IT Security Controls in Saudi State Universities: A Technical Case Study

Waleed A. Alrodhan and Ali M. Alqarni

College of Computer and Information Sciences Al-Imam Muhammad ibn Saud University

Summery
Information security has gained a significant importance in the higher education sector, in the past few years. This was a result of the rapid reliance on technology and information processing and mining services, along with increase of the information security attacks in both number of incidents and sophistication. There are 27 state universities in the Kingdom of Saudi Arabia, and the bear a great resemblance with regard to their IT equipment. Hence, in order to form a general conception on their information security status, we have selected one of the biggest state universities in the kingdom to conduct a technical study upon. In this paper, we provide an overview of the university IT architecture, infrastructure and security controls. Also, we discuss a security analysis of the university's security status before we propose a number of security enhancements.

Key words:
Security, risk, education, eservices, countermeasures

1. Introduction

In this paper we describe a technical case study of the security systems, processes, procedures and other security controls deployed in one of the biggest Saudi universities. This study aims

to form a general conception of the information security states within the Saudi universities, especially the state ones. There are twenty-seven state universities in the Kingdom of Saudi Arabia[1]. All state universities are funded by the government via the Ministry of Education which monitors their academic and operation activities. Hence, there is an evident resemblance in their infrastructures, facilities, and operation hierarchies. Therefore, studying the security controls used by one of them on ground while adhering to using scientific methodologies would help in understanding their general information security status. As mentioned above, we have selected one of the biggest university in the Kingdom of Saudi Arabia to conduct our study upon; however, for confidentiality reasons, we refrain from identifying the selected university. The selected university is a state university that was founded in middle of the twentieth century; it includes twelve colleges held in a number of branches in different cities. It has more than 13000 employees in addition to its 3500 academic staff members. The university's in-campus students are more than 60,000 students; also, there are a big number of distance-learning students. Finally, the studied university's IT administration unit (or the IT Deanship) has more than 120 employees working in ten departments. the departments are:

- Information Security Department.
- Project Management Department.
- Network and Internet Department.
- Service Desk Department.
- Application Department.
- Operations and System Department.
- IT Risk Department.
- Quality Assurance Department.
- Web Portal Department.
- Public Relation Department.

The Figure 1 shows the IT deanship management structure and hierarchies:

[1] https://www.moe.gov.sa/en/HigherEducation/government highereducation/StateUniversities/

Manuscript received March 5, 2018
Manuscript revised March 20, 2018

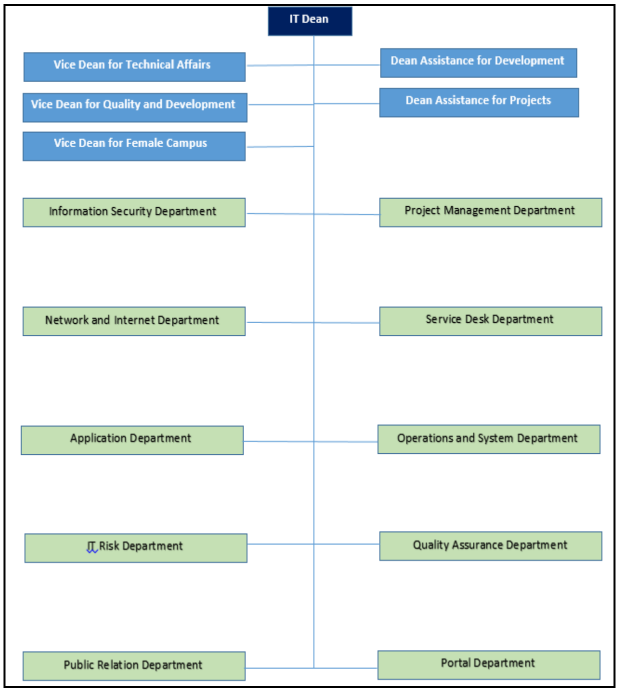
IT Dean
Vice Dean for Technical Affairs
Dean Assistance for Development
Vice Dean for Quality and Development
Dean Assistance for Projects
Vice Dean for Female Campus
Information Security Department
Project Management Department
Network and Internet Department
Service Desk Department
Application Department
Operations and System Department
IT Risk Department
Quality Assurance Department
Public Relation Department
Portal Department

Fig. 1 IT deanship management structure and hierarchies

Our study could readily be projected on other state universities, and the security enhancements proposed in this paper could be helpful for all of them. Our study covers many parts, such as:

- Analysis of the organizational IT architecture including the information systems and solutions with regard to the IT assets, human resources, the relationship between IT and business, the IT network, and the operating environment.
- Identifying security threats and controls.
- Evaluating the existing security controls and their efficiency.
- Linking the identified risk.
- Proposing a number of security enhancements.

The remaining of this paper is divided as follows. In Section 2 we discuss our analysis of the selected university IT architecture. We describe our findings with regard to the university's non-functional security in Section3, before spot the light on the university's security threats and controls in Section 4. In Section 5 we discuss out security analysis, and then we propose a number of security enhancements in Section 6. Section 7 concludes the paper with brief concluding remarks.

1. IT Architecture Analysis

This section we provide and analysis of the university's IT architecture. This analysis focuses on three main parts; the IT resources, the IT network design, and the operating environment.

1.1 IT resources

By IT resources we mainly refer to the IT assets (software and hardware), the IT human resources (employees and contractors), and the relationship between IT and business (the business in our case is providing higher education services).

1.1.1 IT assets

Due to the emerging global demand for innovative, efficient, and smart educational services, most of well-funded universities possess massive IT assets in order to accommodate the educational requirements. Our selected university's IT assets are described below.

According to [1], the university has provided solutions for the growing demands in computer studies by virtualizing its labs to facilitate efficient education systems. The university has moved from the traditional setup of labs which were costly to the Vblock system. The Vblock system supports *Virtual Desktop Infrastructure* (VDI) [2]. Thus, it provides easy access to digital learning resources around-the-clock. Implementation of the system has led to improvement in computing flexibility and scalability. The system facilitates easy and quick expansion of labs; hence, it reduces administration efforts and cost whilst improving the provided education services.

A publication by [3] explains how the university was able to provide better solutions and cut cost by adopting IT virtualization. According to Microsoft, the university was able to implement its virtual platform by using Hyper-V on Microsoft Windows Server 2012 R2. The university has replaced VMware with Hyper-V, which reduced licensing cost. The IT Deanship was able to provide a consistent level of service through the implementation of the virtual platform.

According to [1], the university has solved its business challenges by using EMC VNX to support its storage systems. There was a need for a unified storage solution to enable successful VDI. In order to provide that, the university has chosen VCE Vblock, EMC, and VNX unified storage. It uses EMC Unisphere to manage its storage infrastructure.

The software and hardware resources of IT deanship which providing the IT services to university are listed in Table 1.

Table 1: Hardware and software resource

#	Resource	Type
1	**Cisco and Juniper Network**	**Network and Security Solutions**
2	**VBlock System**	**Computing Environment**
3	**Sun Solaris Operating System**	**Operating System**
4	**Windows 2012 Operating System**	**Operating System**
5	**VMware Virtual Environment**	**Virtual Environment**
6	**SQL Database**	**Database**
7	**Oracle SuperCluster**	**Computing Environment**
8	**Web Applications**	**Applications**

1.1.2 IT Human Resources

The IT Deanship employs 120 employees within ten departments; some of them contain a number of sections. The dean, the vice dean for technical affairs, the vice dean for quality and development, and the vice dean for female campus affairs, all hold Ph.D. degrees in a computer related disciplines. Also, there are twenty-four IT engineers and specialists in the deanship, along with sixty-five technicians who are certified to carry out technical tasks like for example: network support, IP telephony support, and helpdesk operation. Finally, there are thirty-nine employees dedicated for non-IT jobs such as coordination and management.

