THE REPUBLIC OF TURKEY

BAHCESEHIR UNIVERSITY

CYBERSECURITY FRAMEWORK FOR SMALL AND MEDIUM SIZE ENTERPRISES

Master's Thesis

MEVLÜT BÜYÜKKILIÇ

ISTANBUL, 2018

THE REPUBLIC OF TURKEY

BAHCESEHIR UNIVERSITY

GRADUATE SCHOOL OF NATURAL AND APPLIED SCIENCES

CYBER SECURITY

CYBERSECURITY FRAMEWORK FOR SMALL AND MEDIUM SIZE ENTERPRISES

Master's Thesis

MEVLÜT BÜYÜKKILIÇ

Supervisor: ASSIST.PROF. BETÜL ERDOĞDU ŞAKAR

İSTANBUL, 2018

THE REPUBLIC OF TURKEY
BAHCESEHIR UNIVERSITY

GRADUATE SCHOOL OF NATURAL AND APPLIED SCIENCES
CYBER SECURITY

Name of the thesis: Cybersecurity Framework for Small and Medium Size Enterprises
Name/Last Name of the Student: Mevlüt BÜYÜKKILIÇ
Date of the Defense of Thesis: 28 May 2018

The thesis has been approved by the Graduate School of Natural and Applied Sciences.

Assist. Prof. Yücel Batu SALMAN
Graduate School Director
Signature

I certify that this thesis meets all the requirements as a thesis for the degree of Master of Arts.

Assist. Prof. Ahmet Naci ÜNAL
Program Coordinator
Signature

This is to certify that we have read this thesis and we find it fully adequate in scope, quality and content, as a thesis for the degree of Master of Arts.

Examining Committee Members   Signature____

Thesis Supervisor   ----------------------------------
Assist. Prof. Betül ERDOĞDU ŞAKAR

Member   ----------------------------------
Assist. Prof. Ahmet Naci ÜNAL

Member   ----------------------------------
Assist. Prof. Tayfun ACARER

ABSTRACT

CYBERSECURITY FRAMEWORK FOR SMALL AND MEDIUM SIZE ENTERPRISES

Mevlüt BÜYÜKKILIÇ

Cyber Security

Thesis Supervisor: Assist. Prof. Betül ERDOĞDU ŞAKAR

May 2018, 76 pages

In today's cyber connected world, it is almost impossible ignoring to use cyber technology, since governments, organizations and individuals are getting more and more involved and dependent on cyber capabilities. While this inevitable technology provides vital functions for the consumers, it also brings along a big concern, security of this technology; cybersecurity.

There is already a common agreement among all cybersecurity experts, that is informing the public about cyber threats and developing an awareness on the importance of the cybersecurity is the very first and the most important step towards cybersecurity. However, when it comes to the second step, implementing cybersecurity, it becomes complex and confusing for a cyber-awared consumer to choose and implement a solution to become cyber secure. Although cybersecurity experts and vendors are mostly successful to provide cybersecurity awareness to public, they also seem to be a source of this complexity and confusion for the consumers when it comes to cybersecurity implementation. One solution suggested by an expert can be found useless by another, some vendor may claim other vendors' solutions are obsolete, some says other solutions are unnecessarily expensive. While confusion and complexity get bigger, the main concern for the consumer remains the same; how to develop optimum cybersecurity capability spending as minimum resources as possible.

For large size organizations and firms, the path is somewhat clear; there are international standards to provide guidance towards cybersecurity, such as the International Organization for Standardization and the International Electrotechnical Commission (ISO/IEC), Control Objectives for Information and Related Technology (COBIT), Payment Card Industry Data Security Standard (PCI DSS), National Institute of Standards and Technology (NIST), and implementation of some of these standards are legally mandatory for some organizations; financial sector (banks), telecom companies, internet service providers, critical infrastructure companies etc. Although understanding and implementation of these standards require experts and dedicated resources for an organization, this is mostly not an issue for large size firms, they would have enough resources and it is legally mandatory anyway.

However, when it comes to small and medium size organizations, although they have cyber people to manage business IT operations, they do not have enough resources to employ cybersecurity expertise and the main concern for them still stands; how to implement optimum cybersecurity with minimum resources when there is this much complexity and confusion. Struggle to implement cybersecurity continues with consulting some firms and often ends up with implementing vendor driven solutions and overlapping functions, thus possibility of wasting resources.

This study aims to develop an easy to understand and vendor-free framework for small and medium size organizations which enables the organization design, implement, manage and assess cybersecurity in a simple and flexible way to meet business requirements.

Keywords: Cyber, Security, Cybersecurity, Framework, Small and Medium Size Enterprises

ÖZET

KÜÇÜK VE ORTA ÖLÇEKLİ İŞLETMELER İÇİN SİBER GÜVENLİK MODELİ

Mevlüt BÜYÜKKILIÇ

Siber Güvenlik

Tez Danışmanı: Dr. Öğr. Üyesi Betül ERDOĞDU ŞAKAR

Mayıs 2018, 76 sayfa

Bireylerin, kurumların ve devletlerin her geçen gün daha fazla siber kabiliyetleri kullanmaya bağımlı olduğu günümüz siber dünyasında siber teknolojilerin kullanımını göz ardı etmek imkansız hale gelmiştir. Bu teknolojik kabiliyet, kullanıcılarına çok önemli fonksiyonel faydalar sağlıyor olsa da, beraberinde çok önemli bir sorun sahasını da ortaya çıkarmaktadır; bu teknolojinin güvenliğini sağlamak, yani siber güvenlik.

Siber güvenlik uzmanları arasında genel bir görüş birliği olduğu üzere, siber güvenliğin sağlanmasındaki ilk ve en önemli adım, toplumda siber güvenliğin önemi konusunda 'siber farkındalık' oluşturmaktır. Ne var ki, siber farkındalık oluşmuş bir birey veya kurum için ikinci adıma, yani siber güvenliğin 'uygulanması' adımına gelindiğinde, bir siber güvenlik çözümünü seçip siber güvenli hale gelme konusunda işler biraz daha karmaşık hale gelmektedir. Toplumda siber güvenlik farkındalığı oluşturulması konusunda siber güvenlik uzmanları ve siber güvenlik çözüm üreticileri çoğunlukla başarılı olsalar da, aynı zamanda, kullanıcıların siber güvenliğin uygulanması konusunda yaşadıkları karmaşanın da kaynağı olabildikleri görülmektedir. Bir uzmanın önerisi bir başka uzman tarafından işe yaramaz bulunabilmekte, bir üretici diğerinin ürünlerini eskidiğini iddia edebilmekte, bazıları ise diğer bazı ürünlerin gereksiz yere pahalı olduğunu ileri sürebilmektedir. Söz konusu karmaşa ve kafa karışıklığı süre dursun, kullanıcılar için sorun hala ortada durmaktadır; mümkün olan en az kaynağı kullanarak en optimum siber güvenlik nasıl sağlanabilir?

Büyük ölçekli kurumlar ve şirketler için yol haritası nispeten daha açıktır; siber güvenliğin uygulanması konusunda yönlendirici uluslararası standartlar vardır, örneğin; International Organization for Standardization and the International Electrotechnical Commission (ISO/IEC), Control Objectives for Information and Related Technology (COBIT), Payment Card Industry Data Security Standard (PCI DSS), National Institute of Standards and Technology (NIST). Hatta finansal kuruluşlar ve bankalar, haberleşme şirketleri, internet servis sağlayıcıları ve kritik altyapı kuruluşları gibi bazı kurumlar için bu standartların uygulanması yasal bir zorunluluktur. Her ne kadar bu standartların anlaşılabilmesi ve uygulanabilmesi için ekstra kaynakların ayrılması ve siber güvenlik uzmanı personelin istihdam edilmesi gerekiyor olsa da, bu durum büyük ölçekli şirketler için genelde büyük bir sorun oluşturmamaktır, çünkü yeterli kaynakları vardır ve, her hâlükârda, yasal zorunluluk gereği olarak bir şekilde bu uluslararası standartları uygulayabilirler.

Ne var ki, küçük ve orta ölçekli işletmeler için siber güvenliğin uygulanması konusunda bu standartların çok bir faydası olamamaktadır. Her ne kadar küçük ve orta ölçekli şirketlerin de bilişim personeli olsa da, bu personel çoğunlukla şirket faaliyetlerinin yürütülebilmesi için gerekli bilişim hizmetlerinin yürütülmesi konusunda çalışmakta, siber güvenlik uygulamaları konusunda detaylı bilgiye veya standartların uygulanabilmesi için gerekli uzmanlığa sahip olmayabilmektedirler. Bununla birlikte, bu şirketlerin de, iş faaliyetlerinin sürekliliğini sağlayacak şekilde siber tehditlere karşı, en azından kabul edilebilir seviyede, siber güvenlik sağlamaları gerektiğinden, problem hala devam etmektedir; hangi siber güvenlik çözümlerinin uygulanması gerektiği konusunda bu kadar karmaşık bilgi varken, mümkün olan en az kaynağı kullanarak en optimum siber güvenlik nasıl sağlanmalıdır? Siber güvenliğin sağlanması çalışmalarında bu şirketler sonraki adım olarak, çoğunlukla, danışmanlık firmalarına başvurmakta, bunun sonucunda ise marka temelli çözümlerin satın alınması, gereksiz fonksiyonlara yatırım yapılması ve kaynakların boşa harcanması söz konusu olabilmektedir.

Bu çalışma, küçük ve orta ölçekli işletmelerin iş hedeflerine ulaşabilmeleri için ihtiyaç duydukları siber güvenliği tasarlamaları, uygulamaları, yönetmeleri ve değerlendirmeleri için kolay, anlaşılır ve marka bağımsız bir siber güvenlik modelinin geliştirilmesini hedeflemektedir.

Anahtar Kelimeler: Siber Güvenlik, Model, Küçük ve Orta Ölçekli İşletmeler

CONTENTS

TABLES

FIGURES

ABBREVIATIONS

ARP	:	Address Resolution Protocol
BCP	:	Business Continuity Plan
CCTV	:	Closed Circuit Television
CD	:	Compact Disk
CEO	:	Chief Executer Officer
CERT	:	Computer Emergency Response Team
COBIT	:	Control Objectives for Information and Related Technology
DLP	:	Data Loss Prevention
DMZ	:	Demilitarized Zone
DoS	:	Denial of Service
DDoS	:	Distributed Denial of Service
DNS	:	Domain Name System
DVD	:	Digital Versatile Disk
FTP	:	File Transfer Protocol
HIDS	:	Host Intrusion Detection System
HIPS	:	Host Intrusion Prevention System
HTTP	:	Hypertext Transfer Protocol
HTTPS	:	Hypertext Transfer Protocol Secure
HVAC	:	Heating, Ventilation, and Air Conditioning
IDS	:	Intrusion Detection System
IEC	:	International Electrotechnical Commission
IPS	:	Intrusion Prevention System
ISO	:	International Organization for Standardization
ISP	:	Internet Service Provider
IT	:	Information Technology
LAN	:	Local Area Network
L2TP	:	Layer 2 Tunneling Protocol
MAC	:	Media Access Control
MitM	:	Man in the Middle
NIDS	:	Network Intrusion Detection System

NIST	:	National Institute of Standards and Technology
OS	:	Operating System
PCI DSS	:	Payment Card Industry Data Security Standard
PPTP	:	Point to Point Tunneling Protocol
SIEM	:	Security Information and Event Management
SME	:	Small and Medium Sized Enterprises
SOHO	:	Small Office, Home Office
SSH	:	Secure Shell
TUIK	:	Turkish Statistical Institute (Türkiye İstatistik Kurumu)
USB	:	Universal Serial Bus
UTM	:	Unified Threat Management
VPN	:	Virtual Private Network
WAN	:	Wide Area Network
WAP	:	Wireless Access Protocol
WEP	:	Wireless Encryption Protocol

1. INTRODUCTION

1.1 WHY SMALL AND MEDIUM SIZE ENTERPRISES?

In the United Kingdom (UK), small companies (defined as employing fewer than 50 people) account for 99.3% of all private sector businesses and 48% of employment in UK (UK Government, 2017).[1] In Turkey, Small and Medium Sized Enterprises (defined as "Micro" if employing less than 10 people, "Small" if less than 50 people, and medium if less than 250 people) (Turkish Government Official Newspaper, 2012)[2] accounted for 99.8% of all private sector businesses and 73,5% of employment in Turkey in 2014 (TUIK 2016).[3] Despite this huge proportion in the whole, Small and Medium Sized Enterprises (SME) do not typically come into mind when someone thinks about the term *cybersecurity*.

TUIK (2016) also provides statistics about the use of internet by SMEs; 93,5% of SMEs have internet access, computer usage of SMEs in business is 95,8%, web page ownership is 65,2%, and 85,9% of SMEs used internet to communicate with public organizations and institutions. These figures reveal that SMEs are highly integrated with and depending on cyber technologies, and, even if they don't realize, cybersecurity threats may have significant effects for their business existence.

