to this assignment. The alternatives involve all components of PLAN plus PLAN B.

PLAN A	**PLAN B (optional)**
Policy Amendments	Multiple offsite backups
Establishment of a Disaster recovery Site	Virtualization and secure private cloud
Introduction of a Zone-based Firewall	More network administrators
RBAC + HRU Access Control Model	Sandboxing
User Awareness Training	
Network Administrator Recruitment & Training	
Evaluations	
Data Center	
Application Improvement & Security	
Compliance to Standards	

7. CONCLUSION

This network setup ensures that the security of the organization is improved and performance is not affected. The cost spent on prevention is less than the actual cost it would take to fix the issues if there is a security exposure prior to its implementation. Prevention would also increase the overall productivity of the organization.

8. REFERENCES

- https://creately.com/app/?tempID=hp27eh051&login_type=demo#
- http://acronyms.thefreedictionary.com/HIPSA
- https://link.springer.com/chapter/10.1007/11844662_8
- http://doit.maryland.gov/support/pages/securitypolicies.aspx
- https://www.google.com/search?q=cisco+legacy+stateless+packet+filter&source=lnms&tbm=isch&sa=X&ved=0ahUKEwidx7Gq3enTAhXBSCYKHTpUC1gQ_AUIBygC&biw=1600&bih=791#tbm=isch&q=cctv+camera&imgrc=gUNsZ2ogAN-G2M:
- http://www.bigphilcomputers.co.uk/product/dell-optiplex-380-windows-7-professional/
- http://produto.mercadolivre.com.br/MLB-856084781-computador-dell-optiplex-350-_JM#redirectedFromParent
- https://www.cablesandkits.com/cisco-pix-506-vpn-firewall-pix506-p-3805.html