1.1.3 Relationship between IT and Business

In order to establish a healthy relationship between IT and business, an evident communication policy must be set up between the IT Deanship and every other unit in the university. Optimal arrangements would avoid any unacceptable risk (e.g. information leakage, tampering with the university's data used in automated systems, etc.). The relationship between IT and business should be shaped in *supplier-customer* form with appropriate expectations to outsourced IT [4]. With regard to information security, services like for example: maintaining confidentiality, availability, integrity, reliability, and accountability [5], must be conducted efficiently and precisely. In the studied university, some information security tasks are outsourced, and for that the university strives to keep in touch with the partners in that form of relationships. An alternative form of relationships would involve *information mediators* who are the business and IT personnel, or incorporated IT activities, used to fulfill corporate IT functions [4]. They provide efficient competent dialogue between the needs and peculiarities of the business and the matching hardware and software capabilities of IT.

A healthy relationship between IT and business would result in a complete and accurate data and information processing. Accessibility is important when referring to the database as it is needed for the authorized users.

1.2 The Network

The university's network follows the common segmentation. The network segments are:

- **Servers segment**: contains the university's servers (high security zone).
- **Users segment**: contains users' PC and laptops.
- **WAN segment**: connects the university's branches.
- **Demilitarized Zone (DMZ)**: contains external servers that provide services over the internet.
- **Internet segment**: for Internet users (low security zone).

Figure 2 shows the university's network design.

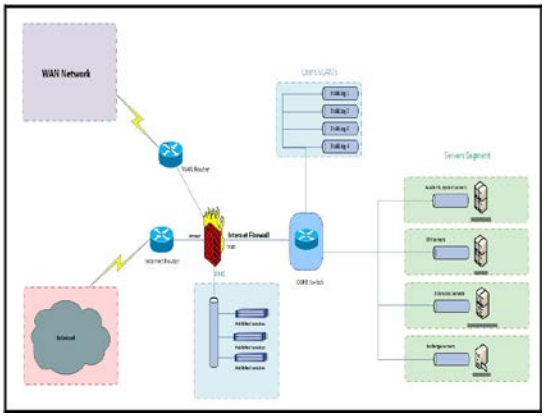

Fig. 2 The university's network design

1.3 The Operation Environment

In this section we provide a brief description of the adopted software and hardware systems and appliances.

1.3.1 Cisco and Juniper Network

Within the university, the main network appliances are Cisco and Juniper devices and systems which resulted in two networks a Cisco one and a Juniper one. Each network has its own specifications and designs. Hence, it is vital to have a comprehensive understanding of the network appliances and their features [6].

Routers and switches within each network work hand in hand to connect the heterogeneous devices and facilitate the data flow amongst them. In order to achieve that and to meet the user requirements, customized configurations of each network have been setup; for example, the university has setup customized configuration to provide security services via Juniper's SRX series [7].

With regard to the networks' designs and topologies, the core routers and edge routers should complement the entire networking process to enhance reliability, effectiveness, and efficiency. Juniper network has proven to be sufficiently fast and reliable. Cisco provides the same level-of-service but at a higher price point. The designs are scalable and modern as they follow the standards and criteria set by the contemporary market [6].

1.3.2 VBlock System

The university has deployed a VBlock system[2]. VBlock Systems from VCE is a powerful computational solution that facilitates a flexible and scalable hyper-converged infrastructure aimed at supporting sophisticated educational solutions (e.g. virtual laboratories) [1]. Users can access files in the memory of different devices that an organization is using. This feature utilizes some of the components used in cloud computing. This raises a number of security issues that should be addressed. Figure 3 shows the VBlock Racks in the university.

Fig. 3 VBlock racks in the university

1.3.3 Oracle SuperCluster

In the selected university, a good number of core applications are running on a Sun Solaris operating system[3]. The chosen hardware to hold this operating system is Oracle's SuperCluster[4]. SuperCluster refers to a secure enterprise cloud infrastructure designed for Oracle Database and application combination [8]. Oracle SuperCluster merges computer storage hardware and networking with virtualization, management software, and operating system into a full, high functioning cloud infrastructure that is very easy to set up, secure, run and maintain [8]. With its ability to incorporate a big number of processors and its distinct features like for example in-memory databases and applications, the SuperCluster has a significant importance in the IT Deanship. Figure 4 shows the Oracle SuperCluster Racks in the university.

Fig. 4 The Oracle SuperCluster Racks in the university

1.3.4 Sun Solaris Operating System

Sun Solaris Operating System is known for its ability to reliably scale multiprocessors, which is an essential requirement for many educational services provided by the university.

It is highly versatile and efficient. One important feature of Sun Solaris is that it is built upon the concept of Solaris Zones [9]. The zones are the isolation points of the Solaris operating system that aim to separate resource controls. In addition to its security benefits, this concept reduces administration costs. Moreover, it can handle voluptuous files. Using ZFS feature, it combines a range of file systems on top of harboring the capability to execute logical volume file management. Also, the ZFS allows JBOD and HBA configuration through a connection to the RAID controllers. Solaris containers offer high

[2] https://www.cisco.com/c/en/us/solutions/data-center-virtualization/vblock-systems

[3] https://www.oracle.com/solaris/solaris11

[4] https://www.oracle.com/engineered-systems/supercluster

virtualization performance, complete consolidation, isolation, and protection of application through individual servers.

1.3.5 Windows 2012 Operating System

The majority of servers deployed in the university's network have Windows Server 2012, which is an improvement of the Windows server 2008 with a number of good enhancements especially with regard to multi-server support, storage, virtualization and user-experience [3].

1.3.6 VMware Virtual Environment

Virtualization has become one of the most important and progressive trends in the IT sphere. In the university; VMware was picked to facilitate a virtual environment for windows servers (Windows 2012 R2). Although it is somewhat an emerging concept (it has been introduced a decade ago), virtualization has gained a huge acceptance in industry [2]. It has evidently helped reducing cost and boosting up performance in the same time.

Virtualization referrers to technologies “designed to provide a layer of abstraction between computer hardware system and the software running on them” [10]. One of virtualization services is *server virtualization* which allows running all operations on a single physical server boosting the efficiency of using resources. Another service is *network virtualization* which presupposes a reproduction of a physical network in software; application in virtual networks act in the same way as in physical networks. Virtualization also support *Software-defined storage* which virtualize the storage environment for users for both storing and retrieving in order to enhance performance and security. Finally, virtualization provides *desktop virtualization* service that virtualize personal computers for user over the network. There are several product lines offered by VMware for desktop virtualization; the university uses vRealize Suite[5].

1.3.7 Web Applications

In the university, many IT services built for users (students, employees and visitors) are offered via web applications. Examples of applications include LMS, webmail, online auctions, and instant messaging services, and many more. These applications were developed using a number of programming languages; yet the vast majority of them are built upon JavaScript and Hyper Text Markup Language (HTML). HTML5 is used in order to eliminated the need for client-side plug-ins and to enable developers to create better graphics and other multimedia capabilities on the webpages as along with improving the webpages semantic content.