Actually, the need for cybersecurity in smaller organizations is not a new problem. In 1996, with the growth of personal computing, Carroll (Carroll, 1996) wrote:
"Most books on security were written for big-time users like banks and government agencies where enormous sums of money, or state secrets were at stake. Most PC systems could never meet the security requirements of these mainframe and

[1] UK Government, Department for Business, Innovation & Skills, Business population estimate for the UK and regions: 2017 statistical release, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/663235/bpe_2017_statistical_release.pdf , [accessed 25 Feb 2018]

[2] Turkish Government Official Newspaper, Regulation on the definition, composition, and classification of small and medium size enterprises, 2012, http://www.resmigazete.gov.tr/eskiler/2012/11/20121104-11.htm , [accessed 25 Feb 2018]

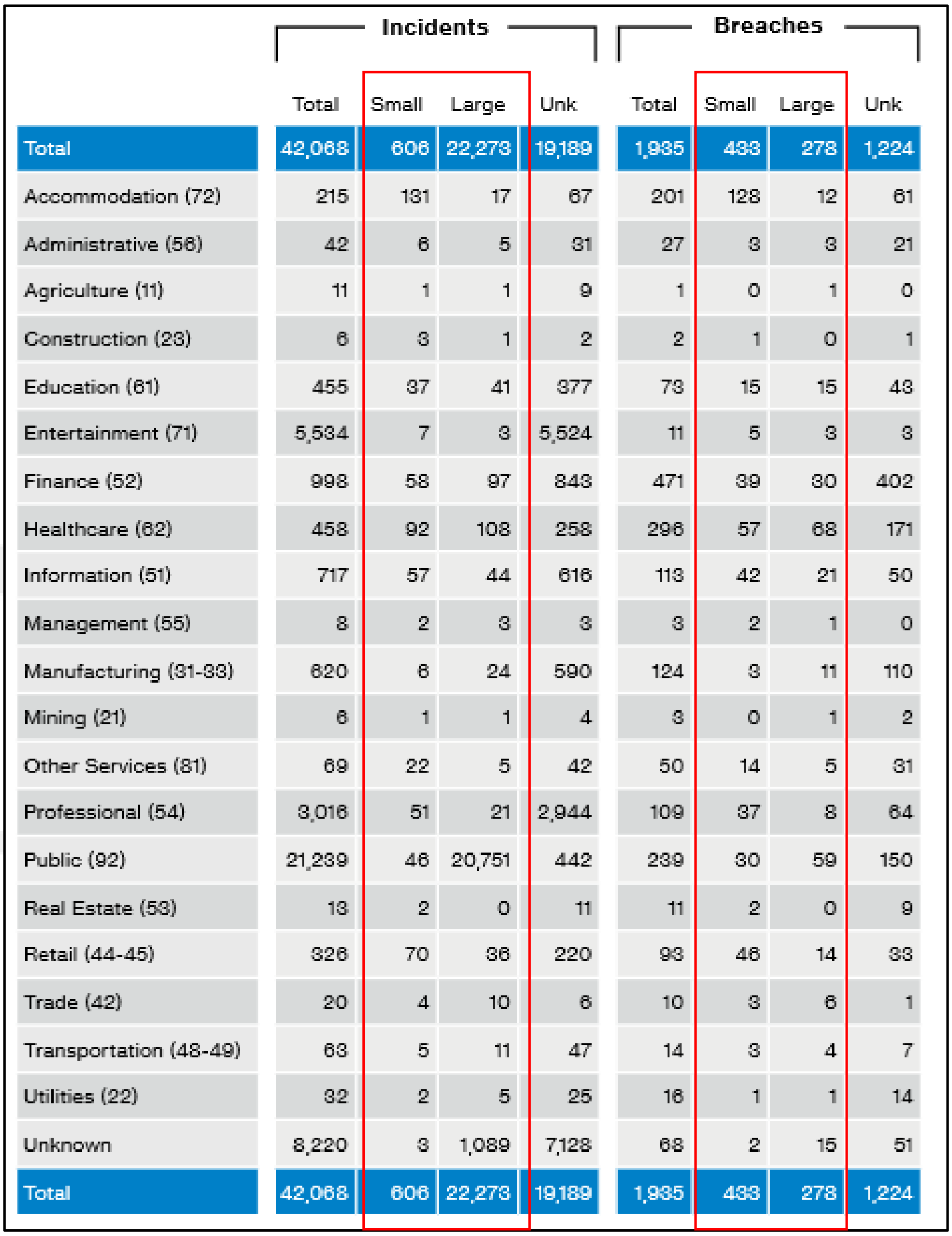
[3] Turkish Statistical Institute-TUIK, The Small and Medium Size Enterprise Statistics 2016, http://www.tuik.gov.tr/PdfGetir.do?id=21540 [accessed 25 Feb 2018]

minicomputer systems. And if they could, the average business or professional person could neither afford them nor be bothered maintaining them." (Carroll, 1996)

In the recent Data Breach Investigations Report of Verizon[4] (2017), security incidents and breaches are studied for several industries with different scales, one of the outcomes can be seen at Figure 1.1. The term "incident" defines a security event that compromises the integrity, confidentiality or availability of an information asset, while "breach" means an incident that results in the confirmed disclosure—not just potential exposure—of data to an unauthorized party. The important outcome of this figure, related with this thesis is that, while Large size enterprises have more total number of incidents (22,273) than the Small size enterprises (606), Large size ones result in less number of breaches (278) than the Small sized enterprises (433). In other words, cybersecurity impact rate of incidents in large size enterprises (1,2%) is way below the ones in small size enterprises (71%). According to this report, it can be concluded that, large size enterprises are, at least the ones studies in this report, more successful at implementing cybersecurity.

[4] Verizon, 2017 Data Breach Investigations Report 10th Edition, [online], https://www.ictsecuritymagazine.com/wp-content/uploads/2017-Data-Breach-Investigations-Report.pdf , [accessed 20 Feb 2018]

Figure 1.1: Data Breach Investigations Report of Verizon (2017)



	Incidents				Breaches			
	Total	Small	Large	Unk	Total	Small	Large	Unk
Total	42,068	606	22,273	19,189	1,935	433	278	1,224
Accommodation (72)	215	131	17	67	201	128	12	61
Administrative (56)	42	6	5	31	27	3	3	21
Agriculture (11)	11	1	1	9	1	0	1	0
Construction (23)	6	3	1	2	2	1	0	1
Education (61)	455	37	41	377	73	15	15	43
Entertainment (71)	5,534	7	3	5,524	11	5	3	3
Finance (52)	998	58	97	843	471	39	30	402
Healthcare (62)	458	92	108	258	296	57	68	171
Information (51)	717	57	44	616	113	42	21	50
Management (55)	8	2	3	3	3	2	1	0
Manufacturing (31-33)	620	6	24	590	124	3	11	110
Mining (21)	6	1	1	4	3	0	1	2
Other Services (81)	69	22	5	42	50	14	5	31
Professional (54)	3,016	51	21	2,944	109	37	8	64
Public (92)	21,239	46	20,751	442	239	30	59	150
Real Estate (53)	13	2	0	11	11	2	0	9
Retail (44-45)	326	70	36	220	93	46	14	33
Trade (42)	20	4	10	6	10	3	6	1
Transportation (48-49)	63	5	11	47	14	3	4	7
Utilities (22)	32	2	5	25	16	1	1	14
Unknown	8,220	3	1,089	7,128	68	2	15	51
Total	42,068	606	22,273	19,189	1,935	433	278	1,224

Source: Verizon, 2017 Data Breach Investigations Report 10th Edition, [online], https://www.ictsecuritymagazine.com/wp-content/uploads/2017-Data-Breach-Investigations-Report.pdf , [accessed 20 Feb 2018]

1.2 ORGANIZATIONAL CYBER SECURITY PROBLEM AREAS

There are several reasons to why Small and Medium Size Enterprises (SMEs) experience difficulty at implementing cybersecurity.

1.2.1 Different Structures, Different Requirements

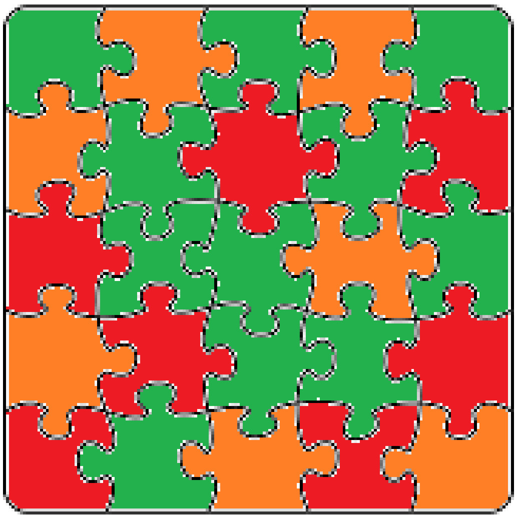
The system architectures employed by SMEs are significantly different from those employed by large corporate or government entities (Osborn et al. 2017). Where large companies' cyber structure may be composed of big number of assets, located in several different locations, connected via a complex network infrastructures, SMEs mostly rely on relatively small network and limited number of assets and locations. While large companies may require a well-designed complex chair, for small organizations it may be enough to safely "sit" on a three legged stool (Figure 1.2).

Figure 1.2: Small company requirement vs. Large company requirement

1.2.2 Excessive Number of Cybersecurity Solutions against Limited Resources

There are lots of cybersecurity technologic devices and software products in the market, most of which are relatively expensive for a small company to share budget for, and this makes it quite hard for them to figure out which ones to choose and implement. It also requires an organization to employ skilled people to properly understand the business requirements, current threats, risks and the functionalities of cybersecurity solutions against these risks to design an optimum cybersecurity structure for the organization. In most cases, since they don't have this manpower, they prefer to trust a consulting firm, which may end up implementing vendor driven, sometimes expensive, solutions and "hoping" to be safe. In other cases, they see it too much to invest on, take the risk and implement poor security or none at all. The framework defined in thesis will provide a clear and simple understanding of which security solutions provide what kind of security to an organization in a puzzle approach, with the motto “The more green, the more secure” (Figure 1.3).

Figure 1.3: Framework parts as a puzzle



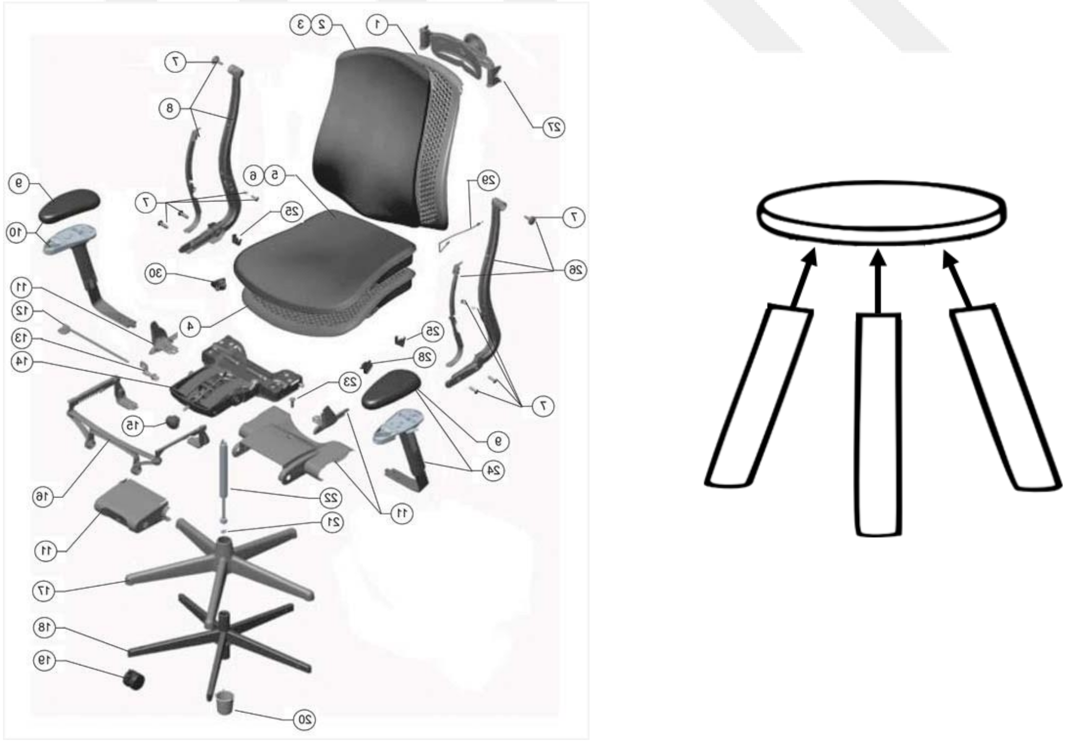
1.2.3 Ignoring the Basics

Protecting a cyber structure against breaches is like protecting a human body against illnesses. Although there are lots of advanced methods or products broadcasted on TVs, it should be remembered that basic healthcare tips (such as, move more, wash your hands, avoid stress, drink more water, eat adequately but frequently, wear clothes suitable to the weather, etc.) would be quite enough to maintain a healthy body. Likewise, although there are excessive number of cybersecurity solutions, implementing the most well-known measures can provide a decent level of security to the organization.

1.2.4 Standards – Aiding or Confusing?

There are international standards to aid the organizations designing and maintaining cyber security (such as, International Organization for Standardization and the International Electrotechnical Commission (ISO/IEC), Control Objectives for Information and Related Technology (COBIT), National Institute of Standards and Technology (NIST), etc.) but they tend to give the part and expect the organization to mount it up, which in most cases still requires an expert to understand and implement it. Some of the large size organizations are legally bound to implement these standards (such as, banks, internet service providers, telecom companies, governmental organizations), but, they already have enough funding to employ expertise for the implementation of these standards. Small and medium size companies need simpler and applicable solutions to implement, as illustrated in Figure 1.4.

Figure 1.4: Standards vs. small organizations' need



Standards provide

Small organizations need

1.3 GOAL OF THESIS

While organizations are more and more depending cyber technologies, cyber capability is becoming a key enabler for businesses. But, this technology also brings up the importance of cybersecurity for organizations. Since cyber threats are increasing every day, it is becoming more challenging to maintain a proper cybersecurity posture.

There is vast amount of cybersecurity products on the market, either hardware or software, but it is very hard for a small and medium size enterprise to analyze the threats, comprehend the functionalities of each type of products. These products may have a relatively high cost considering the organization size, and, proper implementation and maintenance of cybersecurity may require additional employment; cybersecurity experts in the organization. Small and medium size enterprises struggle to find the optimum implementation, balanced between security requirements and limited organizational resources.

The goal of this study is to develop a vendor-free framework, which will make it easy for small and medium size organizations to understand, design, implement, manage and assess cybersecurity for the organization.

