المجلة العلمية لجامعة الملك فيصل
The Scientific Journal of King Faisal University

العلوم الأساسية والتطبيقية
Basic and Applied Sciences

Security Assessment of Large-Scale IT Infrastructure

تقويم أمن البنية التحتية لتقنية المعلومات في المنشآت الكبيرة

Shouki A. Ebad
Department of Computer Science, Faculty of Science, Northern Border University, Arar, Saudi Arabia

شوقي عبدالله عبّاد
قسم علوم الحاسبات، كلية العلوم، جامعة الحدود الشمالية، عرعر، المملكة العربية السعودية

LINK الرابط	RECEIVED الاستقبال	ACCEPTED القبول	PUBLISHED ONLINE النشر الإلكتروني	ASSIGNED TO AN ISSUE الإحالة لعدد
https://doi.org/10.37575/b/cmp/0055	19/11/2020	23/01/2021	23/01/2021	01/06/2021
NO. OF WORDS عدد الكلمات	**NO. OF PAGES عدد الصفحات**	**YEAR سنة العدد**	**VOLUME رقم المجلد**	**ISSUE رقم العدد**
7986	8	2021	22	1

ABSTRACT

Due to today's online interactions, the security of IT infrastructure components is important for organizations. The literature survey revealed that evaluation of security of an IT infrastructure has not received as much attention from the research communities as that of application security. This paper examined an example of Saudi IT infrastructure to identify the challenges that threaten security, along with recommendations to address these challenges. Different qualitative methods were used in data collection, including focus groups, direct meetings, observations, and archival data/documents. Key categories of security threats are found to be networking, (e.g., violation of the principles of secure design), systems and storage (e.g., patching management), and information/endpoint (e.g., operation procedures). The lessons learned indicated that these infrastructure security risks can be addressed through various means, including infrastructure management (e.g., monitoring, documentation, and compliance with project management practices), software business activities (e.g., renewal of vendor support service), network redesigning (e.g., avoiding single point of failure structure), and incident response procedures (through developing and implementing clear, formal procedures). Some kinds of infrastructure security threats, such as cascading threats, are difficult to discover and evaluate. This study will assist security requirements engineers, systems managers, and security compliance officers.

الملخص

نظرًا لأن المؤسسات في الوقت الراهن تعتمد على الإنترنت في أعمالها، فإن أمن المعلومات للعناصر المكونة للبنية التحتية لتقنية المعلومات الخاصة بتلك المؤسسات أمر مهم. وقد أظهرت الدراسات السابقة أن تقويمًا أمنيًّا لبنيةٍ تحتيَّةٍ كهذه - على مستوى المنشآت الكبيرة - لم يلقَ اهتمامًا كبيرًا من الباحثين مقارنةً بنظيره على مستوى البرمجيات. في هذا البحث، تم فحص البنية التحتية لتقنية المعلومات في إحدى المؤسسات الحكومية الكبيرة في السعودية، وذلك من أجل تحديد الثغرات التي تهدد أمن المعلومات في بيئة كهذه، ووضع التوصيات الملائمة لكل ثغرة. تم استخدام المنهج النوعي في هذه الدراسة؛ مشتملًا على مجموعة التركيز والاجتماعات المباشرة والملاحظات والبيانات الأرشيفية. نتائج الدراسة أظهرت أنَّ أهم التهديدات الأمنية يمكن تقسيمها إلى ثلاث فئات: (1) الشبكات (مثال: عدم الالتزام بمبادئ التصميم الآمن للشبكة)، (2) الأنظمة والتخزين (مثال: إدارة الباتش)، (3) المستخدم النهائي ومعلوماته (مثال: الإجراءات التشغيلية). كما تمت الإشارة إلى الدروس المستفادة من هذا التقويم من خلال مناقشة العوامل التي تعالج المخاطر والتهديدات الأمنية، ومن تلك العوامل: إدارة البنية التحتية (مثال: المراقبة الآنية للأنظمة، والتوثيق، واتباع أفضل الممارسات في إدارة مشاريع التقنية)، وأعمال البرمجيات (مثال: تجديد رخص الدعم الفني)، وإعادة تصميم الشبكة (مثال: تجنب التصميم المعتمد على نقطة مفردة)، وإجراءات الاستجابة للحوادث (من خلال تطوير إجراءاتٍ واضحةٍ وتنفيذها). علمًا أنَّ هناك أنواعًا من التهديدات يصعب اكتشافها وتقويمها، مثل التهديدات المتتالية. ستساعد هذه الدراسة المختصين مثل مهندسي المتطلبات الأمنية، ومديري الأنظمة، وواضعي اللوائح الأمنية.

KEYWORDS
الكلمات المفتاحية
Assessment, IT infrastructure, IT security, networking, security engineering, systems management
إدارة الأنظمة، أمن تقنية المعلومات، البنية التحتية لتقنية المعلومات، تقويم، الشبكات، هندسة الأمان

CITATION
الإحالة
Ebad, S.A. (2021). Taqwim 'amn albinyat altahtiat litaqniat almaelumat fi almunshat alkabira 'Security assessment of large-scale IT infrastructure'. *The Scientific Journal of King Faisal University: Basic and Applied Sciences*, **22**(1), 136–43. DOI: 10.37575/b/cmp/0055

عبّاد، شوقي عبدالله. (2021). تقويم أمن البنية التحتية لتقنية المعلومات في المنشآت الكبيرة. *المجلة العلمية لجامعة الملك فيصل: العلوم الأساسية والتطبيقية*، **22**(1)، 136-143.

1. Introduction

IT infrastructure includes everything that supports the processing and flow of information in an organization (Pearlson, 2019). It consists of different IT resources that provide a basis from which to enable current and future business applications. It includes four classes of components: (1) hardware components (e.g., personal computers (PCs) and servers, (2) software components (e.g., operating system (OS) platforms and database management systems, (3) data and storage components (e.g., data quantity, data format, data transfer, and storage media), (4) networking components (e.g., switches, hubs, and routers). Some writers on management information systems add non-technical elements such as 'human' as a fifth class of IT infrastructure components (Sousa and Oz, 2015). These components must also be combined in a coherent model if they are to represent usable infrastructure. IT infrastructure has an impact on an organization at three different levels: processes, assets, and individuals. This impact may be positive or negative depending on factors such as configuration, security, and energy consumption (Shrivastava, 2015). However, infrastructure longevity not only depends on the organization's strategic planning, but also on the degree of advances affecting the technologies on which the IT manager depends (Pearlson, 2019). The matter may become particularly complicated in the case of financial firms, which store their assets (e.g., gold and real estate) in digital form (Priem, 2020). Many technical issues should also be considered when choosing infrastructure; a frequently used criterion is security, which refers to how well an infrastructure component protects the organization against basic information security threats. In other words, it ensures that the infrastructure is configured to resist cyberattack (Sommerville, 2015). In essence, organizations want to protect their infrastructure components from those who may attempt to misuse them. Because organizations increasingly depend on their pervasive applications, vulnerabilities in their systems grows rapidly (Ahmed *et al.*, 2017). This makes IT infrastructure security a critical business concern. Accordingly, IT infrastructure security is not only a technical or engineering issue, but also a managerial one, as system managers must set up their infrastructure to resist attacks (Sommerville, 2015). This requires a set of managerial tasks (e.g., user accounts management, attack management, and software maintenance).