1.3.8 SQL Database

One of the most common databases are relational databases, that use the Structured Query Language (SQL). In the university, the SQL Server (a database management systems developed by Microsoft) is used. Typically, the development and compilation of the data in a relational database take place in a relational manner [11]. Hence, it operates like a spreadsheet.

2. Non-functional Security

This section we describe the non-functional security procedures and concepts that are adopted by the selected university. Generally, our findings in this matter are positive. The efforts made by all of the IT Deanship departments has collaborated and cooperated to successfully reach a good level of non-functional security.

2.1 Security Awareness

Promoting a solid information security culture has become an integral part of information security management. Users are always the weakest link in the security chain, and hence they must be properly trained and cultured with regard to information security. To maintain a high standard of security in university, it needs to establish an awareness of security practices amongst its users. This will help users to use the system as per expectations and in accordance with the security policies and the adopted standard security practices.

In the IT Deanship, within the information security department, there is a dedicated security awareness team. This team has commenced an information security awareness program that targets the university faculty, students and employees. Also, it has deployed a bi-lingual (Arabic and English) online security awareness training course via the web. In order to pass the course, the user has to watch clips on ten different security topics, and pass an online exam on each topic. The user must watch the whole clip before she can take the exam. The user who successfully pass the exam will be given a certificate. The ten topics are: privacy, e-banking, security, social networking, malicious programs, network security, identity theft, email security, social engineering, data backup, physical security, Internet security, and passwords.

[5] https://www.vmware.com/uk/products/vrealize-suite.html

Also, the university uses other awareness channels, like for example posters, kiosks, emails, SMS, and roll-up posters. Finally, the university has a per-defined technical training program for all IT personnel.

2.2 Performance Requirements

There are a number of performance requirements for each e-service provided by the university. Benchmarks, reports, KPIs, and other measures are required by several parties like for example the ministry of education, the e-government program (known as Yesser), and the university itself. Below, we discuss some of the areas that are bound with performance requirements.

2.2.1 User Interface

All published e-services have to be user friendly with a *graphical user interface* (GUI). This interface ensures better usability, security, and efficiency [12].

2.2.2 Hardware Interface

This interface describes the logical and physical characteristics of each interaction between the hardware components of the system and the software products. It usually includes the nature of the data, the supported device types and control interactions between the hardware and software and also the communication protocols to be used [12].

2.2.3 Software Interface

The interface is used by the IT manager to describe the interactions between the product and other specific software components such as operating systems, databases, tools, integrated commercial components, and libraries. It helps in the identification of the inbound and outbound data items and the messages into and from the system while describing the purpose of each message. Also, it describes the nature of the communication [13].

2.2.4 Communication Interface

This interface helps the IT Deanship staff to be associated with any communication functions that are required by the product, and it includes web browser, e-mail, electronic forms and network server communication protocols. It defines any pertinent message formatting while identifying the used communication protocol (e.g. HTTP, FTP, etc.). It helps in specifying the encryption parameters, communication security methods, synchronization mechanisms and data transfer [13]. Figure 5 shows a screenshot of the university's performance dashboard.

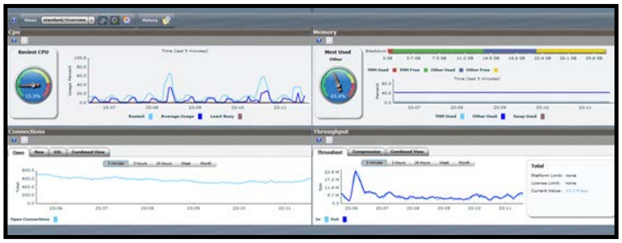

Fig. 5 Performance dashboard in university

2.3 Safety Requirements

Safety controls are set up to safeguard institution's resources from various hazards. Typically, every employee or a student in the university has to adhere to the relevant procedures and standards. One of the safety requirements is to ensure that the staff members have the authority to access and use a specific university resource. Another requirement is that all staff members should maintain the highest level of professionalism whilst handling or using resources and materials. They should not share any information that may lead to damages or harm to the institution.

Moreover, the university has embraced safety policies and guidelines that meet the ISO/IEC 27001 standard. Moreover, the university has invested in physical security and safety systems, for example it has deployed sophisticated fire alarm and firefighting systems that cover the entire building.

2.4 Software Quality Attributes

When new applications appear on daily basis, maintaining quality levels would not be a straightforward task. In the IT Deanship; there is a quality assurance department in charge of assessing the quality of the newly released applications and services before they can be published. Quality check is a vital step in the software development process.

Usually, software products are designed for commercial purposes with precise set of quality levels; however, in the university, in-house developed software products are not commercial and assessing their quality, even in the shadow of relevant standards, can be quite tricky. Yet, conducting the system integration quality assurance tests could help. The main quality assurance tests are *System Integration Test* (SIT) and *User Acceptance Test* (UAT). these two tests involve the following sub-tests:

- Business function test.

- Hosting and environment test.
- Information security test.
- Network and access test.
- User interface test.
- Integration and architecture test.
- Technical support test.

More information about the abovementioned tests can be found in [14].

3. Security threats and Controls

In the first part of this section we will identify the security threats within the selected university, and in the second one we will list its implemented security controls.

3.1 Security Threats

A security threat is an undesirable negative impact on one or more IT assets. This impact would affect the confidentiality, integrity, and/or availability of the IT assets; and its harm depends on the severity of the attacks that could realize it [15]. Attacks exploit security vulnerabilities in order to realize threats. IT assets are hardware, software, data, and reputation [15]. In our case, there are security threats related to the systems, networks, applications, physical appliances.

3.1.1 Networks Threats

One of biggest IT security threats to an organization is stealing their data in transfer. Another threat would be sending malicious content using the network to damage other assets, or even controlling the network itself.

In the university, the Juniper network experienced a security breach when its screen operating system was corrupted. Attacker could use this breach to gain access to classified or private information. Notably, the Juniper confirmed this existence of this vulnerability and issued security patches for it [7]. Another observed threat is the absence of segmentation in the network level, which means that the test and development environment is not segregated from the production environment.

One threat that has been observed that some systems are using *telnet* protocol for administration sessions and *FTP* for file transfer; these two protocols are not encrypted and convey plaintext content. This raises a number of security risks (e.g. an attacker can sniff the transmitted aiming to detect the security credentials and/or other traffic contents). Finally, there is no defense in the depth and many ports are opened even not be used in the business.

3.1.2 Server Threats

There always a threat of systems being hacked by malicious attackers. Due to the univeristy's deployment of virtual computing, the VBlock system is vulnerable to malicious internal users. They might try to access classified data or inject malicious software (e.g. spyware) to the system elements. Computer viruses are a real concern for all the programs that utilize the virtual network [16].

With regard to the Oracle SuperCluster, if its *Integrated Lights Out Manager* was hacked, the attacker can easily change the root password, install new software, shutdown the system, and perform more critical actions. In the university, the Ethernet switch that links to Integrated Lights Out Manager ports is accessible only through telnet; yet this is not sufficient [17]. Therefore, the management port should not at any time be attached to the management network. In the case network access is required, an access to the system via the firewall should be configured to use SSH. The Oracle SuperCluster can be potentially attacked in case intrusion prevention systems are not used to monitor network traffic flow to and from the system [8]. The absence of such systems allows unauthorized access attempts. Network protocols with strong authentication and encryption can reduce the risk of the system being hacked. Finally, the Oracle SuperCluster system usually have default administrative passwords. These passwords must be changed and kept safe merely with the system administrators.