1.4 OUTLINE OF THESIS

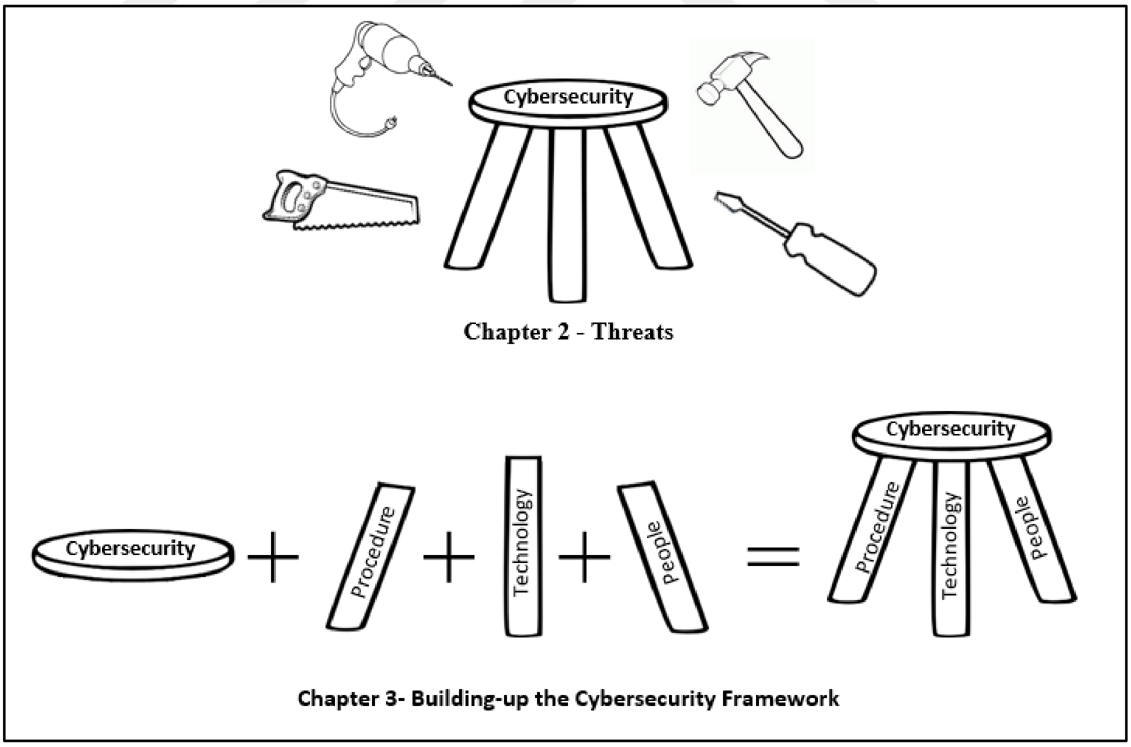
Chapter 1 provides an introduction to Small and Medium Size Enterprises, explains why they need specific cybersecurity measures, and discusses their problem areas.

Chapter 2 explains some common threats an organization may have, with some countermeasure information.

Chapter 3 is all about building the Framework. Since the main goal of this thesis is to simplify cybersecurity implementation as much as possible for small and medium size organizations, the thesis is structured as pieces to build up a cybersecurity capability for an organization as seen at Figure 1.5.

Chapter 4 provides sample implementations of the cybersecurity framework with two scenarios.

Figure 1.5: Outline of Thesis



In Chapter 3, it is also explained how to develop a framework profile, and how maturity assessment can be conducted for a specific organization. Framework governance and implementation methods are also provided in this chapter.

2. THREATS

While this study mainly focuses on developing and implementing cybersecurity for organizations, it will be beneficial to have knowledge about some of the recent threats, vulnerabilities and attack types to understand the necessity of several types of security solutions. Before going into the Cybersecurity Framework details in following chapters, knowing potential cyber-attack types will help the organization to understand the nature of the attacks and develop protection methods against various types of threats.

2.1 FACILITY PHYSICAL THREATS

Depending on the business context and size, small and medium size organizations can be located in different physical locations; such as, on its own premises, on a building in a compound, on a floor of a building or in several offices of a business center. In any case, the organization needs to ensure that proper access control and security measures are taken at the perimeter, building, and office levels at a minimum. Organization should also ensure that it provides its cyber assets with appropriate protection against physical threats such as fire, smoke, water leakages, air condition, etc.

2.2 ENVIRONMENTAL/NATURAL THREATS

Security term requires to consider not only current probable threats, future threats should also be taken into consideration. Depending on the geographical and environmental context, organizations should build proper protection methods. Below are some environmental threats which may affect an organization.

a. Floods
b. Earthquakes
c. Tornadoes

d. Power cuts

e. Explosions

f. Landslides

g. Public health (pandemic flu, ebola)

2.3 HUMAN THREATS

No matter which physical and technological security measures are taken, human still remains as the weakest link in the security chain. Below are some examples to human sourced threats

a. Negligent user

b. Insider threat

c. Organized crime

d. Competitors

e. Industrial Espionage

f. Cybercriminals

g. Hacktivists

Although procedural and technical solutions seem to mitigate some of these human threats, special attention should be given to the Insider Threat. Insider threat basically means the human threat coming from the inside of the organization. Following are some definitions for insider (Probst et al. 2010):

An insider is,

a. a person who is authorized to access to organization resources;

b. a totally or partly trusted asset;

c. an individual who has or, in the past, had access to organization cyber assets;

d. an organization user who may misuse given legitimate privileges;

e. an authorized organization personnel who may try to give damage to organization cyber assets or who can help outsiders to facilitate a cyber-attack;

f. an individual or a third party organization we would trust.

Some characteristics of what makes a good insider:

a. Skill, knowledge, intent, motivation;
b. Possesses authorization to act as agent of the business;
c. Knowledge about underlying business cyber platforms;
d. Knowledge/control over cyber security controls.

2.4 DIGITAL THREATS

There are lots of attack types developed by cyber criminals in cyber history. Although there are new attack types invented every day, most attackers do not try to re-invent the wheel and struggle to find a new attack type for every attack they perform to an organization, they just pick an attack type which is proven effective and use against the organization. For this reason, developing a cybersecurity capability to protect against commonly known attacks would provide a basic level of protection for organizations. Most common attack types are explained below.

2.4.1 Malware Attack

“Malware” refers to various forms of harmful software, such as viruses and ransomware (Rapid7 LLC, no date).[5] Once a malware is on the user computer, it can execute various malicious actions like taking control of the workstation, monitoring user actions and keystrokes, silently sending classified data from the computer to the attacker’s location.

Malware delivery methods

There can be various methods for the attacker to get the malware to user workstation, but eventually it mostly requires a user action to have the malware installed on the computer. These actions may include clicking a link which would download a file or

[5] Rapid7 LLC, [no date]. *The Most Common Types of Cyber Security Attacks*, [online]. https://www.rapid7.com/fundamentals/types-of-attacks [accessed 14 Feb 2018]

opening an attachment which normally looks like a harmless word or pdf file but actually contains malware installer hidden in the file. Most common delivery mechanisms are; Viruses which are self-spreading malware infecting other programs, files or operating systems by injecting a malicious code to the target, Trojan Horses which look like a legitimate program or application but actually used to host a malware inside the program and activates when the program is run on the target, Worms which are designed to spread themselves to other systems even without user interaction, while Viruses and Trojans are localized only on the infected target system. It should be noted that although above attacks occur via network communications such as e-mails, web sites, network services, a malware can also be delivered using physical media such as CD/DVD, USB disk, external hard drive, etc.

Countermeasure against malware attacks

To protect against malware attacks, user training plays a critical role. Users in the organization should be trained to recognize potential malware (phishing emails, suspicious attachments, etc.) and should be warned prevent malware infections (do not run suspicious attachments, do not install unknown applications, do not insert suspicious/unregistered USB/CD/DVD without prior scanning, etc.). Regular announcements and campaigns will be beneficial to develop a user awareness.

Using a decent antivirus software will help actively monitor, detect and remove malware. At this point, in order to enable the antivirus software recognize the malware, it is important that the software signature database is kept up to date.

The organization needs to ensure that access to the organization network is controlled, the organization data and network traffic is continuously monitored and protected by proven protection solutions. Implementation of firewall, IDS, IPS and VPN will provide adequate cyber protection for the organization.

Despite all protection measures taken by the organization, it may be still possible that the organization may be successfully attacked by a malware which may result destruction, disruption of the organization data, or, like in ransomware attacks, the data may become unusable. Organization must develop and implement proper backup procedures and solutions in order to be able to restore organization information as a last line of defense. It is important that backup procedures should include regular verification of backups for a possible restore operation.

2.4.2 Phishing Attack

Attackers already know that in a well-organized and cybersecurity aware organization, users will be careful against commonly known cyber-attacks, users will not just open every attachments or click every link on e-mails.

Figure 2.1: Phishing Attack (Sasneh 2016)

Phishing Methods

In a phishing attack, the attacker will try to trick the user, the malicious e-mail will look like sent from someone the user knows or trusts, (the boss or a colleague in the organization, invoice from telecom company, account statement from the bank etc.)

when the attachment is clicked or the link clicked, malware will be installed on user computer.

One of the common techniques used by attackers is to send a spoofed malicious link to a user which looks like an authentic one but with slight differences (using na1ionalelectriccompany.com instead of nationalelectriccompany.com), thus deceiving the user to click the link.

Another method is spoofing websites. In this method, attacker builds a web site which looks like a legitimate web site and gets the user visit this site using the techniques above. When the users, believing that they are visiting the authentic web site, provide credentials on the sites, these credentials are captured and saved by the attacker.

Phishing Attack Types

Spear Phishing: In this type of attack, the attacker targets a specific individual or an organization. Before conducting the attack, the attacker spends extra effort and collects information about the target (name, address, company logo, co-workers, other companies worked with, etc.) to develop the attack as legitimate as possible to increase the success of the attack.

Whaling: This type of attack targets an organization’s high level executives. When the victim is successfully deceived, the gain from the attack will be considerably more valuable (high level classified company information, company account credentials, etc.)

Clone Phishing: In this type of attack, the attacker gets a legitimate message which the organization had received earlier, makes slight changes inside it to meet the attack requirements and send it to the organization. It will be much easier for the attacker to trick a user receiving this cloned message.

Countermeasure against phishing attacks

Awareness training to all users (ALL, from boss to down) in the organization is the first step and most effective protection against phishing attacks. Educate the users to recognize phishing attacks and develop procedures to guide the users what to do when they receive a suspicious phishing attack.

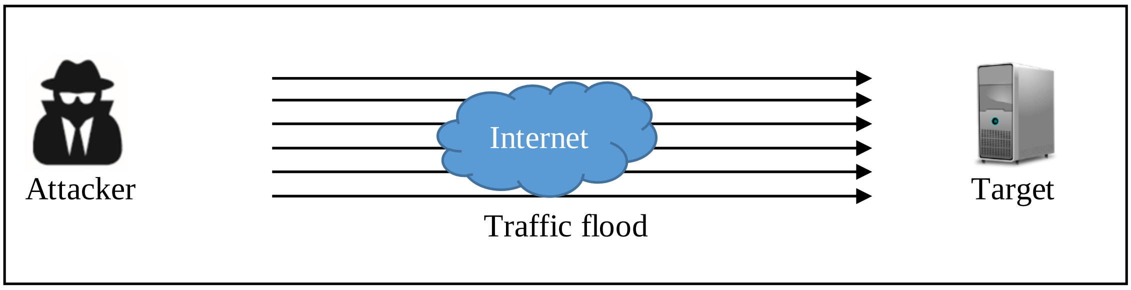
Using email protection technologies and software, attachments known to be suspicious and malicious URLs should be removed and quarantined before they reach to the users.

Domain policies should be applied to force the users use strong passwords (e.g. using minimum 12 characters to include uppercase, lowercase, numeric and alphanumeric characters) with mandatory regular changes (e.g. every 30 days) and enabling password history protection (e.g. disallowing to use former 12 passwords).

2.4.3 (Distributed) Denial of Service (DoS/DDos) Attack

Some organizations (banks, shopping sites, governmental organizations, educational organizations, etc.) rely on their web sites to provide their services to the customers or to the public, it is of great importance that their web services are always up and running, and these organizations build their web services capability to meet this requirement. When people type the URL for the organization's website into the browser, the user browser sends a request to the target website server to use the view the website service. Normally, the target website server is designed to answer only a limited number of concurrent requests. In this type of attack, the attacker floods the target web site with traffic more than it can handle, thus resulting the shutdown of the web site to all users. This is a "denial of service" because legitimate users can't access that site (McDowell 2013).

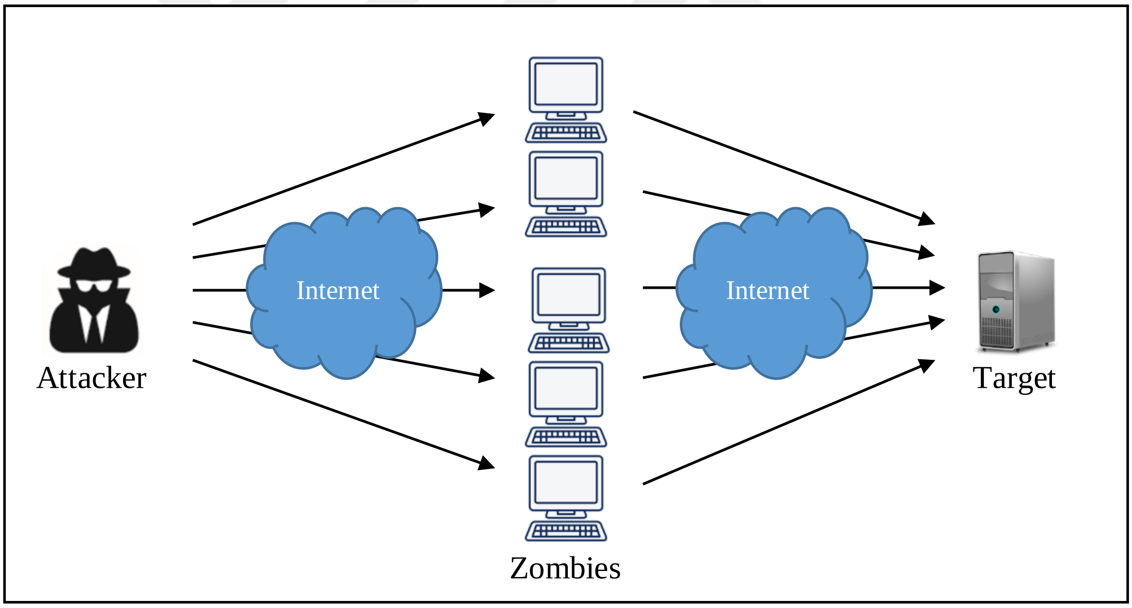
Figure 2.2: DoS Attack



Distributed Denial of Service (DDoS) Attack: In a DDoS attack, the attacker may use other computers to attack another target computer. By using the advantage of cybersecurity vulnerabilities or weaknesses, the attacker can take control of others' computers, these computers become so called zombies. The attacker then forces these zombies to produce large amounts of requests to a target victim website, or flood particular victim email addresses by sending spam emails. This attack is "distributed" since the hacker is utilizing multiple hosts, zombies, to facilitate the DoS attack (McDowell 2013).