Corresponding Author: Shouki A. Ebad shouki.abbad@nbu.edu.sa ,00966508808620 المؤلف المراسل: شوقي عبدالله عبّاد

In addition, disruptions in IT infrastructure may have economic and social impacts on organizations (Ebad 2018a; Alanazi *et al.*, 2020). This has been confirmed by previous studies. For instance, e-government projects and enterprise resource planning projects may fail because of poor IT infrastructure at organizations (Shang and Seddon 2000; Alateyah *et al.* 2013; Ebad, 2018a). Project failure ranges from delays and cancellation to a loss of millions of dollars of technology Ebad, 2018a). It is therefore important that the continuous monitoring of IT infrastructure security becomes part of IT service management best practices (Marrone and Kolbe, 2011). Countries also depend on IT as a key factor in measuring their national e-readiness (Rabii and Abdelaziz, 2015). At a basic level, security is important because it ensures the integrity of the operations that take place on trusted computing infrastructure.

As a consequence of this, organizations must conduct real-world security assessments of such infrastructure to ensure their security of the entire organization, through identifying possible security issues in every functional unit in the organization. However, performing these assessments in is a difficult, time-consuming task, as today's IT infrastructure is increasingly complex and involves diverse relationships (Schoenfisch *et al.* 2018). This study tackles the problem using a qualitative approach, focusing on an example of large-scale infrastructure in the governmental sector in Saudi Arabia. Although the IT field in Saudi Arabia has received governmental subsidization, Saudi organizations still struggle to secure their IT-based systems (Ebad 2018a; Alanazi *et al.*, 2020). The evaluation comprises the detection and diagnosis of the technical problems that threaten infrastructure security, along with recommendations for how to address such problems. Accordingly, the contribution of this study comes from the need to understand the security threats faced by real-world IT infrastructure at big organizations in the public sector. Such a disastrous case explains what happens, why, and where. To the best of our knowledge, while large-scale case studies have been used to assess application security, the research community has given less attention to using them for the assessment of the attribute security of IT infrastructure (Yasasin *et al.* 2020). Furthermore, using a real-world case allows an understanding of the consequences for the whole organization. This is because the focus is based on systems theory, which considers IT infrastructure components as a whole, rather than on traditional approaches, where the parts are examined separately. This improves the chances of converting future security failures into successes. The infrastructure studied herein is also much broader than in previous works (e.g., Antonino *et al.*, 2010; Sanchez-Nielsen 2011; Schoenfisch *et al.* 2018).

2. Literature Review

Sommerville (2015) introduced issues that should be considered when designing secure application systems, such as life-cycle risk assessment, operational risk assessment, architecture and design guidelines for secure systems development, and understanding system survivability. Antonino *et al.* (2010) developed a method for evaluating the security of service-oriented, architecture-based applications at architecture level. The method depends on recovering security-relevant facts about the application by using reverse engineering techniques and subsequently providing automated support for further interactive security analysis at the structural level. Using a questionnaire method, Shrivastava (2015) investigated the influence of IT infrastructure on information security at organization level. The major items in the questionnaire concerned privacy, integrity, vulnerability, unauthorized access, data leaks, forged identities, and email safety. The results showed that 97% of participants know the importance of security, including CCTV cameras and visitor registers, 92% admit that their organizations require a security assessment policy, 96% favor using licensed applications, and 94% admit there must be a backup policy in organizations. Chaturvedi *et al.* (2008) made an attempt to present a snapshot of cyber security infrastructure in an Indian context. The authors stated that their attempt was a precondition for all e-commerce and e-governance initiatives being taken the world over. Shoffner *et al.* (2013) developed the Secure Medical Research Workspace (SMWR) system to enable researchers to use medical data securely. The system minimizes the risk presented when using identifying medical data, thereby protecting researchers, patients, and institutions. It was built on a combination of data loss prevention software and virtualization. The SMWR system can be combined with other security approaches and scaled to production levels.

To achieve high availability of services, Schoenfisch *et al.* (2018) proposed an approach for calculating the root cause of a failure in an IT infrastructure component. They used Markov Logic Networks, which combine logical formulas (to describe dependencies) and probabilities (to express various possible risks) in a single representation, and applied their approach to the small case study of a multifunctioning office printer. Zambon *et al.* (2010) introduced a new qualitative time dependency model and technique for the qualitative assessment of availability risks, based on the propagation of availability incidents in IT infrastructure. They applied the model to a real-world case by carrying out a risk assessment on the authentication and authorization system of a large multinational company. The model provided better results in terms of accuracy and reduced the number of subjective decisions taken by the risk assessor. Sanchez-Nielsen *et al.* (2011) designed and implemented a multi-agent system to support incident management in IT infrastructure and restore normal service operation as quickly as possible. To illustrate the main features of their application, an experimental context simulating real-world IT infrastructure was used. Mastelic and Brandic (2013) introduced a method for comparing IT infrastructures, considering time and capacity. For time, they used two techniques: story points used by agile development teams to estimate project complexity, and Amdahl's law for the possibility of modeling task parallelization. For capacity, they introduced an intuitive resource slicing approach that divides resources into their smallest usable configurations. They evaluated their method by comparing physical infrastructure with cloud infrastructure, focusing only on processor and memory resources. Hashizume *et al.* (2013) categorized security issues for cloud computing with respect to its models (SaaS, PaaS and IaaS). As a result, storage was the biggest security concern, followed by virtualization. Kirby (2015) discussed seven best practices that allow organizations to leverage their physical infrastructure as a strategic advantage and minimize risks. These include matching infrastructure capabilities to the business mission, knowing the risks, building vs. buying decisions (consider internal management vs. the demands of vendor oversight), starting with the end in mind, focusing on operations, trust but with verification, and efficiency.

Ahmed *et al.* (2017) proposed an enterprise architecture model focused on security; it combined the essential elements, features, and relationships that make up a secure organizational framework. Compared with the existing models, theirs included kernel-based security architecture with risk and incidents management systems. Dalol (2018) measured the effectiveness of accounting information systems in light of IT infrastructure security and development. The results showed a strong, positive, significant correlation between the existence of IT infrastructure and the effectiveness of accounting information systems. There was also a nearly strong, positive, significant correlation between the existence of information security and the effectiveness of accounting information systems. Adu and Adjei (2018) investigated cyber security awareness in corporate organizations in Ghana. The main result was that awareness of cyber security remains limited. In addition, most organizations were not integrating legal features into their information security policies. Teymourlouei and Harris (2019) evaluated the importance of cybersecurity in small business organizations and provided recommendations about critical parts of an effective security plan.