3.1.3 Operating Systems Threats

According to our observations, there are some Windows servers that have not joined the domain controller, these servers have local administrator accounts and many of them do not have antimalware appliances. It is vital that all Windows servers join the university domain controller in order to enforce the servers group policy and unify the administration controls. The Sun Solaris operating system is at risk of external attacks, as well.

3.1.4 VMware Virtual Environment Threats

Since VMware relies heavily on the hypervisor, this hypervisor must be properly protected. Processes run at the hypervisor layer are not limited to major object types, but can go beyond them. Consequently, it is easy to lose track and control of such processes. Hence, virtualization presupposes server consolidation, attacking a single physical host will provide the attacker with access to information from various virtual servers. VMware identified several serious security issues within its product lines. The first one is an issue with RPC commands with which a guest can crash VMX processes or gain access to the host. The second risk is the ability to use NFC traffic to overwrite memory, allowing unauthorized code execution.

3.1.5 SQL Database Threats

Some of the features and services provided by the database network expand the attack surface. Moreover, if the *sysadmin* is highly exposed, for example if several people have access to the same account, there will be a higher risk of security breaches. Therefore, it is important to have very few people with access to the *sysadmin* account. Thus, it is quite important to ensure the policy of minimum privilege for all users.

Another security threat is the SQL injection attack, which is a common security threat to databases. The attack launched by injecting unauthorized code into the SQL database. This code interferes with the operation of the database by allowing intruders to gain unauthorized access to it. Also, there is a security threat with regard to the SQL database authentication process; one-factor authentication is used which is, by all means, not sufficient.

3.1.6 Web Applications Threats

We have observed a number of security threats that are associated to the deployed web applications. Below, we list them.

- **Cross-Site Request Forgery (CSRF)**. Cross-Site Request Forgery (CSRF) is a web application vulnerability that can be exploited by an attacker to force the user to take an action in the application. Any request to an application will include the user's session cookies, regardless of whether that request was generated by a legit user activity or by malicious code on another website. If an application is not able to differentiate a legit user activity from a forged one, the application is vulnerable to CSRF, and an attacker could surreptitiously force a user to make changes in the application.

- **Non-scanned uploaded content**. We have observed that uploaded content may not be scanned by the antivirus. Moreover, in some cases, it is not clear whether or not the upload was successful. Content filtering that is performed based on file extension (or type) is always applied; however, content scanning remains vital.

- **SSLv3 Padding Oracle on Downgraded Legacy Encryption (POODLE) vulnerability**. The affected system accepted connections using Secure Sockets Layer (SSL) version 3.0, which suffers from a cryptographic flaw (CVE-2014-3566, known as “POODLE”) when using cipher block chaining (CBC) mode ciphers. An attacker could exploit this vulnerability to compromise transmitted information over secure channels.

- **Enabling Apache multi-views**. We have observed that Apache multi-views were enabled. This could be exploited by an attacker to disclose hidden file processes on the directory and/or gain access to sensitive information.

- **Link-injection vulnerability**. Link-injection is a technique by which an attacker could tamper with the content of the targeted website by embedding in it a URL, or to a script within the vulnerable website. Also, an attacker could exploit this vulnerability to conquer the targeted website and use it as a platform to launch attacks against other websites.

- **Exposed FrontPage extensions**. Improper permissions (and ACLs) were set to many files and directories. This resulted in many exposed FrontPage extensions. Also, we have observed that the Microsoft FrontPage server extensions associated with several files were set with improper permissions. Some of these files contain vital information such as usernames and passwords. For example, we found that the robots.tx file discloses the path to the web services [18].

- **Exposed web services**. A number of unauthenticated web services testers were found. This includes a file listing out the names and locations of all of SharePoint's web service endpoints [18].

- **Absence of CCTV monitoring for an Intermediate Distribution Frame (IDF)**. An IDF is a distribution frame located in the main university building. It cross-connects the user cable to the *main distribution frame* (MDF). We have found out that one of the IDF rooms was not covered by the CCTV monitoring system. Figure 5 shows the abovementioned IDF.

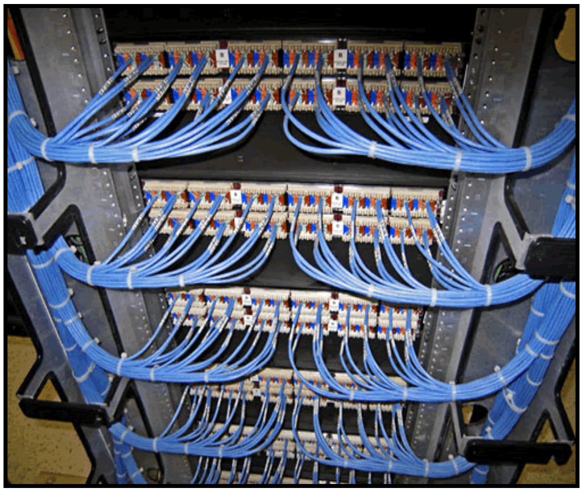

Fig. 6 An IDF within the university's main building

3.2 Security Controls

Security controls can be administrative, technical, or physical. These controls are safeguards or counter-measures that are deployed to mitigate the risk of an attack realizing a threat by exploiting a security unavailability [15]. Security controls preventative, detective, corrective, deterrent and/or compensatory. Lack of effective security controls would result in security holes that could be exploited to penetrate the network [19]. The selected university has set up several security controls aiming to protect its IT. Examples of these controls include security policies, CCTV's, firewalls, antiviruses, antispam appliances, malware detectors, intrusion prevention systems (IPS's), and few more. Below, we briefly describe some of these security controls.

3.2.1 Information security policies

The information security department within the IT Deanship has set up many information security policies. All of the university's users (faculty, students, employees, are contractors) are obliged to adhere to these policies. Information security policies are administrative security controls. Table 2 lists the all of the IT Deanship information security policies.

Table 2: IT Deanship information security policies.

Code of ethics and acceptable usage (with Arabic translation)	**Antivirus**	**Asset management**	**Backup and recovery**
Business continuity management	**Change management**	**Code of ethics & acceptable usage**	**Compliance**
Cryptography & encryption	**Data privacy**	**Database security**	**Document control**
Email security	**HR & personnel security**	**Incident management**	**Internal audit**
Internet access & security	**Laptop & desktop security**	**Logical access control**	**Network security**
Operating system security	**Password security**	**Physical and environmental control**	**Remote access**
System development & maintenance	**Third party security**	**Wireless security**	-

3.2.2 Security Firewalls

The university has deployed packet-filtering firewalls that protect the university's network from the Internet malicious content. A *packet-filtering firewall* monitors both inbound and outbound data packets [20]. Each data packet is analyzed against an *access control list* (ACL), and depending whether or not it conveys malicious content, it either gets discarded or forwarded. It is mandated in the university that if there is not a rule that matches a certain packet, the default action is to discard it.

3.2.3 Antiviruses

Another security control that aims to discover and eliminate viruses is antiviruses. Every PC, laptop and server that belong to the university has a host-based antivirus installed in it. However, some users want to use their own devices (e.g. laptops or mobile phones) to connect to the university’s network or access the university's Internet service. Although that this should be allowed for business reasons, it jeopardizes that the whole system since a malware, for example, could be uploaded into the network through these devices. Therefore, a network-based Antivirus has been installed scan the whole network traffic for viruses [19].