Unusually slow network performance and unavailability of organization website could be signs of a possible DoS/DDoS attack against the organization website.

Figure 2.3: DDoS Attack



Countermeasures against DoS/DDoS Attack

There is no easy and efficient way to protect against this type of attacks. Implementing a technical solution for organizations would too complex and expensive. Optimum technical solution will be utilizing the DoS/DDoS protection service provided by the Internet Service Provider (ISP).

The measures that one should take to reduce the likelihood of becoming a zombie computer are (McDowell 2013):

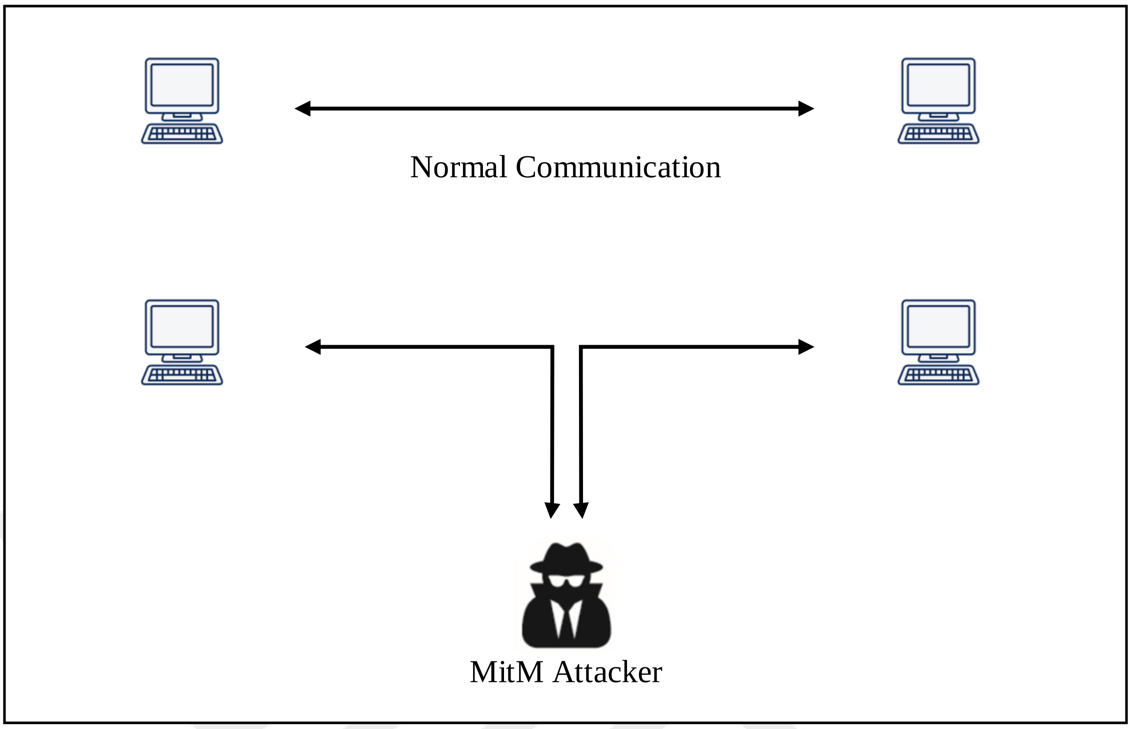
a. Install an antivirus software, keep it updated,
b. Implement a host firewall software, it should be configured to monitor and restrict incoming and outgoing traffic of the computer,
c. Apply proper security procedures and practices for advertising organizational official email address to reduce spam emails,
d. Apply e-mail filters.

2.4.4 Man in the Middle (MitM) Attack

This attack type is named after the basketball game, where two teammate players aim to pass the ball to each other but an opponent player gets in between and grasps the ball without prior knowledge of the two teammates. This type of attacks are among the commonly preferred methods utilized by cyber hacking community. This attack can also be used to facilitate some other attacks such as DoS attack or DNS spoofing. It is more convenient to perform MitM attack in a LAN, utilizing the ARP poisoning method. MitM attack can have several damages to its victims, such as, stealing several account credentials, stealing of local ftp, ssh or telnet sessions etc. (Nayak, G.N. & Samaddar, S.G., 2010).

In a computer network, every instance of network communication normally takes place between two legitimate parties. In the MitM attack, while the two parties believe that they are privately communicating each other during a private session, the attacker manages to intercept this traffic, and listens or, in some cases alters the information without knowledge of the legitimate parties.

Figure 2.4: Normal Communication vs. MitM Attack

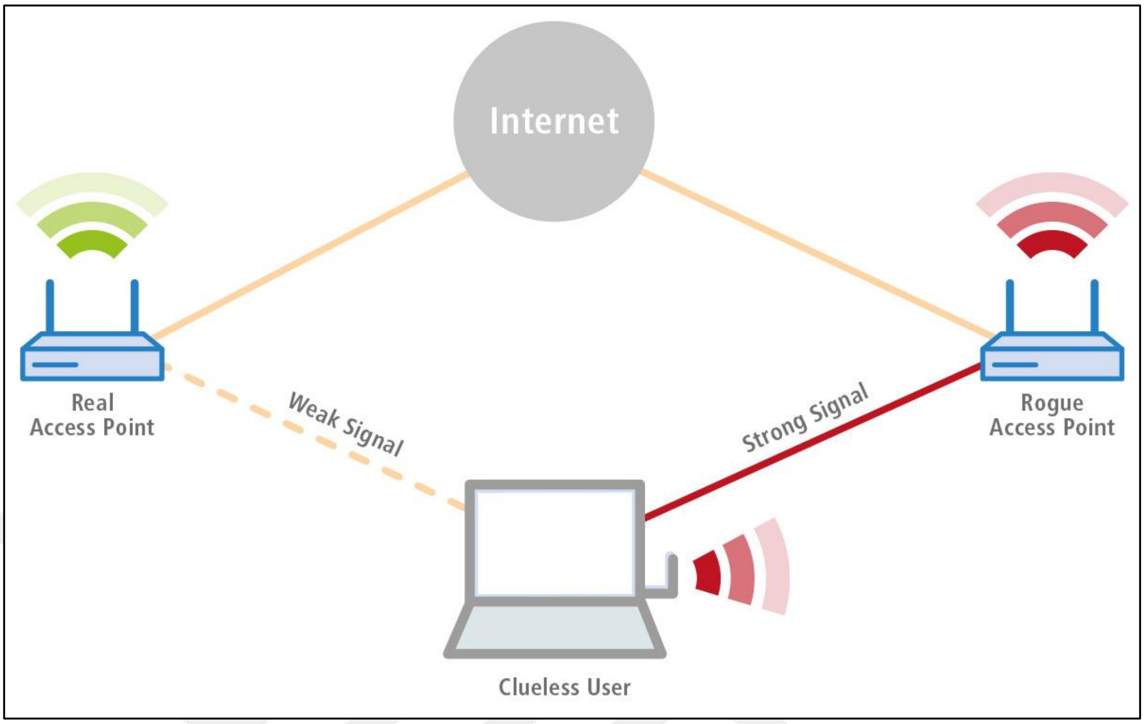


Man in the Middle Attack Types

Rogue AP: In a wireless network utilized cyber infrastructure, there will be wireless access point(s) installed to connect user workstation computers to the network. User devices with wireless ethernet cards mostly intends to automatically connect to the AP that has the strongest signal emitting capability nearby. Attacker may try to implement a rogue access point and deceive the devices in the vicinity to connect to itself. All of the user traffic can now be monitored, even altered to meet the attackers intend (Rapid7 LLC, no date).[6]

[6] Rapid7 LLC, [no date]. *What is a man-in-the-middle attack?*, [online]. https://www.rapid7.com/fundamentals/man-in-the-middle-attacks [accessed 14 Feb 2018]

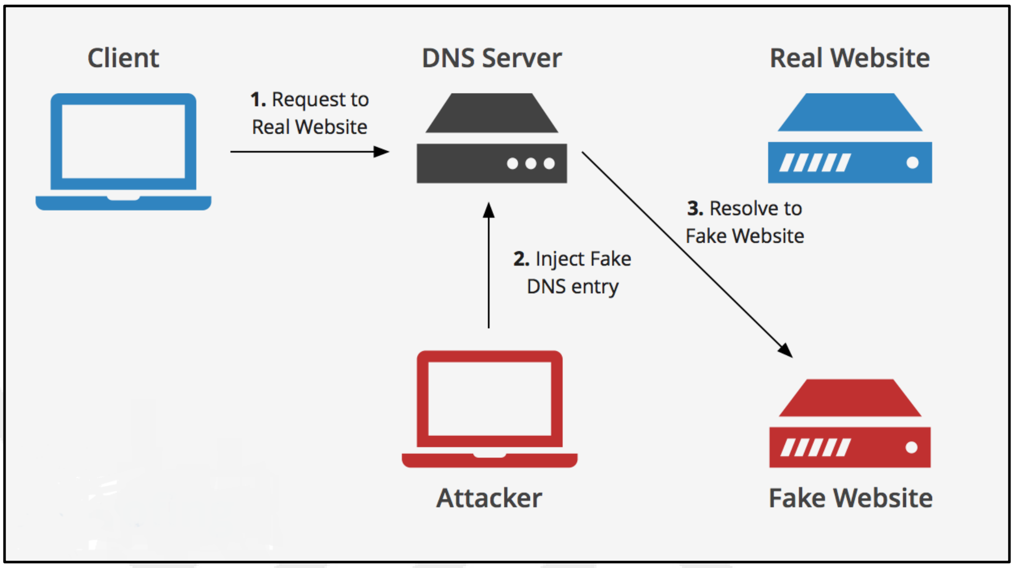
Figure 2.5: Rogue Access Point (Krebs 2015)



ARP Spoofing: Address Resolution Protocol is used to resolve IP addresses to physical MAC addresses in a LAN. If a host requires to communicate with another host with a specific IP address, it looks into its ARP table to resolve the IP address into a MAC address. If there is no corresponding IP address in the ARP table, the host broadcasts a request to the LAN and asks the MAC address of the host with the specific IP. An attacker intending to role as the target host with specific IP may respond to these type of requests, which should not be the case in normal network operation. Utilizing some fine-tuned and located packets, a non-legitimate person can listen to the network traffic between two legitimate hosts. Confidential data can be obtained from these network packets, such as credentials, yielding privileged access to user accounts that the attacker, normally, shouldn’t be able to access.

Domain Name Service Spoofing: Just like the ARP resolves IP to MAC address on a network, DNS converts domain names to the corresponding IP addresses. In a DNS spoofing attack, the attacker tries to send altered DNS address information to a victim host and tries to pose that the attacker computer has the authentic IP address for a legitimate domain site, like www.youronlinebanking.com. This gets the target victim host to start a session with attacking computer and transmitting sensitive information to the attacker, believing that it is sending the information to a legitimate target.

Figure 2.6: DNS Spoofing (Keycdn 2017)



Countermeasures against Man in the Middle Attack

It mostly very difficult to detect a man in the middle attack. For this reason, preventing from these types of attacks is always better than fixing the damage afterwards, because there are quite limited ways to detect these kind of attacks. Preferably, public (and/or free) networks should not be used to work on sensitive subjects (or even to control private e-mails). The best choice to use the public networks should for only basic requirements like checking the new; doing this, even if your traffic is intercepted by a MitM attacker, there will be very little or no damage at all (Hidayatullah 2010).

Implementation of strong WEP or WAP Encryption on APs: One of the best ways to prevent non-legitimate people from connecting and registering to the wireless network just by being close to the access point is to implement a strong encryption method on the access point. If there is a weak encryption mechanism implemented on the access point, an attacker may try to crack (brute force) into the network and start man in the middle attack. It is always better to implement a stronger implementation mechanism. (Rapid7 LLC, no date).[7]

Virtual Private Network: Another solution for preventing man in the middle attacks is to use the virtual private network (VPN). They use a key-based encryption method to create a tunnel for secure network traffic flow. Using such encrypted tunnels provide additional layers which will provide a secure access to the company's confidential network over unsecure links like WiFi. Using this method, even when an attacker manages to get in the network traffic, he won't be able to decrypt the packets in the VPN traffic. Additionally, companies should have proper process auditing and monitoring in place so that they are aware of their staff activities (Hidayatullah 2010).

Force HTTPS: Utilizing the public-private key exchange mechanism, the use of HTTPS protocol can provide secure communication capability over HTTP. Doing this, the data that an attacker may be sniffing will be useless to him. Organization websites should not provide both HTTPS and HTTP, they should only use HTTPS. User browsers in the organization can be set to enforce always using HTTPS.

[7] Rapid7 LLC, [no date]. *What is a man-in-the-middle attack?*, [online]. https://www.rapid7.com/fundamentals/man-in-the-middle-attacks [accessed 14 Feb 2018]

3. THE FRAMEWORK

There are several standards, guidelines, and ways of developing a cybersecurity for organizations. Some studies focus on the threats, some of them depend on risk assessment strategies, and some builds on available protection technologies. This study will develop the cybersecurity framework focusing on high level set of capabilities, which are basically phases of necessary actions to handle cybersecurity incident. This approach will cover the necessary capabilities before, during and after a cyber incident, thus will enable this framework to include all aspects of cybersecurity requirements in a more comprehensive method.