In conclusion, most of the previous research discussed focuses on other aspects of IT infrastructure, rather than on security. Some studies concentrate on specific types of infrastructure components, such as memory (Mastelic and Brandic, 2013), or on physical infrastructure components (Kirby, 2015). Some focus on quality attributes, such as availability (Schoenfisch *et al.* 2018; Sanchez-Nielsen 2011; Zambon *et al.* 2010) or awareness (Adu and Adjei, 2018). Many studies focus on a specific kind of infrastructure, such as cloud computing (Mastelic and Brandic 2013; Hashizume *et al.* 2013), while others evaluate the security of IT infrastructure using the questionnaire method (Shrivastava 2015; Dalol 2018; Adu and Adjei 2018) or literature surveys (Hashizume *et al.* 2013). Such research methods are insufficient when it comes to identifying security issues because, while they may reflect opinions, they cannot address the "why" and "how" questions as effectively as the case study method, which addresses the case as a phenomenon. A few studies have evaluated, to some extent, the security of infrastructure, but only by focusing on a particular type of application, such as service-oriented, architecture-based applications (Antonino *et al.* 2010), medical applications (Shoffner *et al.* 2010), accounting information systems (Dalol 2018), or small organizations (Teymourlouei and Harris, 2019). Some researchers have performed assessments on simulated IT infrastructure. To the best of our knowledge, no existing study has presented an assessment of security in the real-world IT infrastructure of a large organization. This study investigates the security issues faced by practitioners, and discusses the lessons that can be learned.

3. Case Study Design

Case studies are a research method conducted to investigate a contemporary phenomenon in its real-life context (Wohlin *et al.*, 2012). They are used for empirical studies in various fields, such as medicine, policy, sociology, politics, psychology, and public administration, and are suitable for the evaluation of industrial IT-related phenomena and establishing how or why they occur, as in this study.

3.1. Management and Business Context:

A case study at a large government organization in Saudi Arabia (hereafter, Org.) was carried out. Org. has over 50 departments distributed throughout four branches in four cities. It employs approximately 5,000 staff members and has 20,000 clients and business partners. The procurement department provides every employee with a PC, laptop, or tablet, and the IT department (ITD) supports the business by offering several applications accessed via these devices. The ITD facilities for all branches are located at the headquarters, where this evaluation was conducted. ITD consists of six main functional units. Each unit has a head, who communicates with the top management (i.e., three hierarchical levels: unit staff, unit heads, and top management). Table 1 presents these units, sizes, and their responsibilities.

Table 1: ITD units in Org.

Unit description	Responsibilities
Unit #1 Networking & servers). Size: ~10 people.	(a) the network foundation including incidents, virtual private network, protocols, and creating/maintenance of wired/wireless access points (b) physical and logical servers including maintenance, security, hosting, and creation (c) administration of the active directory, and (d) domain name system (e) virtualization
Unit #2 (Data center). Size: ~5 people.	A data center houses and maintains Org.'s IT infrastructure for the continuity of daily operations. The data center operators are responsible for monitoring the status of equipment, cooling, heating, power, adding new equipment, removing equipment due to defects. They are also responsible for managing the entrance of ITD people or visitors to the data center.
Unit #3 (E-services). Size: ~5 people.	E-mail, Web site (e.g., maintenance & contents), message service, user accounts, application development
Unit #4 (Technical support). Size: ~10 people.	Solving the employees' problems related to hardware (e.g., PCs, laptops, tablets, printers, scanners), software (e.g., OS, software update, antivirus)
Unit #5 (Telephone &Videoconferencing). Size: ~5 people.	Hardware/software-related issues or support of the landline phone, fax, e-fax, and videoconference machines (e.g., installation, configurations).
Unit #6 (Business Applications). Size: ~4 people.	Maintaining enterprise systems, e.g., enterprise resource planning, e-corresponding, and document management.

Org. in its entirety relies on these units for the continuity of its services and business. Around 50% of the business applications are developed to assist Org.'s clients to access the necessary information. However, due to a lack of experienced IT professionals, the critical IT services and applications (e.g., email, network, and enterprise resource planning) are developed, operated, and maintained by a third party, through an approximately three-year contract. Despite this, the IT infrastructure contains numerous security issues, most of which were not addressed by the ITD's top management.

3.2. Objective:

The objective of this research can be expressed as follows:

"To analyze the experience and perspectives of IT infrastructure practitioners in an industrial context, in order to identify the security threats pertaining to real-world IT infrastructure".

3.3. Data Collection:

In case studies, data come from interviews, documentation, direct observations, archival data, participant observation and physical artifacts (Wohlin *et al.*, 2012). According to Lethbridge *et al.* (2005), there are three levels of data collection: (1) direct methods, in which the researcher directly contacts the subjects and collects data in real time, (2) indirect methods, in which the researcher directly collects data without actually interacting with the subjects, and (3) independent methods, in which the researcher uses compiled data or already-available artifacts. Herein, we, to some extent, used all three of the above techniques, as shown in Table 2.

Table 2: Data collection methods

Level	Technique	Details	Time
Direct	focus groups/ subjective	Unstructured meetings. Open-ended nature. For effective and authoritative responses, members of the focus group were the unit heads described in Table 1.	Several visits to the data center were done at different times. Most of the discussion rounds were on-site, while the rest were remote. The team can access the systems at any time/place via virtual private network. A number of meetings were conducted; only the considered people participated in the meetings. Few meetings/visits were in Org.'s branches. The assessment took around three months. Different samples of Network Node Manager and NexThink reports were taken (daily; weekly, monthly).
	Observations in meetings/subjective	While meeting attendees interact with each other, notes and feedback are taken.	
Direct/Indirect	direct observations/ objective	Multiple visits to the data center, with discussion with people there.	
Independent	Archival data/objective	Reports generated by monitoring software, including NexThink and Network Node Manager.	
	Documentation/objective	Org.'s network structure. The security policies.	

3.4. Technical Context:

The network topology consists of Cisco-based networks and wireless devices. In Org.'s headquarters, the switch models vary between high-performance data center backbone switches (Model 6509) and small access L2 switches (Models: 3560, 2960, and 3850). Unfortunately, the network was designed with no redundancy, i.e., if a core switch (6509) goes down, then all servers connected to this switch also go down. On the building floor, the users connect to the access switches using an RJ45 connection; the network traffic reaches these switches based on the ID of a virtual local area network, which is configured on the switch ports. The traffic is not balanced among servers because the load balancer is not connected. Access switches are connected to each other by cascade; only one link is connected to the distribution switch. Additionally, only one link is connected between point-to-point and WiMAX. Figure 1 provides a physical diagram of Org.'s network. This shows how the uplink and physical connectivity look. Details about the switch models used in every building/floor for each type of connection (P2P, WiMAX, and virtual private network) are available online. (https://drive.google.com/file/d/1ZV3tkkVgGNjdYcDXDQEx5FLbDMMyZ6wG/view?usp=sharing).