3.2.4 Antispam Appliances

Thousands of spam emails are sent daily to the email users that are irritating and irrelevant. Moreover, some of these emails might have malware attached to them [21]. An antispam appliance is therefore installed in the university to eliminate spam emails. The antispam examines all received emails consulting a set of predefined rules in order to determine whether or not the received email has been sent by a genuine source. The antispam is located in the DMZ network facing the Internet so it can receive the SMTP traffic.

3.2.5 Intrusion Prevention System (IPS)

This security control helps preventing intruder from illegally gain access to the university's network [22]. It detects intrusion events based on an attack signature scheme. The process of malicious activity detection involves a comparison between that activity’s pattern and a set of predefined attack patterns. Suspicious activities are blocked. The IPS reports every malicious activity and logs it. The IPS is installed right behind the Internet firewall so that only passed traffic gets inspected by the IPS.

3.2.6 CCTV

The university pays a good attention to its physical security. A state-of-art access control system and monitoring system (CCTV) has been installed. It covers the critical IT areas such as data center, main distribution frame (MDF) and majority of intermediate distribution frame (IDF). Fire alarming and fighting systems along with public address tools are properly implemented.

3.3 Adequacy of the Existing Security Controls

In this section we briefly introduce our findings on the adequacy of the security controls deployed in the university. Stating that a specific security control is adequate to address a specific security threat does not necessarily mean that the risk of that threat has been fully waived. For the purpose of this paper, we merely provide a mapping between the security threats and the security controls without further details on their efficiency nor practicality. Table 2 shows a matrix that maps the security threats with the security controls by indicating their adequacy and practicality vis-à-vis addressing each identified security threat.

4. Security Analysis

In this section we discuss the selected university's IT risk before we analyze the current security countermeasures and evaluate them using the ISO/IEC 27001 standard.

4.1 Risk Identification

As we have shown in Section 3, there are a number of serious security threats associated to almost all kinds of IT assets. Hence, there is a security risk of these threats being realized by an attacker. For example, the university could suffer from denial of service (or DoS) if some of network threats got realized via a successful attack. Disclosure of classified information is another risk the university should mitigate. Also, Financial losses or reputation damage are risks that are bound to many attacks. OS security threats lead to serious security risks since that the operating systems are the backbone of almost all computing systems. Risks associated to databases, storage, web application, and all other assets should be properly identified and managed.

There a number of security risks associated with the university-provided IT services. Services provided by the IT Deanship can be divided into three categories:

- Academic services; like for example:
    - The academic registration services provided by the Banner by Ellucian[6] system.
    - The learning management services provided by Blackboard[7].
- Communication and business services; like for example:
    - The e-mail services.
    - The E-litters services provided by Etisalat (a proprietary system).
    - Councils meetings management system.
- Infrastructure services; like for example:
    - Hosting and storage services.
    - VPN access.

[6] https://www.ellucian.com/student-information-system

[7] http://www.blackboard.com

Table 3: Existing security controls and their adequacy

#	Security Threats	Firewall	Antivirus	Antispam	Intrusion Prevention System (IPS)	CCTV	Information security policies
1	Network Threats	√			√		
2	Server Threats (VBlock)		√		√		
3	Server Threats (Oracle SuperCluster)	√			√		
4	OS Threats (Sun Solaris)	√			√		
5	OS Threats (Windows 2012)		√		√		
6	VMware Virtual Environment Threats	√	√		√		
7	SQL Databases Threats	√			√		
9	Web Application Threats (CSRF)	√			√		
10	Web Application Threats (Non-scanned uploaded content)	√			√		
11	Web Application Threats (SSLv3 POODLE)	√			√		
12	Web Application Threats (Enabling Apache multi-views)	√	√				
13	Web Application Threats (Link Injection)	√			√		
14	Web Application Threats (Exposed FrontPage Extensions)	√			√		
15	Web Application Threats (Exposed Web Services)	√			√		
16	Web Application Threats (Absence of CCTV monitoring for IDF)					√	

These services are posed by many security risks with regard to their confidentiality, integrity and availability. Examples of IT services risks include: DoS, unauthorized alteration of students' academic records, disclosure of sensitive information, failure to comply with the government and international requirements, physical damages of servers and other IT appliances, and many more.

4.2 Risk Assessment using CRAMM

In order to assess the security risk that poses the university, we have manually conducted a risk analysis project using a well-known risk assessment method named CRAMM [8] (CCTA Risk Analysis and Management Method). CRAMM is a risk analysis and management methodology that was first introduced in 1987 by the Central Computer and Telecommunications Agency (CCTA), now renamed into Cabinet Office of the United Kingdom government [23]. CRAMM is currently on its fifth version, and it is built on three stages:

1. *Asset identification and valuation*. Table 4 shows our findings at this stage.

2. *Threat and vulnerability assessment*. This is conducted by building a matrix giving mapping each asset to the likelihood of it being affected by realizing its associate threats with regard to confidentiality, integrity, and availability. Also, the matrix maps each asset to its value. A score from 0 to 4 is used in the first mapping (none (0), low (1), moderate (2), high (3), and very high (4)), and four-level qualitative score is used in the second mapping (low, medium, high, and very high). Table 5 shows our findings at this stage.

3. *Countermeasure selection and recommendation*. In this stage we identify the recommended countermeasure and to identify the changes required

[8] https://managementmania.com/en/cramm-ccta-risk-analysis-and-management-method

to manage the CIA risks identified in the previous stages. We have proposed five main enhancements that should help mitigating the opposing risks:

- Combating Advanced Persistent Threats (APTs).
- CCTV Surveillance.
- Second layer of Intrusion Prevention Systems (IPS).
- Configuration and access right review for network security solutions.
- Virtual environment hypervisor security.

These proposed enhancements will be discussed in further detail in Section 5 below.

Table 4: Assets register

Asset Type : Asset Group : Asset List	Units
1 Company Image & Reputation	
Banners / Letterheads / Logos / Rubber Stamps / Seals	
Blank Letterheads	Variable
ID-Cards	Variable
Logos	1
Signature Rubber Stamps	Variable
Rubber Stamps/Seals	Variable
2 Information Assets	
Configuration Files	
Oracle Database	4
SQL Server	4
Oracle ASM	1
Storage Config	2
Server Config	14
OS Config	14
Core Switch	2
Router	2
Firewall	2
Network Switches	170
Vulnerability Manager	1
IPS	1
VPN	1
Endpoint Security	1
Source Code	
Application Source Code	3
Manuals / Diagrams	
Video Conference Manual	Variable
Electrical Diagrams	1
Work Place Floor Diagrams	1
Training Manuals	Variable
Operational Documents	
Anti Virus Procedures	1
IPS Procedures	1
Firewall Procedure	1
VPN Procedure	1
Vulnerability Manager Procedure	1
Router Procedure	1
Active Directory User Creation/ Modification/ Deletion	1
Data Center Access Request	1
Network/ Internet Access	1
Systems Vulnerability Assessment Request	1
Websites Vulnerability Assessment Request	1
Blocking Spam Emails	1
Update/ Modify IPS	1
Information Security Incident Reporting	1
Infosec Awareness Program Request	1
Legal Documents	
Signed NDAs	Variable
Vendor Contracts	Variable
Databases	
Sql Server Database	3
Standards / Agreements / Proposals	
RFP (Before Floating)	Variable
RFP (After Floating)	Variable
Non Disclosure Agreements	Variable
Proposals Against RFP	Variable
Vendor Contracts / Invoices	
Vendor Contracts	Variable
4 People Assets	
Managers / Executives	
Dean of IT deanship	1
Vice dean of IT deanship for Quality and development	1
Vice dean of IT deanship for technical affairs	1
Departments Manager	9
Employees	
Network Administrator	2
System Administrator	2
Developer	1
Information Security Engineer	1
Database Administrator	1
5 Physical Assets	
Access Control System	
Biometric Access Control	1