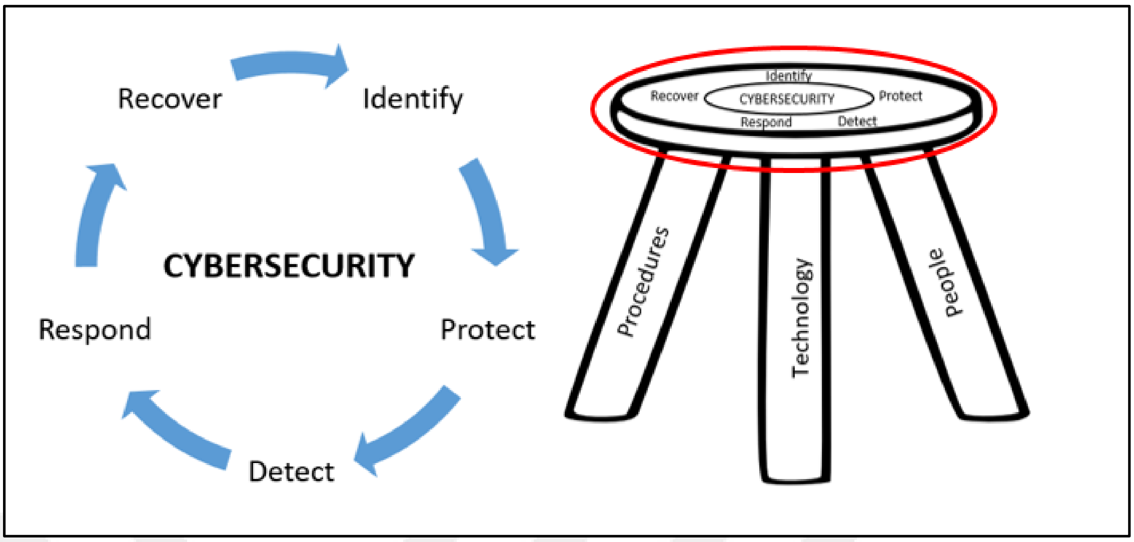
For every cybersecurity capability, the framework will cover;
Procedures: what actions are required and how it will be conducted,
Technology: which technological solutions can be applied,
People: who will be doing what in the organization.

3.1 CYBERSECURITY GOALS: THE CAPABILITIES

Developing a cybersecurity posture requires implementation of continuous set of capabilities at the highest level, procedures and functions needs to be designed to feed into these capabilities. NIST[8] (2014, p. 7) has identified five high level functions to organize basic cybersecurity activities. These capabilities can also be considered as phases of an organizational continuous cybersecurity capability (Figure 3.1).

[8] National Institute of Standards and Technology (NIST), Framework for Improving Critical Infrastructure Cybersecurity,2014, https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf [accessed 14 Feb 2018], p.7.

Figure 3.1: Cybersecurity Capabilities



Identify: Development of cybersecurity posture for an organization starts with identifying assets, systems, applications, data, organizational context, operational needs, risk to systems, and available resources. This phase helps the organizations to give answers to these questions; who are they, what do they have, what they want to protect and to what extent, what is their risk assessment, and what are their available resources.

Protect: After identification phase, the organization needs to develop protection capability which would enable the organization to protect the identified cyber assets against identified threats. This capability should focus on preventing or limiting possible cybersecurity events, and containing the incident should it happens inevitably.

Detect: No matter how much protection is implemented to prevent a cyber incident, the organization needs to develop the capability to timely monitor its cyber assets and detect possible cybersecurity events should they occur.

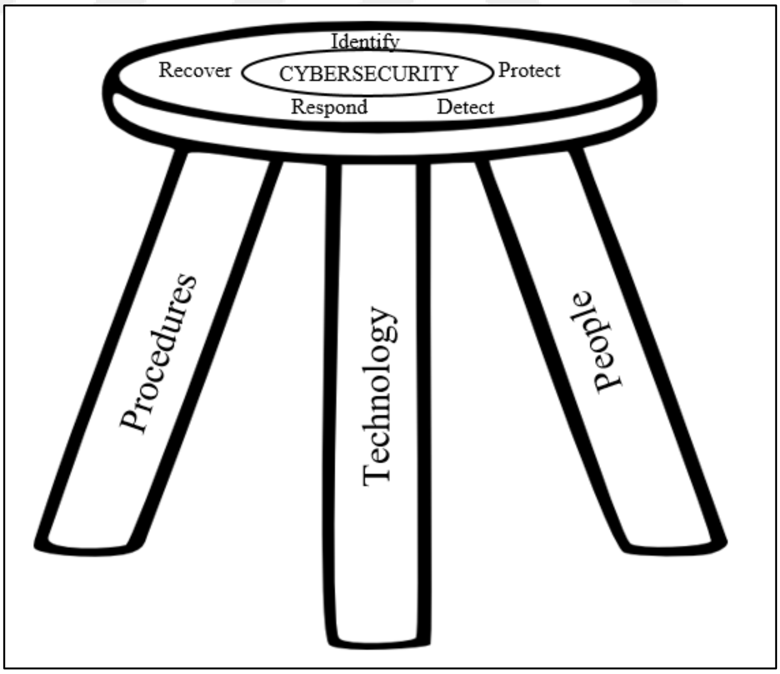
Respond: Organization needs to develop responding capability to implement necessary activities to react against a cybersecurity incident. Activities in this capability will enable the organization analysis the incident, and limit and contain the impact of the potential cybersecurity event to the organization.

Recover: Organization will develop plans and implement the necessary actions to restore any services which were affected due to a cybersecurity event back normal operation.

3.2 PILLARS OF CYBERSECURITY: PROCEDURES, TECHNOLOGY, PEOPLE

Technology, people, and procedures are main pillars of achieving a proper organizational cybersecurity posture. In order to develop and maintain the cybersecurity capabilities explained in this study, organizations must ensure combination of procedures, people and technology. These three main pillars can be illustrated as a three legged stool (Figure 3.2). As it can be seen on the figure, none of these pillars can be ignored, if one fails, cybersecurity fails.

Figure 3.2: Pillars of Cybersecurity (Merkow et al. 2014)



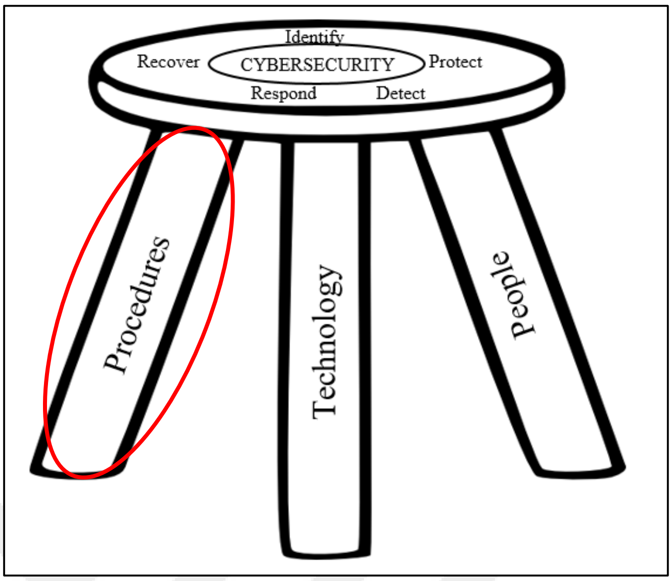
Technology, as the enabler of cyber environment, is the most reliable resource to provide information confidentiality, integrity and availability (Patsis 2013). However, organization should never solely rely on technological security solutions. Technology can fail, and without people to notice and fix technical problems, cyber systems would stop working permanently. As an example of this type of waste is implementing an expensive firewall system (a network perimeter security device that blocks traffic) and leaving it without proper configuration, opening all the ports that are intended to block certain malicious traffic from entering the network (Merkow et al. 2014). Another example is that, no cybersecurity technology can protect the organization if the users, or even administrators, ignore to keep the credentials (usernames and passwords) as safe as they should. Consequently, technology itself cannot be considered as a substitute for organizational cybersecurity.

People are essential to both business and cybersecurity lifecycles in an organization. Since people are the information owners, custodians, consumers and users, they need to be properly trained and motivated in all aspects of security. Human intelligence, the decision-making capabilities and the inquiring mind is inevitably required, but an organization should be able to add controls into all business processes to mitigate the risks human factor may bring, whether accidental or malicious (Patsis 2013). Unfortunately, human factor is always considered the weakest link in security chain, and most attacker still base their successful attacks relying on the people’s ignorance or lack of awareness.

Procedures are implemented to ensure that same operations can always be performed by different people in the same way. Processes are documented as procedures on how to perform a specific security related activity. An example is that the steps of configuring a server operating system to run securely is documented as one or more procedures so that administrators can use and can be sure that everything is done correctly (Merkow et al. 2014). Another example is that, a user should know the necessary security steps to take before plugging any USB stick into the organization network.

3.2.1 Procedures

Figure 3.3: "Procedures" Pillar of Cybersecurity



The development of internet and information technology have significantly influenced human life. However, information security still stands as source of concern for users and organizations. Technological solutions cannot solely ensure a secure environment for information; the human factor of information security should be taken into consideration along with the technological implementations. Reasons of common users' mistakes are lack of cyber security training and awareness, ignorance, negligence, misbehavior, and resistance. A decent organizational cybersecurity policy would aid the organization to shape and mitigate risks resulting from human factor (Safa et al. 2016).

Organizations need to develop and implement necessary procedures to achieve the desired cybersecurity posture for the organization. These procedures should aim to explain the activities to be performed to deliver a certain cybersecurity capability defined in this study. If necessary, especially for the technical ones, procedures should be further explained as detailed instructions to ensure that a specific procedure is done exactly same way no matter who the executer is.

An overview of the procedures defined for cyber capabilities are shown in the Table 3.1. As it is previously stated, it is important to keep in mind that, cyber threats are increasing and evolving every day, and security measures should increase and evolve as such. The procedures defined in this study cannot cover all current measures and cannot last forever. Organizations should take this framework as a living document and update as necessary.

Table 3.1: Procedures (NIST 2014)

CAPABILITIES	**Identify**	**Protect**	**Detect**	**Respond**	**Recover**
PROCEDURES	Organizational context	Access Control	Anomalies Detection	Response Planning	Recovery Planning
	Asset Management	Security Awareness and Training	Detective Technology	Communication & Coordination	Disaster Recovery Planning
	Risk Assessment	Data Security	Multiple Sensors Implementation	Analysis	Business Continuity Planning
	Governance	Maintenance	Continuous Cyber Security Monitoring	Mitigation	Improvements
	Framework Profile	Protective Technology	Detection Processes	Improvements	Communication & Coordination

3.2.1.1 Identify

The procedures provided in this capability are basis for effective utilization of the Framework. Understanding the organization's business context, the cyber assets that provide critical capabilities, and the assessed cybersecurity risks provide an organization with the ability to focus and prioritize its efforts to meet its strategic business requirements. Some examples procedures to provide this capability are as follows:

Organizational Context: Before initiating the development and implementation of a cybersecurity structure, it is important to know the organization, its context and goals, its organizational structure and how it manage its business. This covers the consideration of the internal and external issues that could affect organization's goals, objectives, and cybersecurity infrastructure. One important matter in this respect is the issues that could potentially have a cybersecurity risk to the organization’s business goals cyber systems. It is also important to consider the organization’s risk culture and appetite in order to properly design, implement and manage the cybersecurity within the organization. Organization personnel needs to understand that cybersecurity is an integrated part of business context, not a separate function, and it should be considered as a business enabler (Humphreys 2016).

Asset Management: Organization should identify and manage the organization data, employees, equipment, cyber systems, and facilities in accordance with their importance to organization’s business goals and the risk appetite (NIST 2014).

Procedures may include:

a. Physical devices, systems and equipment are inventoried,
b. Software and applications used by the organization are inventoried,
c. Organizational cyber network diagrams are available,
d. Organizational cyber assets (e.g., equipment, software, systems, applications, data) are prioritized in accordance with relative sensitivity and importance to the organization,
e. Security roles and responsibilities in the organization manpower are established.

Risk Assessment: Organization needs to understand the cyber risks to business strategic functions, reputation, cyber assets, and manpower. Threats, vulnerabilities, likelihoods, impacts should be identified, documented and used to determine risks, and risk responses should be identified and prioritized in accordance with organizational context and priorities (NIST 2014).

Governance: Cybersecurity roles and responsibilities should be coordinated and synchronized with internal and external stakeholders. Legal and regulatory requirements (organizational, national, and international) regarding cybersecurity, including privacy obligations should be understood, documented and managed.

Framework Profile: A framework profile is a modified version of this reference framework to fit organizational context, business requirements, available resources, and risk assessment. Detailed information on profile development is provided in 3.4 "FRAMEWORK PROFILE" chapter.

3.2.1.2 Protect

In order to deliver the Protection capability, organization should develop necessary procedures to provide the ability of limiting or containing the impact of a potential cybersecurity incident. Examples of procedures within this capability may include the following:

Access Control: Organization should limit the access to organization facilities and cyber assets to authorized users (NIST 2014).

Procedures may include:

a. Where appropriate, a layered physical security (perimeter, building, floor, room, etc.) is implemented to ensure that physical environment used to access to organization assets is properly managed and effectively protected.
b. User identities and credentials are managed for authorized devices and users.
c. If necessary, remote access control procedures should are identified.
d. Access control procedures are implemented in accordance with least privilege, need to know and separation of duties principles.

Security Awareness and Training: Different from the other lines of operation, security is the responsibility of every single individual in an organization. From the top (including executives and bosses), down to the very bottom of the organization, every individual can access to cyber assets that might pose a vulnerability and be source of a potential cyber incident. Top level executives mostly tend to be the first to behave against security principles because they believe they should not be limited. In many cases, it is this attitude which leads to a big security breach in the organization, but eventually it becomes the security people blamed at the end of the day. In most cases, the people at the bottom of the organizations (e.g. cleaners, facility maintenance people and workers) actually may have more physical access to facility rooms and organization cyber assets than many of the higher level staff; that' why, it is important that they are aware of the risks and potential attacks that could be based on scenarios involving them or their teammates. Attackers will preferably choose a target person with lower pay grade and utilize social engineering methods to advise him to gain unauthorized access to organization facilities or cyber assets. (Campbell 2016).