Figure 1: Network physical diagram

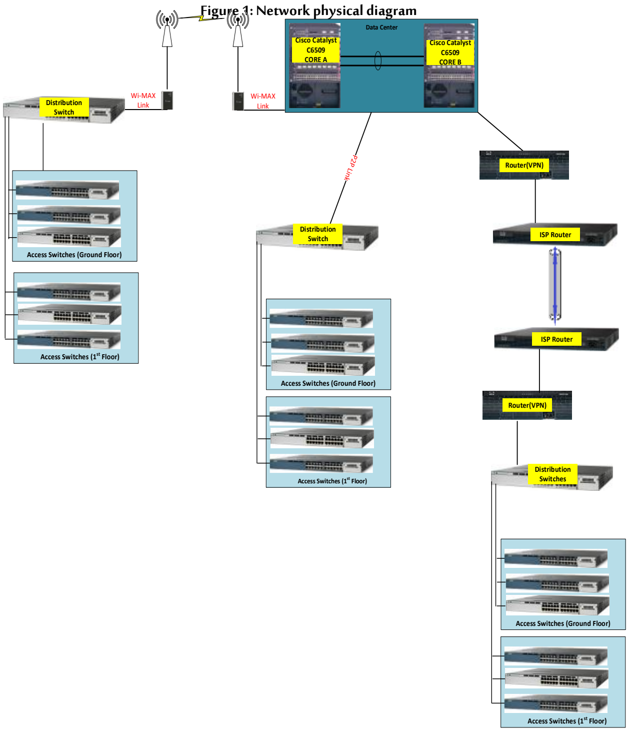

Data Center
Cisco Catalyst C6509 CORE A
Cisco Catalyst C6509 CORE B
Distribution Switch
Wi-MAX Link
Wi-MAX Link
P2P Link
Router(VPN)
ISP Router
ISP Router
Router(VPN)
Distribution Switch
Distribution Switches
Access Switches (Ground Floor)
Access Switches (1st Floor)
Access Switches (Ground Floor)
Access Switches (1st Floor)
Access Switches (Ground Floor)
Access Switches (1st Floor)

Figure 2 is a logical diagram of Org.'s network. A clear violation of the design standards is that the Cisco 3845 router is a single point of failure for the entire network. In other words, if this router fails, the entire network stops. In addition, there is a single firewall (Model: ASA5585-SSP20) for the data center. The top managers at ITD stated that they were required to build the IT infrastructure quickly due to financial considerations (i.e., money versus quality).

Figure 2: Network logical diagram

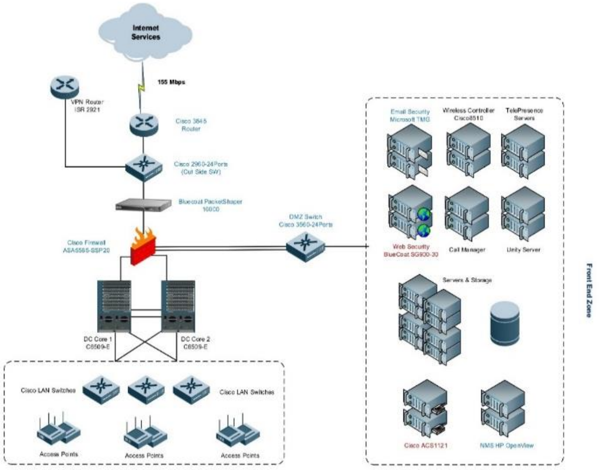


Table 3 shows more information about the systems and storage components. Often, these devices and associated facilities are located in the data center, which houses and maintains them for the continuity of daily operations. In Org., the data center is based on the American Power Conversion Corporation by Schneider Electric. It contains over 200 virtual and physical servers, some of which are completely or partially unused.

Table 3: Description of systems and storages components

Storage model	Disk type	Disk size	Hosts connected
HP 3PAR7400	SAN	21.76 TB	+50 (all blade servers in Org.'s data center)
	NL-SAS	43.3 TB	
EMC VNX 5300	SAS	14 TB	8 for two enterprise systems; 4 for each.
EMC VNX 5100	SAS	14 TB	+10 for e-corresponding system, archiving system, and others
HP MS5000	SAS	40 TB	+10 for messaging systems including email, e-fax, and SMS system
HP EVA P6000	SAS	12 TB	+10 for virtualization test environment and Hyper-V
HP StoreOnce 4220	SAS	N/A	+10 for disk-based backup and data protection manager
OSs: Windows server 2012 DC & Enterprise Red Hat Linux. Database management system: Oracle Database 11 g Enterprise Ed. & MySQL Server 2012. Wired and wireless networking: Cisco-based, including the IP Telephony & Call Manager. Most e-services offered: Microsoft, such as Active Directory (for network domain), Windows (for OS), Sharepoint (for Website environment), Exchange (for email), Lync/Skype for Business (for chat), Hyper-V (for virtualization), and Visual Studio (for development). Security appliances: BlueCoat proxy, and two Microsoft products: Windows Defender as the endpoint protection & data protection manager, DPM ver. 4.1.3465.0. End-user hardware: Dell & HP (for PCs, Intel processor), iPad (for tablets) Fujitsu (for laptops & scanners), Cannon & HP (for printers), & CiTrix (for virtual desktop). Business applications: enterprise resource planning by Oracle & document management by Laserfiche.			

3.5. Procedures for Evaluation Process:

The IT infrastructure evaluation was performed after a formal consent. The evaluation team consisted of five technicians who belong to an IT firm. Because the infrastructure is large and complex, the technical members were highly-qualified, and were chosen based on consultation. The profile of the team members is summarized in Table 4, which shows their experience, qualifications, ages, and current roles in their organizations.

Table 4: Profile of the evaluation team members

#	Degree	More Certificates	Age	Current Role	Experience
1	BS in IT	Microsoft (MCSE). Cisco (CCNP, CCIE). EMC (System Engineer). FireEye (Systems Engineer Certification)	35	Security Engineer	12 years managing small to enterprise networks infrastructure
2	MS in IT	Microsoft (MCSE), Cisco (CCNP) EMC Certified on VMAX 10K and Backup/ Recovery, Red Hat Certified Systems Engineer	< 40	Senior Systems Engineer	7 years in system and network administration
3	BSc in Electronics & communications Engineering	Cisco (CCNA, CCNP). Foundry Networks Certified Network Engineer (FNCNE). Blue Coat (BCCPA, BCCPP, Blue Coat Certified Sales Consultant)	< 40	Head of Technical Support	12 years in the IT industry, in the field of systems and network engineering.
4	BS in Engineering – Electronics	Cisco (CCNA-Security, CCNP-Security, CCIE- Data Center, CCIP) Juniper (JNCIS-ER, JNCIA-EX, JNCIA-ER, JNCIA-JUNOS, JNCIS-SEC) Brocade (BCNE)	30	Network Support Engineer	7 years in data communication, networking & security
5	BS in Electronics & Communications Engineering	Cisco (CCNA, Brocade (BCNE), Aruba Wireless Mesh Professional	36	Network Engineer	15 years in network engineering and procurement

After conducting several meetings, the team determined three issue levels that could be applied to each condition or problem. These were based on the action that would need to be taken, as shown in Table 5.