Surveillance System	
CCTV	**4**
Building Infrastructure	
Data Centre	**1**
Manager rooms	**5**
Administrator Rooms	**4**
Meeting Rooms	**1**
Power supply room	**1**
Vice Dean's Room	**1**
Desktops	
Desktops	**8**
Fire Fighting Sytem	
Smoke Detector	**10**
Fire Extinguishers: Hand held	**8**
Fire Alarms	**5**
Fire Hydrant Pump	**4**
Servers	
Proxy Servers	**3**
DHCP Server	**1**
Syslog	**1**
Windows Physical Servers	**35**
Physical Servers – Linux	**5**
Intel Rack (HP & Dell)	**10**
Storage Devices	
Storage Box	**6**
6 Service Assets	
Air Conditioning	
Air Conditioning Units	**10**
Power Supply	
Power Sources (AC)	**2**
UPS	**5**
Batteries	**25**
7 Software Assets	
Operating Systems / Patches / Upgrades	
Windows Server 2012	**Variable**
Windows Server 2008 R2	**Variable**
Linux	**Variable**
Applications – Enterprise	
ERP	**Variable**
McAfee SIEM Solution	**2**
Databases	
SQL Server – Symantec	**1**
Utility Software	
Application: Adobe Acrobat PDF Writer	**Variable**
Application: Adobe Acrobat PDF Reader/ Viewer	**Variable**
Application: Win Zip	**Variable**
Application: Win rar	**Variable**
Application: Windows Media Player	**Variable**
Application: Internet Explorer	**Variable**
Application: Power DVD	**Variable**
Application: Microsoft Office 2016	**Variable**
Application: Microsoft Project	**Variable**
Awareness Solution	**1**

Table 5: CIA value for each asset

Asset Type : Asset Group : Asset List	Units	C	I	A	Asset Value
1 Company Image & Reputation					
Banners / Letterheads / Logos / Rubber Stamps / Seals		3	4	2	Very High
Blank Letterheads	Variable	2	2	2	Medium
ID-Cards	Variable	3	2	2	High
Logos	1	1	4	2	Very High
Signature Rubber Stamps	Variable	3	4	2	Very High
Rubber Stamps/Seals	Variable	2	2	2	Medium
2 Information Assets					
Configuration Files		3	4	3	Very High
Oracle Database	4	3	4	3	Very High
SQL Server	4	3	4	3	Very High
Oracle ASM	1	3	4	3	Very High
Storage Config	2	3	4	3	Very High
Server Config	14	3	4	3	Very High
OS Config	14	3	4	3	Very High
Core Switch	2	3	4	3	Very High
Router	2	3	4	3	Very High
Firewall	2	3	4	3	Very High
Network Switches	170	3	4	3	Very High
Vulnerability Manager	1	3	4	3	Very High
IPS	1	3	4	3	Very High
VPN	1	3	4	3	Very High
Endpoint Security	1	3	4	3	Very High
Source Code		3	4	3	Very High
Application Source Code	3	3	4	3	Very High
Manuals / Diagrams		3	4	2	Very High
Video Conference Manual	Variable	3	4	2	Very High
Electrical Diagrams	1	2	3	2	High
Work Place Floor Diagrams	1	2	3	2	High
Training Manuals	Variable	2	3	2	High
Operational Documents		3	3	2	High
Anti Virus Procedures	1	1	3	2	High
IPS Procedures	1	3	3	2	High

Firewall Procedure	1	3	3	2	High
VPN Procedure	1	3	3	2	High
Vulnerability Manager Procedure	1	3	3	2	High
Router Procedure	1	3	3	2	High
Active Directory User Creation/ Modification/ Deletion	1	1	3	2	High
Data Center Access Request	1	1	3	2	High
Network/ Internet Access	1	1	3	2	High
Systems Vulnerability Assessment Request	1	2	3	2	High
Websites Vulnerability Assessment Request	1	1	2	2	Medium
Blocking Spam Emails	1	1	2	2	Medium
Update/ Modify IPS	1	1	2	2	Medium
Information Security Incident Reporting	1	1	2	2	Medium
Infosec Awareness Program Request	1	1	2	2	Medium
Legal Documents		2	4	3	Very High
Signed NDAs	Variable	2	3	3	High
Vendor Contracts	Variable	2	4	2	Very High
Databases		3	4	3	Very High
Sql Server Database	3	3	4	3	Very High
Standards / Agreements / Proposals		4	4	3	Very High
RFP (Before Floating)	Variable	4	3	3	Very High
RFP (After Floating)	Variable	1	4	3	Very High
Non Disclosure Agreements	Variable	3	4	3	Very High
Proposals Against RFP	Variable	3	4	3	Very High
Vendor Contracts / Invoices		2	4	3	Very High
Vendor Contracts	Variable	2	4	3	Very High
4 People Assets					
Managers / Executives		1	4	3	Very High
Dean of IT deanship	1	1	4	3	Very High
Vice dean of IT deanship for Quality and development	1	1	4	3	Very High
Vice dean of IT deanship for technical affairs	1	1	4	3	Very High
Departments Manager	9	1	4	3	Very High
Employees		1	4	3	Very High
Network Administrator	2	1	4	3	Very High
System Administrator	2	1	4	3	Very High
Developer	1	1	3	3	High
Information Security Engineer	1	1	3	3	High
Database Administrator	1	1	3	3	High
5 Physical Assets					
Access Control System		1	3	4	Very High
Biometric Access Control	1	1	3	4	Very High
Surveillance System		1	3	4	Very High
CCTV	4	1	3	4	Very High
Building Infrastructure		3	3	4	Very High
Data Centre	1	3	3	4	Very High
Manager rooms	5	2	2	2	Medium
Administrator Rooms	4	2	2	2	Medium
Meeting Rooms	1	2	2	2	Medium
Power supply room	1	2	2	2	Medium
Vice Dean's Room	1	2	2	2	Medium
Desktops		1	3	3	High
Desktops	8	1	3	3	High
Fire Fighting Sytem		1	3	3	High
Smoke Detector	10	1	3	3	High
Fire Extinguishers: Hand held	8	1	3	3	High
Fire Alarms	5	1	3	3	High
Fire Hydrant Pump	4	1	3	3	High
Servers		3	4	4	Very High
Proxy Servers	3	2	4	3	Very High
DHCP Server	1	2	4	3	Very High
Syslog	1	2	4	3	Very High
Windows Physical Servers	35	3	4	4	Very High
Physical Servers – Linux	5	3	4	4	Very High
Intel Rack (HP & Dell)	10	3	4	4	Very High
Storage Devices		2	4	3	Very High
Storage Box	6	2	4	3	Very High
6 Service Assets					
Air Conditioning		2	4	3	Very High
Air Conditioning Units	10	2	4	3	Very High
Power Supply		2	3	4	Very High
Power Sources (AC)	2	1	3	4	Very High
UPS	5	2	3	3	High
Batteries	25	2	2	3	High
7 Software Assets					
Operating Systems / Patches / Upgrades		1	3	3	High
Windows Server 2012	Variable	1	3	3	High
Windows Server 2008 R2	Variable	1	3	3	High
Linux	Variable	1	3	3	High
Applications – Enterprise		1	3	3	High
ERP	Variable	1	3	3	High
McAfee SIEM Solution	2	3	4	4	Very High
Databases		3	4	3	Very High
SQL Server – Symantec	1	3	4	3	Very High
Utility Software		1	3	3	High
Application: Adobe Acrobat PDF Writer	Variable	1	3	3	High
Application: Adobe Acrobat PDF Reader/ Viewer	Variable	1	3	3	High
Application: Win Zip	Variable	1	3	3	High
Application: Win rar	Variable	1	3	3	High
Application: Windows Media Player	Variable	1	3	3	High
Application: Internet Explorer	Variable	1	3	3	High
Application: Power DVD	Variable	1	3	3	High
Application: Microsoft Office 2016	Variable	1	3	3	High
Application: Microsoft Project	Variable	1	3	3	High
Awareness Solution	1	1	3	2	High

4.3 Security Evaluation Standard

The university is legally committed to ensure adherence to leading industry standards and best practices. This has been considered when it chose adhere to a standard of information security evaluation and management.