In order to change the staff behavior, the fastest and most effective way would be to train them by providing regular security induction and awareness trainings. It is important that every single organization staff attends this trainings, and trained on how they are supposed to respond and handle the situations that can potentially lead a security violation.

Data Security: It should be ensured that organization data is managed and protected in line with the risk assessment for the protection of the confidentiality, integrity, and availability of organization's cyber assets and data.

Procedures may include:

a. The data in rest and the data in transit is protected.
b. Procedures identify the security measures for cyber assets that hosts organization data, to include acquirement, operation, transfer, and disposition of the assets.
c. Data is created, used, stored, transferred and destroyed in accordance with the organization's information management policy.
d. Backups of data are regularly conducted and maintained, and periodically tested.

Maintenance: Procedures should be developed to ensure secure maintenance and repair operations of the organization cyber assets, in a logged and timely manner, and with approved and controlled tools. This includes the maintenance of physical facility assets. Special attention should be given to maintenance activities conducted by outsourced (external) contractors who conducts maintenance of security and safety systems, such as smoke alarms, HVAC systems, lighting, and CCTV equipment.

Protective Technology: Procedures for the design, implementation and operation of technological security solutions (identified in “Technology” chapter) should be developed to deliver the protection capability for the organization at network, host, application, and data levels.

3.2.1.3 Detect

The Detection capability provides the organization with the capability to timely detect and discover cyber incidents. It is to be understood that early recognition of an attack is key to early and effective respond. Procedures within this Capability include:

Anomalies Detection: Procedures should enable timely detection of anomalous activity and assessment of potential damage of the cyber incidents. A good practice would be to develop a baseline for normal network traffic activity and data flow for systems and organization users and to set alert thresholds to identify abnormal activity.

Detective Technology: Since detection process requires continuous monitoring, it is not possible to provide it with manpower, especially for small and medium size organizations who would not have enough resources to implement a Security Operations Center. For this reason, it is better for them to implement proper detection technologies and applications to provide automatic detection capability.

Multiple Sensors Implementation: It is always better to collect and correlate incident data from multiple sources and detectors. Detected cyber incidents will need to be analyzed to understand attack targets and methods, thus enable to understand the impact of the incident. Technologic solutions (i.e. Security Information and Incident Management-SIEM) can support the detection and analysis efforts in a centralized approach.

Continuous Cybersecurity Monitoring: In order to verify the effectiveness and efficiency of the protection measures and to identify cybersecurity incidents, organization cyber systems and assets should be continuously monitored or randomly checked (NIST 2014).

Procedures may include:

a. Monitoring the network to detect cybersecurity incidents,
b. Monitoring the physical environment to detect cybersecurity incidents,
c. Monitoring the employee activity to detect cybersecurity incidents,,
d. Monitoring the service provider traffic to detect cybersecurity incidents,
e. Monitoring unauthorized individuals, connections, hosts, and applications to detect cybersecurity incidents,
f. Detection of potential harmful code,
g. Scanning messages for abnormal pattern (signature) or behaviors,

Detection Processes: In order to provide timely and sufficient awareness of abnormal events, detection procedures should be developed and tested (NIST 2014).

Procedures may include:

a. Organization should identify detection roles and responsibilities to provide accountability,
b. Developed detection activities should be tested to verify effectiveness,
c. Organization should communicate event detection data with proper parties, to include the stakeholders inside and outside the organization,
d. Detection processes should be continuously improved.

3.2.1.4 Respond

The Respond Capability provides the organization with the ability to contain the impact of a potential cybersecurity event. Examples of procedures within this Capability include:

Response Planning: Response processes and procedures should be developed, tested and maintained before a cyber incident occurs, to ensure that the organization can properly and timely respond to a detected cybers events.

Communication and Coordination: Organization should communicate response activities with internal/external parties as necessary. It may incorporate external coordination with governmental law enforcement entities.

Procedures may include:

a. Personnel should be informed and trained on their duties and response steps when there is a response needed,
b. Events should be recorded and reported in accordance with the predefined criteria,
c. Incident information should be communicated in accordance with the response plans,
d. Incident should be coordinated with internal/external stakeholders as identified in the response plans,

Analysis: Cyber event should be analyzed to enable sufficient response and to support the recovery phase efforts.

Procedures may include:

a. Assessment is conducted for the alerts from sensors and detection assets,
b. Identification of the impact of the event is completed,
c. Cyber forensics activities are conducted,
d. Events are categorized in accordance with developed response plans.

Mitigation: Organization should ensure necessary steps actions are taken to prevent spreading of an attack, mitigate its damage to organization cyber assets, and finish the event. If the organization has identified new vulnerabilities, they should be mitigated appropriately or the risks should be considered and registered as accepted.

Improvements: Lessons learned activities should be conducted after each incident to include current and past incidents to improve organizational response capability. These lessons learned should be integrated to update the organization's response plans.

One important note here is that, if penetration tests are used to test the organization's cybersecurity team's ability to detect and respond to incidents, they should not be punished when a vulnerability or breach is discovered. This can seriously demotivate the team, so instead this should be used as a learning experience, asking yourself why did this happen and what can be done to remediate the breach and stop it from happening again (Campbell 2016).

3.2.1.5 Recover

The Recover Capability supports timely recovery to normal operations to reduce the impact from a cybersecurity event. In severe attack scenarios, business survival may depend on this capability. Examples of procedures within this Capability include:

Recovery Planning: Organization should recovery develop plans to provide recovery processes and procedures to timely restore cyber systems and turn back to normal business operations after responding a cyber incident.

Some of the procedures may include the following:

a. Most of the time, recovery involves the administrator returning systems to their pre-incident state, such as restoring systems from backups, that restore system access and network access and ensure that the business can go back to pre-incident status.
b. In cases where multiple desktop systems are affected by malware, such as during a malware or ransomware outbreak, administrators may choose to perform a clean installation of the standard operating environment (operating system and standard applications) since it would be quicker to do this than try to deal with a contaminated system. The reason is that it is very hard to guarantee the malware has been fully erased, because some infections are intelligent enough to hide

multiple copies of themselves and could remain undiscovered for weeks or even months without detection.

c. Administrators need to find the best way to recover from each of incident categories (lessons learned would be helpful) and ensure that the technical mechanisms are in place to allow those recovery processes to work, it would be useless to say recovery will be done from backups if the backup system hasn't worked for the last couple of months (Campbell 2016).

Disaster Recovery Planning: Despite all measures taken, some systems of the organization may be disrupted or failed due to an attack or an environmental event (power cut, communication lines outage, etc.). Properly identified procedures would support timely recovery of affected services by, for instance, utilizing alternate power source, switching to backup communication lines or activating a disaster server.

Business Continuity Planning: In some cases, due to a natural or environmental threat (such as earthquake, fire, flood, etc.) or an extreme incident, systems may become unrecoverably disrupted. In such cases, critical services that keep the business up and running can be moved to a BCP site (maybe in the cloud) and whatever considered critical business functions continues to work at an acceptable level (Campbell 2016). BCP implementation mostly requires additional funding. BCP planning should be considered as part of risk management to assess the threat and vulnerability depending on the organization context.

Following steps can help to develop a BCP procedure:

a. Identify the assets that is critical and require to be available during the incident

b. Design the methods, techniques and system that will be needed to protect the organization

c. Test and validate all of the procedures and systems within the plan

d. Communicate the details of the plan to all staff

Improvements: Lessons learned activities should be conducted after each incident to include current and past incidents to improve organizational recover capability. These lessons learned should be integrated to update the organization’s recovery plans.

Some of the procedures may include the following:

a. Forensic log is created to explain how the incident was handled,
b. Closure report is created which analyses and quantifies the effectiveness of each stage of the Recovery Plan and considered all aspects of the methods, techniques, methodologies, and findings relating to this incident,
c. Lessons learned are integrated in the recovery plans,
d. Recovery plans are updated as necessary.

Communication and Coordination: Recovery activities should be communicated with internal/external stakeholders, such as organization managers, ISPs, managers of identified or potential attacking systems, identified or potential victims, vendors, national authorized CERTs (if necessary).

Some of the procedures may include:

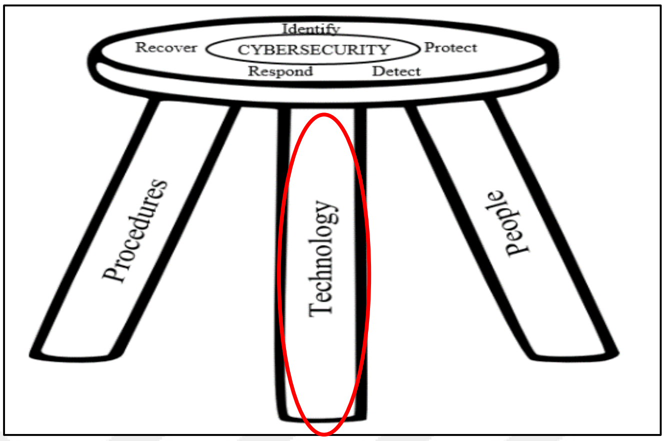
a. Management of public affairs,
b. Restore of organization’s reputation following a cyber incident,
c. Recovery actions are coordinated within the organization, to include related staff including executive level.

3.2.2 Technology

It should be noted that there are lots of security technologies produced in the market, but the problem is to identify what their functionalities are and where they fit in a cyber infrastructure. When it comes to small and mid-size organizations, since they usually do not have cyber experts employed, it becomes more difficult for them to figure out which solutions they really need to invest with their limited knowledge and resources.

This section explains the “Technology” pillar of cybersecurity capabilities. In the section, in order to explain technological solutions and functions of the products, first, some example architectures will be studied, then how they fit in The Framework will be explained and finally main functions of each technology will be provided.

Figure 3.4: "Technology" Pillar of Cybersecurity



It is important to state that, in this study, the term "technology" refers both the hardware and software solutions developed to deliver specific security functions for cybersecurity implementation.

Depending on the organization's business context and needs, there can be different types of cyber structure implementations. Figure 3.4 represents an example small-size company cyber structure, Figure 3.5 and Figure 3.6 represent medium size company cyber structures (Osborn et al. 2017).

Figure 3.5: Sample Small-Size Company

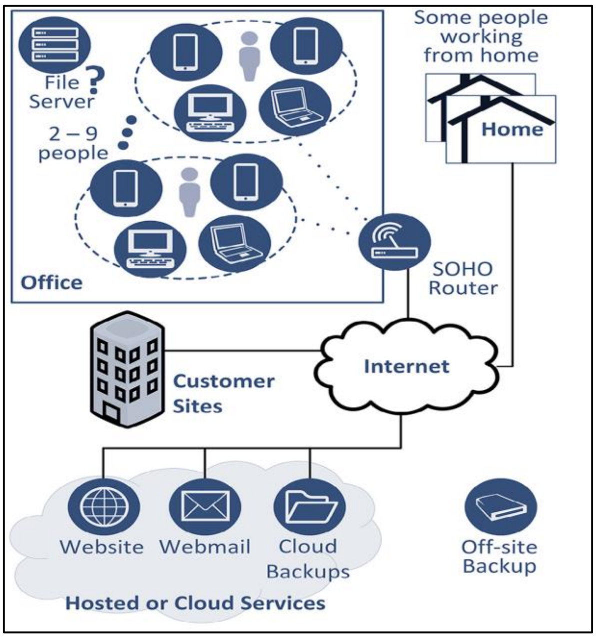


Figure 3.6: Sample Medium-Size Company Network (Osborn et al. 2017)