Table 5: Security threat level determination

Level	Impact	Description
High	Serious	The corrective plan must be put in place as soon as possible, though the current infrastructure component may continue to operate.
Moderate	Significant	A corrective plan is required so that it must be developed to integrate the corrective actions within a reasonable period of time.
Low	Marginal	The infrastructure component's owner must determine whether a corrective plan is still needed or decide to accept the threat.

4. Analysis of Results

The resultant threats are divided into three classes: networking, systems/storage, and information/endpoint. Because the case study is a large, real-world organization (a representative example of organizations), the results of this kind of analysis are expected to assist not only IT professionals but also organization leaders. As mentioned in the introduction, in all organizations, regardless of size or level of sophistication, protecting the infrastructure components against possible threats remains a managerial challenge. Data were analyzed using categorization and tabulation, in which the data were organized in summary tables, as in most qualitative research. Table 6 presents the three classes of threats, the corresponding subcategories, and their cause and/or effect in the real-world situation. These threats may unintentionally form a security risk (e.g., be used to damage infrastructure resources or render them inaccessible to authorized users). The 'Level' column is determined based on the definitions in Table 5. The reader is assumed to be familiar with the concepts of security from networking, systems/storage, and information/endpoint aspects (e.g., link utilization, Telnet, patching, and malicious code). It is clear that the threats are interconnected, and consequently, the suggested solutions vary in nature, including networking, management, systems, and operational solutions.

Table 6: critical Org's infrastructure security issues/threats

#	Threat category	Threat sub category	Threat cause or/and effect	Level	Suggested solution
1	Networking	Violation of the design standards	single point of failure design Access switches are connected by cascade only No stacking between switches	High	Redundancy solution: configuring switches as redundancy
2		Link utilization	No monitoring Unwanted traffic from/within Org. may cause link congestion Unwanted traffic from/within Org. may also cause services interruption	High	Monitoring all uplinks on daily basis in Org.'s headquarters, branches, and remote sites. The suggested software is NetFlow Analyzer tool.
3		Services & performance degradation	Flaws, bugs, and defects in software affect Org.'s network devices/hardware resources	Mid	Monitoring CPU, memory, drivers, and other network perimeter devices, such as switches, routers, firewalls, modems, and hubs.
4		Complexity in accessibility	Permission delegation mechanism is not straightforward All network devices are configurable with local administrative accounts	Mid	Reconfiguring all network devices with a centralized authentication system. The suggested software is LDAP or RADIUS.
5		Network protocols	Use of Telnet to access some network devices (Telnet is a clear text protocol that does not encrypt data sent, including passwords) Unused open protocols	Mid-High	(a) For all supported devices, disabling clear text protocol (e.g., Telnet) and enabling SSH protocol (b) Unnecessary TCP/IP port must be disabled or removed from all servers. System administrator must identify the required ports to be allowed from the firewall
6	Systems/ storage	Patching management	The server-level patching process was not regular. This may allow a remote attacker to compromise the system	High	Implementing an automated patching system to manage vulnerability across Org.
7		Troubleshooting	Complexity in troubleshooting process of an application server	Mid	Enhancing the end user experience through knowledge transfer, training, etc.
8		Unavailability	One cause was performing maintenance tasks on the production systems, such as upgrading and backup restoration	High	Similar to the production systems, there is a need to build a virtual environment for test and development, to test all major changes prior to applying them to the production systems.
9		Active directory auditing	Auditing is disabled	Mid-High	Enabling auditing after establishment of audit policy
10		Insufficient storage	Use of SAS as storage technology. It is "out of support". The current infrastructure of government resource planning Oracle e-business suite consists of two copies: production environment and test environment. The production environment is installed on one server. The server of the production environment is also used for the database backup (Figure 4(b) illustrates the current government resource planning infrastructure at Org.).	Mid-high	The minimum requirements are as follows: Two servers: one for application and one for data. Four copies of government resource planning suite: development environment, test environment, backup environment, and production environment. Both backup and production environments should be connected using cluster technology.
11	Information/ endpoint	Operation documentation	Org.'s personnel (individuals, teams, and departments) work with no documentation for operational processes.	High	Implementing documentation to manage processes, changes, and risks.
12		Unauthorized remote access	This happens due to allocation of the systems/server	Mid	Remote access should be restricted to the owner and/or administrator. It is recommended that allocation of the systems be on the basis of data classification.
13		Malicious code (Note: the kinds of malicious code are virus, Trojans, logic bomb, time bomb, trapdoor/ backdoor, worm, and rabbit. Malicious code has different forms, including Java applets, ActiveX controls, and browser plug-ins (Mimura and Suga, 2019))	This occurred because of unfiltered traffic from Org.'s remote sites/buildings. Malicious code can lead to 'unauthorized remote access' (Threat #12)	High	Remote buildings should not communicate with other buildings. It is recommended that traffic be denied by default and allowed by exception (e.g., for some vendors).
14		Spreading malicious code	This took place because the ITD did not define any security incident response procedure	Mid	Defining IT security incident response procedures. This would control any security incident and reduce its impact
15		Data loss/theft	Some storage devices are unsuitable physically; used with no testing Data restoration procedures Endpoints allow for access to removable storage devices (e.g., USB)	Mid	(a) Implementing a new backup solution (b) Data restoration from backup media must be performed at least twice a year to ensure data and systems recovery (c) To ensure only legitimate business use and eliminate a common security blind spot, there is a need to deny endpoint access to removable storage device.
16		Password disclosure	Procedures of password reset Using weak passwords No certain threshold for failed log-in to critical systems Password changing is done manually	High	(a) Self-reset password must be implemented to avoid any social engineering attack; this will make the password changing for end users automated, i.e., more secure (b) Password policy must also be implemented (c) Automatic alert must be generated after a certain number of failed log-in attempts.

5. Discussion and Lesson Learned

5.1. Infrastructure Management:

Infrastructure management is the management of all operational components. This includes not only hardware, software, data/storage, and networking components but also processes, human resources, and policies. With effective infrastructure management, several threats could be addressed. For instance, the use of an efficient monitoring mechanism would mitigate threats #2, #3, and #11. Heads of ITD units, described in Table 1, could monitor their infrastructure components or systems. This would range from micro-level to macro-level monitoring, i.e., daily status, activity reports, weekly progress reports, risk and assumptions analysis reports, review reports, downtime reports, and defect reports (Pearlson, 2019). Network analyzer tools also play a vital role, allowing the diagnosis of performance problems across the networks and monitoring performance metrics.