The security standard that selected is ISO/IEC 27001:2013[9]. The ISO/IEC 27001 standard is divided into twelve high level domains: risk assessment, policy, organizational security, asset management, human resources, physical and environmental, communications and operations management, access control, system development and maintenance, security incident management, business continuity, and compliance and regulations. The university has been officially certified for two consecutive circles for its adherence to this standard.

4.3.1 Standard Objectives

In order to mitigate identified information security risks, this standard's framework shall be applied to all information processing systems. This framework forms a baseline from which more specific policies and procedures may be derived. The standard objectives for the selected university are:

- Developing a coherent system for information security management aligned with the university’s strategy.
- Designating owners to classify information based on the requirements of confidentiality, integrity and availability.
- Building a security function for coordinating the implementation and maintenance of all security policies.
- Defining clear roles and responsibilities for each staff member with regard to information security; and to implement an effective awareness program.
- Ensuring the safety of personnel from physical and environmental threats.
- Establishing accountability for all actions the interact with the university's information or information systems.
- Building a continuous risk management process for regular reviews and reassessments.
- Reducing disruptions of the university’s critical business and IT services.
- Ensuring all necessary measures are taken for protection of information and information systems to meet relevant legislations and contractual obligations.

5. Proposition and Implementation of Security Enhancements

It is quite normal for any organization to be confronted by several IT risks threating its information systems and data. Countermeasures and security control should be properly deployed to mitigate these risks and protect the IT assets. The selected university possesses a number of state-of-art security controls. However, in this section we propose a number of security enhancements that can be either improvements to currently used controls or adoption of new controls; along with a proposed implementation plan.

5.1 Security Enhancements

A fundamental security principle is system isolation; which means isolating all operational servers within physical environment that is more secure, and hence, easier to manage its penetrability risk. Additionally, resource-sharing systems have to be designed in a way that safeguards each user from the system itself and anther users, along with preserving privacy. By their nature, computer systems bear normally a number of vulnerabilities. These vulnerabilities can be hardware vulnerabilities, software vulnerabilities, or human vulnerabilities. The security framework design must consider addressing all these types of vulnerabilities, which can be exploited deliberately or accidently. Below, we propose some enhancments to the currently used security controls.

5.1.1 Combating Advanced Persistent Threats

Advanced Persistent Threats (APT) which are sophisticated and covert attacks bent on secretly stealing valuable data from unsuspecting and targeted companies [24]. Their persistent nature targets key users within an organization to gain access to intellectual properties, computer source code, trade secrets, and any form of valuable information. Since APTs operate covertly, and are hard to detect, months could pass without any visible compromises to the university. Individual instance maybe detected while multiple others within the same organization go undetected.

One of the key steps to safeguarding against the quiet and subtle attacks that are part of APT is to have a suitable set of tools inplace [25]. These entails the natively integrated contextual security of the traps, firewall and aperture, to prevent APTs at every stage of the network

[9] https://www.iso.org/standard/54534.html

attack, at endpoints, as well as within cloud environments. APT prevention can thus beachieved through granular security controls that reduce content based signatures, attack surface and URL categorizations that block delivery, command along with control channels, as well as signature-less exploit preventions elements the safeguard endpoints from threats [24]. These tools should be automatically updated. The university needes to fight the APT within the three main network segments:

- User gateway segment (the university campus and branches).
- Premiter segment (ISP connected link).
- In the front of the data center VLAN (servers gateways).

5.1.2 CCTV Surveillance

The university should implement a more advance CCTV surveillance system than its current one. The IT Deanship should handle the monitoring of the new CCTV. This system will facilitate the identification, apprehension and presecution of criminals in relation to crimes including unauthorized access to restricted areas as well as stealing or vanderlization of assets. In addition to the data centre, it will monitor an MDF room that it is held within another building.

5.1.3 Intrusion Prevention Systems (IPS)

Intrusion prevention systems should always be connected in line, which enables them to drop specific packets, as well as defend against an attack before it infiltrates the internal network. IPS technologies use a combination of a number of methodologies for detecting attacks. The university should add a second layer of IPS protection that will increase its detection of an incredibly wide array of attacks, and particularly attacks that have never been seen before (e.g. attacks that cannot be detected by signature-based detection methodologies). The added layer can establish benchmarks of normal activities derived from continual monitoring over time; where subsequent deviations from these baselines will be indicators of possible attacks [26]. This should help in detecting distributed denial-of-service attacks, as well as malware infections within the university network through anomalous network activity patterns. Also, it can parse and examine email and web activity in order to self-develop novel detection strategies.

5.1.4 Configuration and Access Right Review

The university should commence a routing job of configuration and access right review of the network security solutions such as the firewalls and virual private network (VPN). This is very important to avoid any miss configurations and/or mistakes. These reviews must take please peroidcly following a well-studied schedule.

5.1.5 Virtual Environment Hypervisor Security

Securing the virtual environments is more complicated than securing the physical one due to their complexity. In the university, there are security concerns that a malicious code or a malware may spread between workloads. The virtualization abstracts applications from the physical server hardware running underneath, which allows the servers to run multiple workloads simultaneously and share some system resources. The university has a VMware hypervisor, which uses the vShield security tool[10]. The university needs to inspect its hypervisor in order to optimize file-level security functions, such as antivirus and file integrity monitoring; this can be achieved by properly configuring and managing vShield. In VMware virtualized environments, vShield offloads antivirus and anti-malware agent processing to a dedicated secure virtual appliance delivered by VMware partners.

5.1.6 Federated Identities

Due to some implementation complications and issues, the university has not deployed a single sign-on (SSO) service. SSO enhances security and user-convenience by requiring the user to sign-on only once (i.e. a sole authentication check) during a given working session that might involve access to multiple servers and applications [27]. We suggest providing SSO service via a federated identities scheme. Federated identities schemes are reliable, scalable, and can be implemented in heterogeneous environments [27].

5.2 A Proposed Security Controls Implementation Plan

As discussed above, we have proposed several security enhancements; some of them were improvements on the currently deployed ones, whereas some mandate adopting new controls.

Table 6 shows our proposed implementation plan for those enhancements. The table specifies the team that should engaged in implementation, the dependencies, and the implementation time frame for each proposed security control enhancement. This plan was developed after a focused study that we have conducted with technical personnel of the IT Deanship.