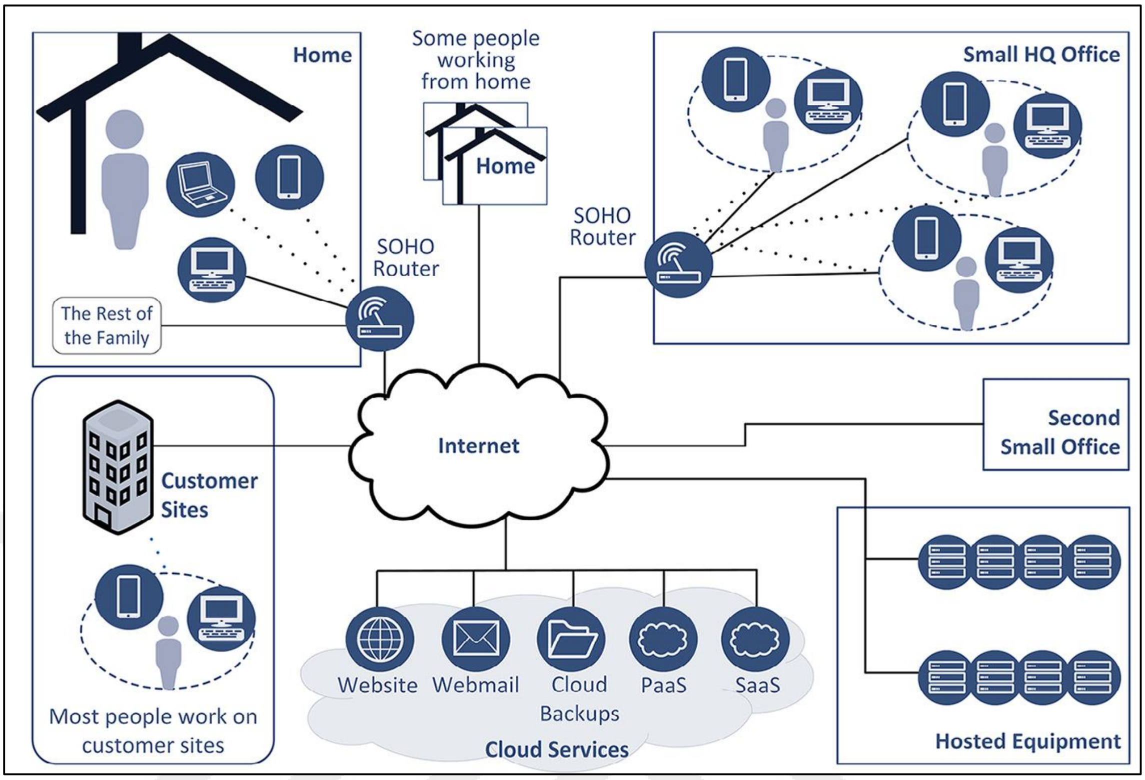
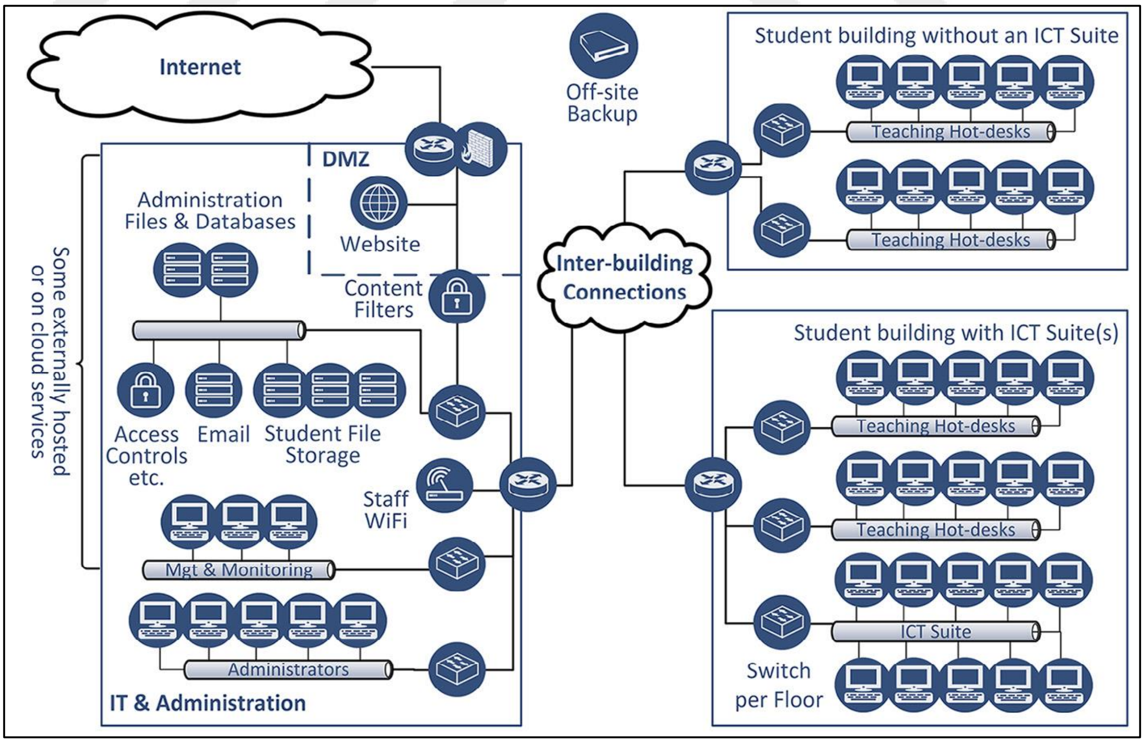
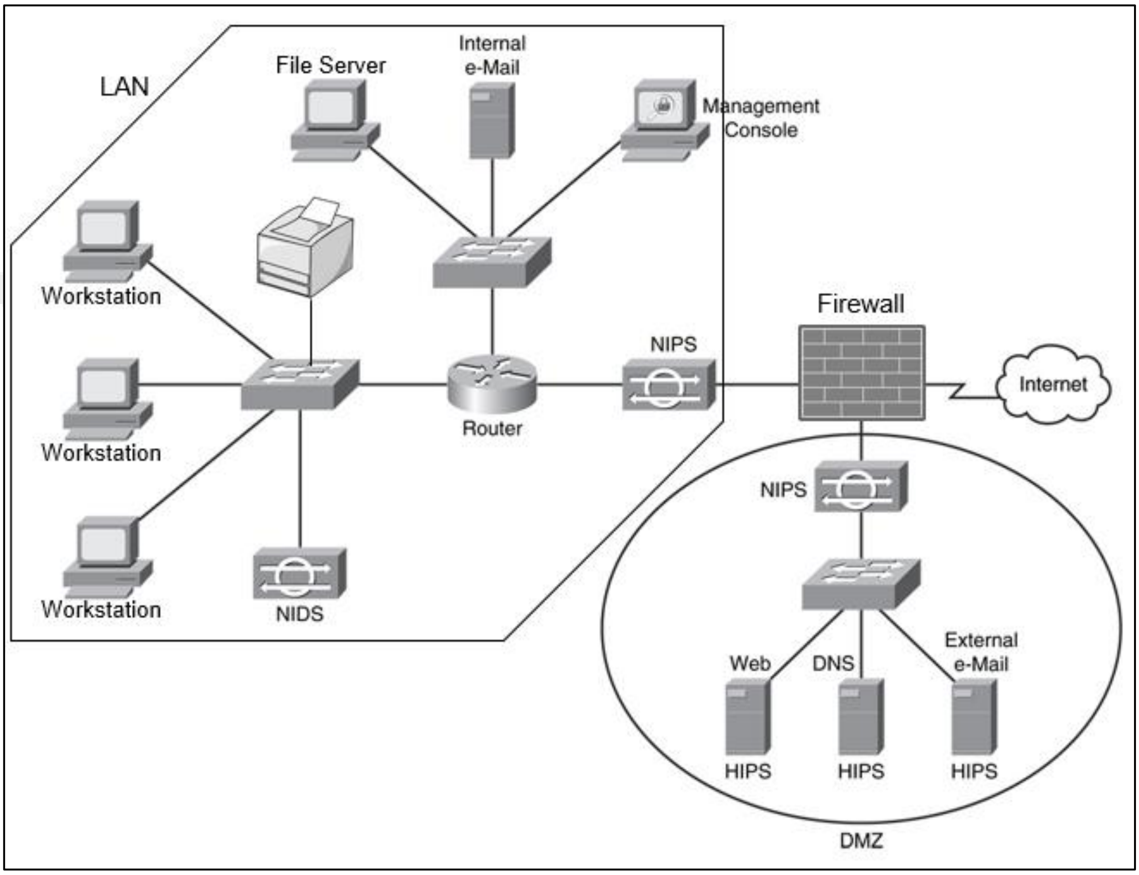


Figure 3.7: Sample Medium-Size Company Network (Osborn et al. 2017)



In addition to example company networks above, a sample reference cyber network in Figure 3.8 can be used to explain how the cybersecurity technologies are positioned in a network.

Figure 3.8: Sample Reference Cyber Network

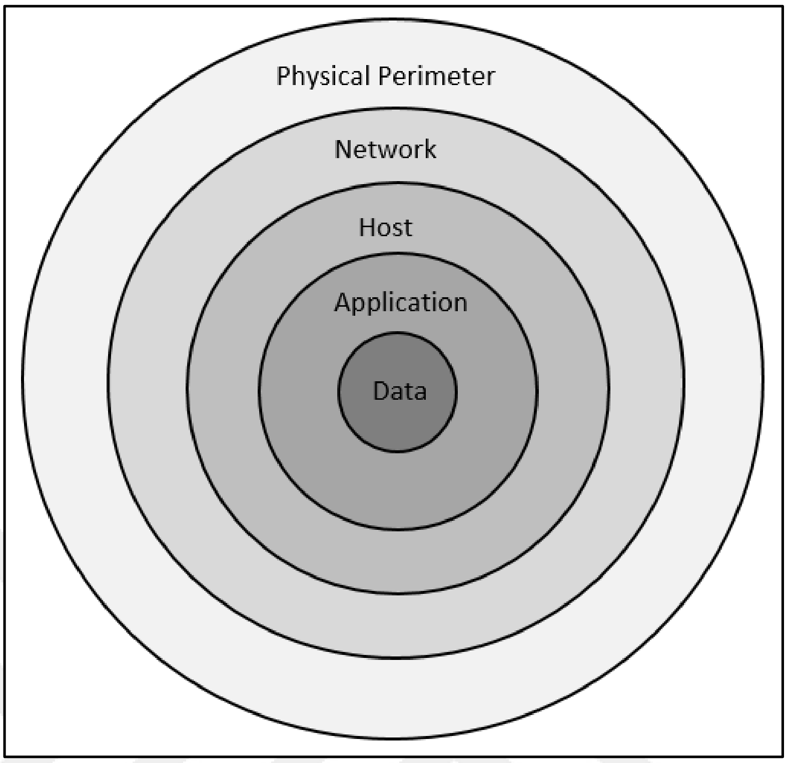


According to the sample structure, an organization would have an internal local area network (LAN) and hosts on this LAN where there are services to be used by the organization internally. This LAN would be connected to internet and there would be components to provide necessary cybersecurity functions to the organization.

3.2.2.1 Layered Approach

To better understand the technological solutions, technology components will be analyzed in a layered approach as shown in Figure 3.9.

Figure 3.9: Layered Approach to “Technology” Pillar



Data Layer: This layer addresses organization data which can be in several formats depending on the applications used by the organization.

Application Layer: Organization data is processed by applications to meet organization requirements. Examples of applications would include operating systems, financial management applications, human resources applications, word processing utilities etc.

Host Layer: Organization data is processed by applications which reside on several types of host. Some example hosts are servers, workstations, datastores, printers, etc.

Network Layer: There is a cyber network which connects the organization hosts to each other and to the internet as necessary.

Physical Perimeter Layer: Physical infrastructure and its security components, such as barriers, fence, guards, turnstile, CCTV, fire alarm, etc.

3.2.2.2 Technologic solutions

In this section, technologic cyber security solutions will be explained which can be implemented against cyber threats. The aim is not to include all technology available on the market, only most common well-known ones will be listed. The main goal is to explain which solutions can be used to meet which “Capability” aimed in this framework, as seen at Table 3.2.

Table 3.2: Cybersecurity Technologic Solutions

CAPABILITIES		Identify	Protect	Detect	Respond	Recover
TECHNOLOGY	Data Layer	File Management tools, Content Management Services	Encryption, classification, DLP, Access Control, Antivirus	DLP, Antivirus	Antivirus, Antimalware, Data wiping cleansing	Backup & Restore
	Application Layer	Change Management, Service Management	Antivirus, Update/Patch, Application whitelisting, Hardening	Database monitoring, SIEM	Antivirus, Antimalware, Log Analysis, Update/Patch	Backup, Re-installation, Re-configuration,
	Host Layer	Inventory tools	Antivirus, Host Firewall, HIPS, HIDS, Hardening, Hard drive encryption	Antivirus, HIPS, HIDS, SIEM	Antivirus, Antimalware, Log Analysis, Update/Patch, Cyber forensics	Re-installation, Re-configuration
	Network Layer	Network reconnaissance/ discovery/monitor tools	Firewall, IPS, DMZ, VPN, network device hardening, encryption	IDS, IPS, Firewall, Log management, SIEM	IPS, Log Analysis	Configuration Backup & Restore Alternative Communication Means
	Physical Perimeter	Access Control ID Management Tools, Authorized Personnel badge, visitors’ badge,	Barrier, Fence, Lock, Lighting, Security Guards, Security Dogs, Air-condition, UPS	Sensors, CCTV, Breach Alarm Systems, Fire Detection, Intrusion Detection Systems,	Fire Extinguisher, UPS, Air-condition	Equipment Repair, Movement to Alternate site

Antivirus/Antimalware: The use of antivirus software is one of the basics to provide cybersecurity for computers. These applications are designed to detect and eliminate malicious software (such as virus, worm, trojan horse, ransomware, etc.) from harming the computer. Once installed, first, a complete scan is conducted, then continuous monitoring is done by antivirus software. Although there are several commercial and free solutions, it is always better to implement a trusted and reputable one. What is important at this point is that, antivirus programs have a database of signatures of known malware, and, in order to identify if a file is a virus or not, the antivirus program compares the file against this database. Consequently, keeping this signature database up to date is what makes an antivirus program effective. Another issue to consider is that, comparing every file against the signature database may have negative effect on computer performance, but there are antivirus solutions implementing algorithms to provide efficient performance. As result, best antivirus solution can be found triangulating cost, signature database effectiveness and performance efficiency.

Data Loss Prevention (DLP): DLP systems are software applications used to protect organization's confidential information from being lost, improperly used or reached by unauthorized parties. Normally, DLP aims to prevent organization information shared by organization personnel, unintentionally or maliciously. DLP applications monitor and manage endpoint traffic, additionally the data flowing on the organization network (Lord 2017).

Firewall: Main function of firewalls is to isolate and control the flow of traffic between networks. They provide a security control point in the network where administrators can choose what will pass and what will be blocked. Firewalls also provide a real time logging of every permits and blocks they do, which can be used as triggers of alarms for attacks, which may enable the administrators manage the incident and detect the attacker at the network layer. These can also be used for post attack analysis to understand what happened (Campbell 2016).

Intrusion Detection System (IDS): IDS monitors the network traffic and seeks for abnormal activity and warns the system or network administrator. Sometimes, the IDS may also react to suspicious or malicious traffic by reacting the detection, as blocking the user or source IP address from accessing the network.

One type of IDS, signature-based IDS, checks the packets on the traffic and analyses it comparing them against a signature database which is composed of already known malicious codes. This way, it works like the way most antivirus software detects malware.

Another type of IDS, anomaly-based IDS, checks the network traffic and compares it against an identified behavior baseline. This baseline identifies what the “normal” traffic is for that network, what is the bandwidth mostly used, which are the usually used protocols, which ports and hosts commonly in communication with each other, and warns the administrator when a suspicious traffic is detected which looks anomalous, or considerably different than the established baseline.

A passive IDS, is the one which simply detects and alerts. If an anomalous or malicious network flow is detected, the passive IDS generates an alert and send it to the administrator, so that the administrator decides to react to block the traffic or respond in another way.

Different from a passive IDS, reactive IDS doesn’t only provide detection of abnormal or harmful traffic and warn the administrator, it also takes pre-defined reactions against the identified threat. Mostly this will mean to block network traffic from the originating IP address or the user (Bradley 2018).

Network Intrusion Detection Systems (NIDS): NIDS are implemented at a strategic point(s) in the organization network to monitor all inbound and outbound traffic of all devices. In ideal conditions, a NIDS is configured to scan all inbound and outbound traffic but doing so can have a drawback of causing a bottleneck and slowing down the network speed (Bradley 2018).