In addition, the lack of formal infrastructure documentation is another management-related problem. Documentation often provides system maintainers with the necessary information (e.g., structure, features, and how to use the system). The lack of documentation was the main obstacle that the evaluation team faced in their assessment. Without documentation, a considerable time was spent trying to understand Org.'s infrastructure configuration. The ITD personnel work without documentation (threat #11). According to ITD management, the reason for the infrastructure management issues is an unacceptable level of ITD staff and manager turnover, especially in the branches. Another management-related problem is that the ITD personnel suffer from poor project management skills, and thus many of the IT projects were not completed or were cancelled. An example is the virtualization infrastructure/environment, which stopped after operating for only a few months. Besides enormous cost overruns, this resulted in large numbers of unused virtualization components, including servers and desktops. Security products, such as Forefront Identity Manager and DPM (for data protection and recovery), by Microsoft, could address several of the above threats. For example, threats #5 and #15 could be addressed (fully or partially) with DPM and Forefront Identity Manager, respectively. The evaluation team investigated the reasons for not running the above infrastructure components (i.e., virtualization and Microsoft security products). They found that Org.'s infrastructure was not suitable for virtualization because Org. was still growing, and traditional PCs were considered sufficient. Virtualization was adopted as a response to the 'surge in popularity of' virtualization technology, and no feasibility study was performed. The evaluation team recommended that the ITD use VMware rather than Hyper-V if there is a need to adopt virtualization. Although there is a need to adopt Microsoft products, these were a source of staff dissatisfaction due to a lack of relevant training. In addition, none of the ITD personnel were able to effectively operate the security products. This project management problem (inadequately qualified and experienced people) led to another security risk in Org., namely disabling the auditing feature in the Active Directory (threat #9). Although the Active Directory administrator was able to enable the auditing feature for a particular user and group of users, he was not sure about the side effects on other systems or subsystems. The administrator justified this by saying that he was waiting for the support service by Microsoft that often comes after the renewal of their product

In addition, permission delegation (threat sub category in threat #4) can be categorized as infrastructure management. Permission delegation is a difficult organizational trade-off between operational speed/overheads (lots of delegation) and higher security awareness (centralized control).

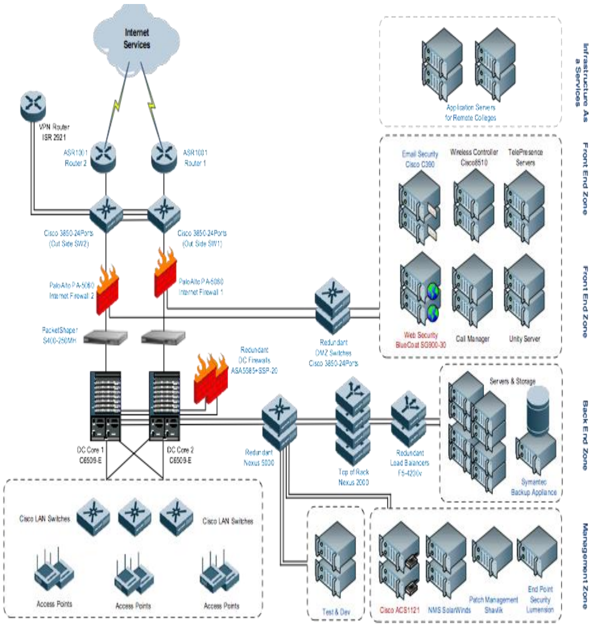
5.2. Software Business:

Software business refers to commercial activities such as licensing, vendor support, pricing, upgrading, and outsourcing of systems with a large amount of stored and processed data (Ebad, 2018b). A lack of awareness in relation to some of these activities was a root cause of several security threats in Org. According to the ITD staff, several security incidents happened because the patching process (threat #6) had not been automated. In addition, the patching/change/release process can essentially be delayed until the relevant vendor rolls out critical patches for the IT infrastructure components, i.e., some components remain in a known insecure state for some time. The evaluation team found some components were "out of support" or that "licensing for this product has expired" (e.g., enterprise resource planning by Oracle and Red Hat OS). The head of the Business Applications Unit at ITD (unit #6 in Table 1) stated that some of their enterprise systems suffer from the downtime issue every 3-4 months (threat #8).. When such a problem occurs, the head of unit #6 contacts a third party for support (incurring more cost). The same happens with hardware components, such as the single network firewall shown in Figure 2 (Model: Cisco ASA 5545-SPP20), and proxy caches and web filters (by Bluecoat). These products were either unlicensed or "out of support". In general, any cyber-attacker discovering a security vulnerability will wait until the vendor has stopped supporting the release before exploiting the vulnerability. Besides the security risk, the use of unlicensed software puts the whole organization at risk of legal consequences by vendors and developers.

5.3. Infrastructure Redesign:

Some of the threats came from the current design of the network, which depends on a single point of failure structure (threat #1). The evaluation team proposed a new design for the network, taking into account the redundancy mechanism to optimize the utilization of the network links and avoid the single point of failure structure. Figure 3 illustrates the proposed design.

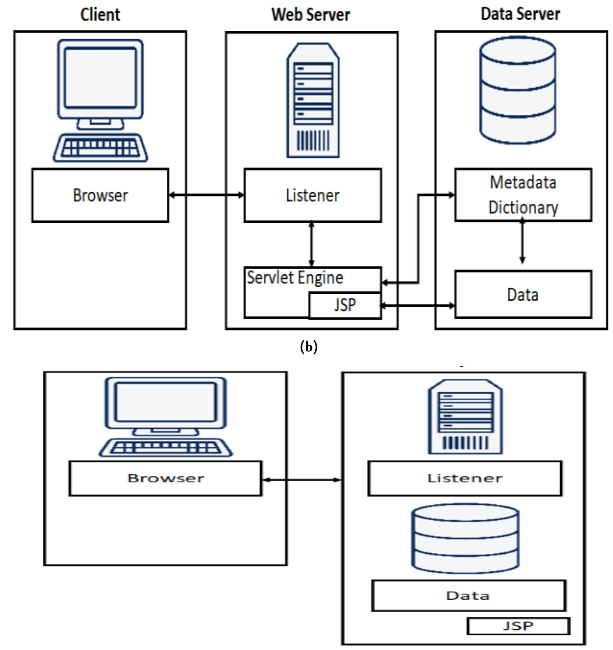
Figure 3: The proposed network logical diagram


Internet Services
VPN Router ISR 2921
ASR1001 Router 2
ASR1001 Router 1
Cisco 3850-24Ports (Out Side SW2)
Cisco 3850-24Ports (Out Side SW1)
PaloAlto PA-5060 Internet Firewall 2
PaloAlto PA-5060 Internet Firewall 1
PacketShaper S400-250MH
Redundant DC Firewalls ASA5585+SSP-20
Redundant DMZ Switches Cisco 3850-24Ports
DC Core 1 C6509-E
DC Core 2 C6509-E
Redundant Nexus 5000
Top of Rack Nexus 2000
Redundant Load Balancers F5-4200v
Cisco LAN Switches
Cisco LAN Switches
Access Points
Access Points
Access Points
Application Servers for Remote Colleges
Infrastructure As a Services
Email Security Cisco C390
Wireless Controller Cisco8510
TelePresence Servers
Front End Zone
Web Security BlueCoat SG900-30
Call Manager
Unity Server
Front End Zone
Servers & Storage
Symantec Backup Appliance
Back End Zone
Test & Dev
Cisco ACS1121
NMS SolarWinds
Patch Management Shavlik
End Point Security Lumension
Management Zone