[10] https://pubs.vmware.com/vsphere-50

Table 6: Security controls implementation plan

Security Control Enhancement	Engaged team	Dependencies	Implementation time frame
Combating Advanced Persistent Threats (APTs)	Information Security Network Service Desk	It needs network downtime to install the appliance in-line	3 weeks after appliances delivered.
CCTV Surveillance	Information Security Operation and Maintenance	Making sure that the currently used CCTV monitoring system is compatible with new CCTV devices.	2 weeks for installations and one week to configure it in the monitoring system.
Second layer of Intrusion Prevention Systems (IPS)	Information Security Network Systems	The sizing for the IPS throughput and interface of the next hub devices.	2 weeks for installations and four weeks for fine-tuning.
Configuration and access right review for network security solutions	Information Security Network Application	Having access to the request systems and access control systems.	It is routing job review, have to be quarterly period.
Virtual environment hypervisor security	Information Security Network Systems Application	Virtual environment active support. Available computing resources on the virtual environment system (VMware).	1 week for installations on test hypervisor then the installation on the production will takes 2 weeks.
Federated identities management system	Information Security Network Systems Application	Requires focused integrations on the application layer. Requires several occasions of testing downtime. The identity provider must be highly secured. Cryptographic controls and key management system must be defined.	8 weeks for integration, installation, and configuration. 3 weeks test period before it is ready to be released to the production.

6. Concluding Remarks

Since all state universities in the Kingdom of Saudi Arabia are funded by the same body (i.e. the Ministry of Education) and there IT legislations are set by the same body (i.e. Yasser), they bear an evident resemblance to one another. We have conducted a security assessment research on one the biggest and oldest Saudi state universities that has a number of branches scattered over different cities. Our first observation was that because of the strong IT governance and solid legislations mandated by the government, and their adherence to well-known standards (e.g. ISO/IEC 27001), the non-functional security level is satisfactory.

With regard to the IT infrastructure, the university is equipped with state-of-art system, servers, and solution. It possesses a certified data-centre (T3) with powerful appliances. The university provides a variety of operational and educational services using modern techniques like for example virtualization and cloud computing.

In this paper, we have provided an overview of our security analysis, by which we have identified the threats and controls posed and deployed by the university. Also, we have proposed a number of security enhancements based on our on-the-field study. Moreover, we have proposed an implementation plan for the proposed enhancements.

Finally, the findings and propositions of this paper can be readily projected to other Saudi state universities from a general prospective.

References

[1] DELL EMC. *Dell EMC VxBlock Systems, Converged Infrastructure*. 2016. http://www.vce.com/products/converged/vblock/overview [last accessed: March 2018].

[2] Keith Schultz. Review: *VDI without the server connection*. InfoWorld. 2012. https://www.infoworld.com/article/2619594/virtualization/review--vdi-without-the-server-connection.html [last accessed: March 2018].

[3] Mitch Tulloch. *Introducing Windows Server 2012 R2*, 1st Edition. Microsoft Press. ASIN: B00JYE19VM. 2013.

[4] Bob Lewis. Fixing the relationship between business and IT. InfoWorld. 2012. https://www.infoworld.com/article/2618423/it-strategy/fixing-the-relationship-between-business-and-it.html [last accessed: March 2018].

[5] International Organization for Standardization (ISO). *ISO 7498-2: Information processing systems -- Open Systems Interconnection -- Basic Reference Model -- Part 2: Security Architecture*. 1989.

[6] Walter J. Goralski. *Juniper and Cisco Routing: Policy and Protocols for Multivendor IP Networks, 1st Edition*. Wiley. ISBN: 0471215929. 2002.

[7] Thomas M. Thomas II and Doris E. Pavilchek and Lawrence H. Dwyer III and Rajah Chowbay and Wayne W. Downing III and James W. Sonderegger. *Juniper*

Networks Reference Guide: JUNOS Routing, Configuration, and Architecture, 1st Edition. Addison Wesley. ISBN: 0201775921. 2002.

[8] Oracle Corporation. *Oracle SuperCluster Security: Technical Implementation Guide (STIG) Validation and Best Practices on the Database Servers*. An Oracle technical white paper. 2014.

[9] Trent Jaeger. *Operating System Security (Synthesis Lectures on Information Security, Privacy, and Trust), 1st Edition*. Morgan and Claypool. ISBN: 1598292129. 2008.

[10] John K. Waters. *Virtualization Definition and Solutions*. CIO. 2007. https://www.cio.com/article/2439494/virtualization/virtualization-definition-and-solutions.html [last accessed: March 2018].

[11] Chris Fehily. SQL. Peachpit Press. ISBN: 0321118030. 2002.

[12] Mark D. Murton and Dale T. van Dongen and Michael P. Ross and Francis A. Bouchier. *Toward a performance requirement for sensored conformable apertures*. Proceedings of the IEEE International Carnahan Conference on Security Technology (ICCST). USA. 2012.

[13] Li-RenYang and Jieh-Haur Chen and Xing-LiangWang. *Assessing the effect of requirement definition and management on performance outcomes: Role of interpersonal conflict, product advantage and project type*. The International Journal of Project Management, Elsevier. Volume 33, Issue 1, Pages 76–80. January 2015

[14] Pete Houser. *Best Practices for Systems Integration*. Northrop Grumman Corporation. 2011.

[15] Dieter Gollmann. *Computer Security*, 3rd Edition. John Wiley & Sons. ISBN: 0470741155. February 2011.

[16] Michael Sanchez. *The 10 most common security threats explained*. Cisco Blogs. 2010. https://blogs.cisco.com/smallbusiness/the-10-most-common-security-threats-explained [last accessed: March 2018].

[17] Oracle Corporation. *Oracle SuperCluster T5-8 Security Technical Implementation Guide (STIG) validation and best practices on the database servers*. An Oracle Technical White Paper. February 2014.

[18] Zachary Kessin. *Building Web Applications with Erlang*. O'Reilly Media. ISBN-13: 9781449309961. 2012.

[19] John R. Vacca. *Computer and Information Security Handbook*, 2nd Edition. Newnes. ISBN: 0123946123. 2012.

[20] Adolfo Rodriguez and John Gatrell and John Karas and Roland Peschke. *TCP/IP Tutorial and Technical Overview*, 7th Edition. Prentice Hall. ISBN: 0130676101. 2001.

[21] Hamid R. Nemati (Editor). *Security and Privacy Assurance in Advancing Technologies: New Developments*. IGI Global. ISBN: 1609602005. 2010.

[22] V. S. Bagad. *Network and Information Security*, 4th Edition. Technical Publications. ISBN: 9350380188. 2011.

[23] Hank Marquis. 10 Steps to Do It Yourself CRAMM. Itsm Solutions. December 2008. http://www.itsmsolutions.com/newsletters/DITYvol4iss50.htm [last accessed: March 2018].

[24] McAfee Incorporation. *Combating Advanced Persistent Threats: How to prevent, detect, and remediate APTs.* 2011.

[25] Jason Andress. Advanced Persistent Threat: Attacker Sophistication Continues to Grow? The ISSA Journal. ISSA. Volume 9, Issue 6. June 2011.

[26] Karen Scarfone. *Enterprise benefits of network intrusion prevention systems*. TechTarget. 2015. http://searchsecurity.techtarget.com/feature/Enterprise-benefits-of-network-intrusion-prevention-systems [last accessed: March 2018].

[27] Waleed A. Alrodhan. *Privacy and Practicality of Identity Management Systems: Academic Overview*. VDM Verlag Dr. Müller GmbH, Germany. ISBN-13: 978-3639380255. 2011.