Insufficient storage (threat #10) is considered an important cause of software unavailability (Ebad, 2018b). The evaluation team established that Org. had used SAS storage technology. This was not only fairly old but was also "out of support". Accordingly, the evaluation team's recommendation was that either the current storage technology be replaced, or the technical support for the current storage resources be renewed. Otherwise, Org. infrastructure would be in danger because the servers, in their current state, are expected to fail in attaching to the storage. Another suggestion was to reconfigure the current government resource planning e-business suite so that at least two separate servers are created—a web server and a data server (illustrated in Figure 4(a))—in order to install it properly: This would improve the current design, shown in Figure 4(b), which puts the database backup with the applications in a single server.

Figure 4: (a) A suggested design for the government resource planning e-business suite (b) Infrastructure of government resource planning e-business suite at Org.

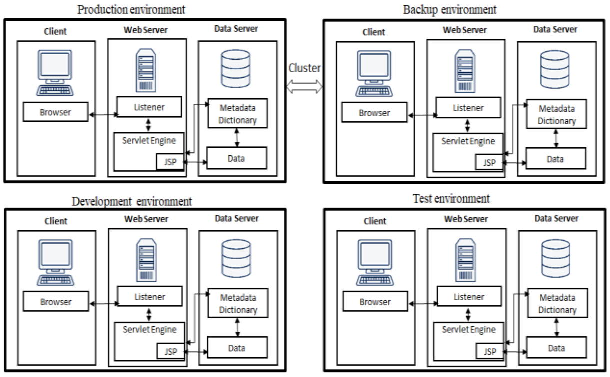
(a)



(b)

Furthermore, according to the evaluation team's recommendation (threat #10), there should be four government resource planning suite copies rather than two: development environment, test environment, backup environment, and production environment (shown in Figure 5). This would allow a clearer separation of concerns between applications and infrastructure. Accordingly, developers could construct their applications and schedule them to be run in the production environment without a great deal of expertise. As shown in the figure, the cluster technology would be more suitable for connecting the backup environment to the production environment. Through this approach, several security threats shown in Table 6 would be addressed.

Figure 5: A suggested design for the entire infrastructure



5.4. Security Incident Response Procedures:

An important recommendation by the evaluation team was related to policies and procedures. The evaluation team was shocked to discover that the ITD has worked without clear, formal policies. At the present time, any security incident occurring in Org. is addressed based on the experience of the people present at the time. In some critical cases (e.g., 'service temporarily unavailable'), where considerable time is required to solve the problem (mentioned in Section 6.2), the ITD asks for assistance from a third-party IT firm, which usually makes some modifications to important infrastructure components, including the production environment. Those changes are not managed properly due to the lack of policies. This means there is a high probability that the ITD personnel will not be able to deal with the same problem if it happens again in the future.

Furthermore, policies, including security incident response procedures, are the basis for accomplishing compliance to standards, and should be considered a living infrastructure artifact; that is, as the infrastructure changes at any level, the policies should change too (they must evolve over time). As policies evolve or change, the vulnerability to attacks typically degrades. A set of practices became *de facto* standards over the years, but are now actively dangerous or outdated (Topper, 2018). For example, password policy (threat #16) is considered a living artifact or evolving policy (in 2017, the National Institute of Standards and Technology in the U.S. published new rules on passwords, available at https://pages.nist.gov/800-63-3/sp800-63b.html). It is worth noting that the most important solution among those suggested by the evaluation team is the development and implementation of the security incident response procedures. It is clear that Org. was spending little effort on this important field. It has no chief information security officer, no security strategy, and no adequate monitoring of the network and systems. Dealing with security risks in this way is arguably reckless. With the correct procedures in place, several of the threats would be addressed, including threat #7 (troubleshooting), threat #11 (operation documentation), threat #14 (spreading malicious code), threat #14 (Data loss/theft - restoration procedures), and threat #16 (password disclosure - manual change).

6. Conclusion and Future Work

IT infrastructure has an impact on an organization's processes, assets, and personnel. Because today's organizations depend on their online interactions, the security of infrastructure components is important when choosing infrastructure. This study identified the technical problems that threaten IT infrastructure security, and suggested how such problems might be addressed. The infrastructure examined in this study was much broader than that in previous research, and different qualitative methods were used in data collection, including focus groups, direct meetings, observations, archival data, and documents.

Key categories of security threat were found to be networking, (e.g., non-compliance with the network design standards), systems and storage (e.g., patching management), and information/endpoint (e.g., operation procedures). The lessons learned indicated that infrastructure management (e.g., monitoring, documentation, and compliance with project management practices), software business activities (e.g., renewal of vendor support services), network redesign (e.g., avoiding the single point of failure structure), and incident response procedures (through developing and implementing clear, formal procedures) play a vital role in reducing infrastructure security risks. It is expected that this industry study will assist IT professionals, including systems engineers, network engineers, storage engineers, security requirements engineers, and organization leaders.

There is an aspect of infrastructure security that requires more research. Cascading security threats are difficult to discover and evaluate. For instance, incidents affecting the security of infrastructure component X may propagate to other components in the same infrastructure. Such dependencies are important if security issues are to be identified. Malicious code (threat #13) may lead to another security threat by allowing remote access to the organization's computers (threat #12). The situation is further complicated when infrastructures are interconnected. In such a case, a security incident may propagate (or provoke unexpected threats) not through different systems in the same infrastructure, but through different infrastructures within a city (i.e., infrastructure interoperability). In extreme cases, the incident propagation may be at higher levels, such as intra- or inter-country. In this situation, national laws and international agreements, respectively, play a significant role because the traditional evaluation approaches, which depends on the experience and intuition of the evaluator, may then be insufficient to identify this kind of security threat. While the IT industry and researchers are attempting to solve the technological and operational issues that IT infrastructure faces, legislators and regulators should monitor the rapid development of IT infrastructure so as to identify the need for regulatory action, especially in the case of financial firms (Priem 2020).

Biography

Shouki A. Ebad

Department of Computer Science, Faculty of Science, Northern Border University, Arar, Saudi Arabia, 00966508808620, shouki.abbad@nbu.edu.sa

Dr. Ebad received his Ph.D. in computer science and engineering from King Fahd University of Petroleum and Minerals, Saudi Arabia, in 2012. He is an Associate Professor. He is a Sun-Certified Programmer for the Java 2 Platform. His current research interests are software engineering, IT project management, and information security.

Acknowledgements

This work was supported by Northern Border University under Grant SCI-2019-1-10-F-8406.

References

Adu, K.K. and Adjei, E. (2018). The phenomenon of data loss and cyber security issues in Ghana. *Foresight*, **20**(2), 150–61.

Ahmed, M.T.U., Bhuiya, N.I. and Rahman, M.M. (2017). A secure enterprise architecture focused on security and technology-transformation (SEAST), *The 12th International Conference for Internet Technology and Secured Transactions*, (ICITST-2017), Cambridge, UK, 11–4/12/2017.

Alanazi, S.T., Anbar, M., Ebad, S.A., Karuppayah, S. and Al-Ani, H.A. (2020). Theory-based model and prediction analysis of information security compliance behavior in the Saudi healthcare sector. *Symmetry*, **12**(9), 1544. DOI: 10.3390/sym12091544

Alateyah, S.A., Crowder, R.M. and Wills, G.B. (2013). Identified factors affecting the citizen's intention to adopt e-government in Saudi Arabia. *World Academy of Science, Engineering and Technology*, **7**(8), 904–12.

Antonino, P., Duszynski, S., Jung, C. and Rudolph, M. (2010). Indicator-based architecture-level security evaluation in a service-oriented environment. In: *The Fourth European Conference on Software Architecture*: Copenhagen, Denmark, 23–26/08/2010. DOI: 10.1145/1842752.1842795.

Chaturvedi, M., Gupta, M. and Bhattacharya, J. (2008). *Cyber Security Infrastructure in India: A Study, Emerging Technologies in E-Government*. Available at: http://www.csi-sigegov.org/emerging_pdf/9_70-84.pdf (Accessed on 15/11/2020).

Dalol, M.H. (2018). *Effectiveness of Accounting Information Systems in Light of Development of IT Infrastructure and Information Security*. Master's Dissertation, The Islamic University of Gaza, Gaza, Palestine.

Dooley, K. (2001). *Designing Large Scale LANs: Help for Network Designers*. USA: O'Reilly Media.

Ebad, S. (2018a) An exploratory study of ICT projects failure in emerging markets. *Journal of Global Information Technology Management*, **21**(2), 139–60. DOI: 10.1080/1097198X.2018.1462071.

Ebad, S. (2018b). The influencing causes of software unavailability: A case study from industry. *Software Practice and Experience*, **48**(5), 1056–76. DOI: 10.1002/spe.2569.

Hashizume, K., Rosado, D.G., Fernández-Medina, E. and Fernandez, E.B. (2013). An analysis of security issues for cloud computing. *Journal of Internet Services and Applications*, **4**(5), n/a. DOI: 10.1186/1869-0238-4-5.

Kirby, L. (2015). *Beyond Cyber Security: Protecting Your IT Infrastructure*. Available at https://uptimeinstitute.com/images/Documents/ProtectingYourITInfrastructure.pdf (accessed on 15/11/2020).

Lethbridge, T.C., Sim, S.E. and Singer, J. (2005). Studying software engineers: Data collection techniques for software field studies. *Empirical Software Engineering*, **10**(3), 311–41.

Marrone, M. and Kolbe, L.M. (2011). Impact of IT service management frameworks on the IT organization. *Business and Information Systems Engineering*, **3**(1), 5–18.

Mastelic, T. and Brandic, I. (2013). TimeCap: Methodology for comparing IT infrastructures based on time and capacity metrics. In: *The IEEE 6th International Conference on Cloud Computing*, 131–8, Santa Clara, CA, USA, 28/06–03/07/2013.

Mimura, M. and Suga, Y. (2019). Filtering malicious JavaScript code with Doc2Vec on an imbalanced dataset. In: *The 14th Asia Joint Conference on Information Security* (AsiaJCIS), Kobe, Japan, 24–31/08/2019.

Pearlson, K.E., Saunders, C.S. and Galletta, D.F. (2019). *Managing and Using Information Systems*. 5th edition, USA: Wiley.

Popp, K. and Meyer, R. (2011). *Profit from Software Ecosystems Models, Ecosystems and Partnerships in the Software Industry*. Norderstedt, Germany: Books on Demand.

Priem, R. (2020). Distributed ledger technology for securities clearing and settlement: Benefits, risks, and regulatory implications. *Financial Innovation*, **6**(11), n/a. DOI: 10.1186/s40854-019-0169-6.

Rabii, L. and Abdelaziz, D. (2015). Comparison of e-readiness composite indicators, *The 15th International Conference on Intelligent Systems Design and Applications* (ISDA), Marrakech, Morocco, 14–16/12/2015.

Sanchez-Nielsen, E., Padron-Ferrer, A. and Marreo-Estevez, F. (2011). A multi-agent system for incident management solutions on IT infrastructures. In: *The 14th Conference of the Spanish Association for Artificial Intelligence* (CAEPIA 2011), La Laguna, Spain, 07–11/11/2011.

Schoenfisch, J, Meilicke, C., Stülpnagel, J.V. and Ortmann, J (2018). Root cause analysis in IT infrastructures using ontologies and abduction in Markov logic networks. *Information Systems*, **74**(2), 103–16.

Shang, S. and Seddon, P.B. (2000). A comprehensive framework for classifying the benefits of ERP systems. In: *The 2000 American Conference of Information Systems*, Long Beach, California, 10–13/08/2000.

Shoffner, M., Owen, P., Mostafa, J., Lamm, B., Wang, X., Schmitt, C.P. and Ahalt S.C. (2013). The secure medical research workspace: An IT infrastructure to enable secure research on clinical data. *Clinical and Translational Science,* **6** (3), 222–5.

Shrivastava, A.K. (2015). The impact assessment of IT Infrastructure on information security: a survey report. In: *International Conference on Information Security and Privacy* (ICISP2015), Nagpur, India, 11–12/12/2015.

Sommerville, I. (2015). *Software Engineering*. 10th edition, UK: Pearson.

Sousa, K.J. and Oz, E. (2015). *Management Information Systems*. 7th edition, USA: Cengage Learning.

Teymourlouei, H., and Harris, V. (2019). Effective methods to monitor IT infrastructure security for small business. In: *The 2019 International Conference on Computational Science and Computational Intelligence* (CSCI), Las Vegas, NV, USA, 5–7/12/2019.

Topper, J. (2018). Compliance is not security. *Computer Fraud and Security*, **2018**(3), 5–8. DOI: 10.1016/S1361-3723(18)30022-8.

Wohlin, C., Runeson, P., Host, M., Ohlsson, M.C., Regnell, B. and Wesslen, A. (2012). *Experimentation in Software Engineering*. Germany: Springer.

Yasasin, E., Prester, J., Wagner, G. and Schryen, G. (2020). Forecasting IT security vulnerabilities –an empirical analysis. *Computers and Security*, **88**(n/a), n/a. DOI: 10.1016/j.cose.2019.101610.

Zambon, E., Etalle, S., Wieringa, R.J. and Hartel, P. (2010). Model-based qualitative risk assessment for availability of IT infrastructures. *Software and Systems Modeling*, **10**(4), 553–80.