Host Intrusion Detection Systems (HIDS): While NIDS are located on network, HIDS are located on hosts on a network. The HIDS check the network packets to and from the implemented hosts only and warns the user or system admin if it detects something abnormal.

Intrusion Prevention System (IPS): An IPS is a network security and threat prevention device that analyzes network traffic to detect and prevent exploit of possible vulnerabilities. IPS is normally located behind a firewall to provide a complementary function of security. While an IDS is a passive system that aims to detect threats and notify the user or the administrator, an IPS provides the function to actively analyze the traffic and react as necessary. As the reaction, the IPS may only warn the administrator (like an IDS would), drop the identified malicious packet, or block the traffic from the malicious address. At this point, it is important that the IPS is capable of detecting and responding accurately, to effectively eliminate threats while preventing false positives (non-malicious packets misanalysed as malicious).

Host Intrusion Prevention System (HIPS): A HIPS is implemented on hosts and works similar to an IPS, actively analyzes host traffic to detect and prevent cyber-attacks when necessary.

Firewall vs. IDS vs. IPS: To clear out any confusion, the main functions and differences are:
A firewall is the first line of defense at perimeter network which denies all incoming traffic by default and only allows the necessary ones (http. Exchange, ftp, etc.) as defined in “rules”, but doesn’t analyze if the allowed traffic has malicious content.

An IDS monitors the traffic allowed by the firewall, and alerts the administrator if detects a malicious packet, further action is taken by the administrator.

An IPS can be considered as a firewall with network and application level filtering, which also functions as a reaction capable IDS, proactively protecting the network. The IPS analyzes packets on traffic and can take actions against any detected malicious packets.

It is obvious that with development of new technologies, firewall, IDS and IPS will take on more functionalities from each other and blur the line between them.

Unified Threat Management (UTM): Recently, vendors are producing UTM devices which are beneficial to meet security requirements of small and mid-size organizations. UTM systems integrate various network security capabilities (firewall, IDS, IPS, etc.) which are normally delivered by separate devices. In addition to integrating different functions, most of the UTM solutions also provide sandboxes at the network layer. A sandbox is a specially controlled mirror of the operating systems used within the cyber environment (not managed by the internal administrators) that the UTM can use to run potential malware samples, capturing each of the attempts it takes and then determine what damage it might do (Campbell 2016).

Security Information and Event Management (SIEM): With the implementation of security measures on several cyber assets (computers, servers, firewalls, IDSs, IPSs, etc.) there will be lots of alerts and information produced by these sensors. Security events require a level of analysis, either automatic or by a trained analyst to make sense of the information and use it to detect potential threats. SIEM allows the cyber people collect all alerts and information, thus monitor the environment at one location, and make the information meaningful for further action. If an event or alarm is detected which serves as an indicator of compromise, then the incident management process can be initiated.

The Demilitarized Zone (DMZ): One of the most well-known and implemented cybersecurity architecture is the demilitarized zone (DMZ). This is actually not a single device, but a special network segment dedicated to providing security between two networks. As seen on Figure 3.8 reference network, common usage is to position the DMZ between the trusted organization network, LAN, and the untrusted internet (WAN). The firewall would have its WAN interfaces configured to face the untrusted network, filtering unwanted traffic and only allowing certain protocols through into the DMZ. The devices in this zone provide a variety of special security functions, such as content filtering, malware scanning and intrusion prevention, thus trapping any discovered malicious connections or content before they have a chance to reach the internal network (Campbell 2016). Another important use of the DMZ is that, positioning external business services (i.e. such as web server, mail server, ftp server, etc.) in the DMZ. By doing this, external requests requiring connection to these organization services will never be able to go to internal network, instead they will be directed to the servers hosted in DMZ, and these servers will be protected by several security solutions.

File Encryption: File encryption provides access to a file only by people who knows the encryption password. This makes is extremely difficult for a hacker to break into files and access sensitive organizational information. File encryption functionality can be provided embedded operating systems, if not, third party (even free) programs are available.

Hard drive encryption: This method encrypts the whole data on a hard drive. The data on hard drive is only accessible when the computer is logged in by an authorized user. It is an effective and commonly used security method to protect sensitive information against asset (computer/laptop) loss or theft.

Backup: No matter what security measures are implemented, it is always a threat that organization data somehow may become corrupted or unavailable, and without proper backups, organizations may face to force extreme and expensive ways to recover the data. Although there are several highly functional third-party backup solutions, small size organizations can also effectively utilize backup functions provided operating systems.

Updates/Patches: Operating systems (OS) and software applications vulnerabilities are prime targets for malicious software writers and OS and application writers are continuously developing updates and patches to eliminate vulnerabilities. That's why, it is very important that OS updates are conducted properly. Even a fully updated system is at some risk, but the risk is considerably less than a system that is not updated. Easiest method is to leave the “Automatic Updates” on unless there is a constraint, such as confliction with a special application used by the organization. Procedures should also include the patching of application software which may have newly discovered vulnerabilities.

Hardening: Hardening is a term coming from metallurgy, which means rendering a material to make it stronger and more resistant. It has the same meaning in cyber security, configuring cyber assets to make them more resilient. Hardening is actually, in general terms, implementing security. What is important here is to remind the organizations that one of the preferred targets of attackers are default configured cyber assets, such as, printers, scanners, switches, routers, etc. While most of the security measures on computers are commonly known, hardening on printers (disabling web service, etc.) is mostly overlooked. It is very common that attacker utilize a vulnerability on a network printer and find a way to infiltrate other devices such as computers or servers. IT people should keep in mind that every cyber asset can be configured to make it and the enterprise network more secure. Hardening guides can be found on product documentation or on website for most devices.

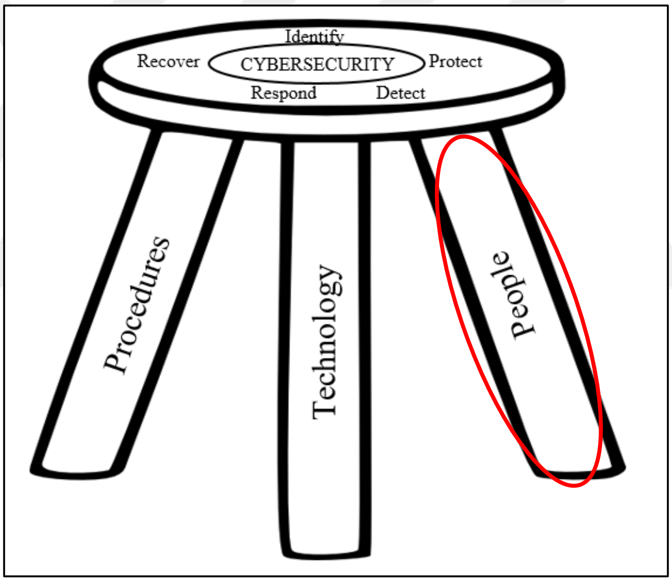
Virtual Private Network (VPN): VPNs are used to establish secure connections over unsecure networks, such as the internet. It provides secure remote connection capability: a person can work as if inside the enterprise network while physically located elsewhere. For example, if the organization requires to enable some employees to remotely connect to organization network and execute duties, a VPN solution could be implemented. Some main methods of implementing VPNs are Point to Point Tunneling Protocol (PPTP), Layer 2 Tunneling Protocol (L2TP), and Internet Protocol Security (IPSec). Depending on the preferred method, implementation requires configuration on network devices (such as firewall, router) and computers.

Device Whitelisting: This will prevent users from reading or writing to devices attached to their cyber devices (removable media, printers, etc.), unless they are specifically authorized to do so. The system can be configured so that users cannot read or write to USB connected flash drives unless they are identified clerks who have been trained in the company’s import and export procedures. Device control can reduce the risk posed by the “autorun” features in operating systems.

Application Whitelisting: This refers to technologies used to prevent users from running unauthorized applications and codes on computers. The philosophy is that, all applications are considered as black (insecure), and only the authorized ones considered as the white (secure). This is very strong protection mechanism as it stops users installing unauthorized applications on the systems. Furthermore, if malware somehow gets installed on the system, it cannot execute because of the application control policy. The Windows operating system comes with a built-in application whitelisting feature called AppLocker.

3.2.3 People

Figure 3.10: "Technology" Pillar of Cybersecurity



People is one of the most important pillars of cybersecurity for organizations, especially for small and medium size organizations (Figure 3.10).

Unfortunately, every cyber system, no matter how well it is designed is vulnerable to attacks if the people using it or managing it make mistakes. Cybersecurity people need to consider the manpower as just another business asset that needs to be considered when developing security mechanisms. People, like cyber systems, have their own weaknesses (vulnerabilities) and are subject to threats and attacks just like anything else (Campbell et al. 2016).

Since small organizations are not expected to be capable of implementing high level and complex cybersecurity technologies, trained and aware personnel will play a key importance at securing the business. Although it is a widely accepted phenomenon that people are the weakest link of the security chain, small and medium sized organizations should use the size of the organization as an advantage by developing and implementing proper procedures and maintain a decent level of cybersecurity.

When looked at today’s cyber related roles and responsibilities in organizations, it could be seen that there are several roles and responsibilities under different names. In order to make it easier to understand for small and medium size organizations, the organization will be studied in less number of roles as much as possible as seen at Table 3.3.

Table 3.3: Cybersecurity Roles

Some Roles in Cyber Society:	Roles in this Study:
a. IT Management b. System Manager c. Designer d. Administrator e. Security Director f. Chief security officer g. Chief information security manager h. Information security manager i. Information risk manager j. Incident Handling Officer k. Forensics Analyst l. Operational security manager m. Digital forensics analyst n. eDiscovery expert o. Security architect p. Penetration tester q. Security requirements manager	a. Business Manager: Decision maker, budget owner, risk owner, the boss. b. IT Manager: Cyber services manager, this role may not exist in small size organizations. c. IT Administrators: Daily operation of cyber services d. Users: Consumers of cyber structure

Business Manager: Depending on the size of the organization, this may be a person (boss, CEO, etc.) or a group of people (executive board, etc.). This is where the organization strategic decisions are made, risk is managed, and resources are distributed. Special attention should be given to the training and awareness of management level people, because these users tend to insist on having some privileges on the IT system, and, unfortunately, privileged and ignorant users are the most beloved targets for attackers.

IT Manager: This is the person who is responsible of the management of the organizational cyber services, cybersecurity will be one of his/her responsibilities. This position may not exist in small sized organizations.

IT Administrators: Administrator are responsible for the daily operation of the cyber services. They are also responsible of the implementation of security measures defined by the IT manager.

An important note here is that, since IT managers and administrators are privileged users of the cyber structure, it is important that additional security measures are taken for these people, such as, conducting background checks before employment, establishment of "separation of duties" principle (a task is conducted by at least two or more people).

Users: Users are authorized consumers of the cyber structure. Training and awareness of users plays a critical role in the organization security. Regular trainings and random checks should be conducted to keep the awareness level at maximum. Although most of the small and medium size organization do not need to implement data classification procedures, "need to know" and "least privilege" principles should be implemented at a minimum. Need to know principle is allowing a user access only to the information needed to perform his/her duties, least privilege principle is granting a user with a level of access rights not above what is required to perform the duties.

3.3 THE OUTPUT: REFERENCE FRAMEWORK

After studying Framework Capabilities and Pillars, it can be concluded to come up with a Reference Cybersecurity Framework matrix (Table 3.4). This can be considered as a starting point and a guidance for organizations in order to see the big picture and to comprehend what procedures and technologies are available.

Table 3.4: Reference Cybersecurity Framework Matrix

Reference Cybersecurity Framework						
CAPABILITIES		**Identify**	**Protect**	**Detect**	**Respond**	**Recover**
PROCEDURES		Organizational context	Access Control	Anomalies Detection	Response Planning	Recovery Planning
		Asset Management	Security Awareness and Training	Detective Technology	Communication & Coordination	Disaster Recovery Planning
		Risk Assessment	Data Security	Multiple Sensors Implementation	Analysis	Business Continuity Planning
		Governance	Maintenance	Continuous Cyber Security Monitoring	Mitigation	Improvements
		Framework Profile	Protective Technology	Detection Processes	Improvements	Communication & Coordination
TECHNOLOGY	Data Layer	File Management tools, Content Management Services	Encryption, classification, DLP, Access Control, Antivirus	DLP, Antivirus	Antivirus, Antimalware, Data wiping cleansing	Backup & Restore
	Application Layer	Change Management, Service Management	Antivirus, Update/Patch, Application whitelisting, Hardening	Database monitoring, SIEM	Antivirus, Antimalware, Log Analysis, Update/Patch	Backup, Re-installation, Re-configuration,
	Host Layer	Inventory tools	Antivirus, Host Firewall, HIPS, HIDS, Hardening, Hard drive encryption	Antivirus, HIPS, HIDS, SIEM	Antivirus, Antimalware, Log Analysis, Update/Patch, Cyber forensics	Re-installation, Re-configuration
	Network Layer	Network reconnaissance/ discovery/monitor tools	Firewall, IPS, DMZ, VPN, network device hardening, encryption	IDS, IPS, Firewall, Log management, SIEM	IPS, Log Analysis	Configuration Backup & Restore Alternative Communication Means
	Physical Perimeter	Access Control ID Management Tools, Authorized Personnel badge, visitors' badge,	Barrier, Fence, Lock, Lighting, Security Guards, Security Dogs, Air-condition, UPS	Sensors, CCTV, Breach Alarm Systems, Fire Detection, Intrusion Detection Systems,	Fire Extinguisher, UPS, Air-condition	Equipment Repair, Movement to Alternate site

3.4 FRAMEWORK PROFILE

As stated earlier, this is not one-size-fits-all framework, it is flexible, and organizations should adapt it to meet their business needs. A framework profile is the adjusted (and approved by the management) version of the reference framework to fit organizational context, business requirements, available resources and risk assessment.

Framework profile development is basically filling in the cells (Table 3.5), in other words, identifying what technologies and procedures will be implemented to meet which of the five main capabilities to meet organization requirements. The “cells” which are not applicable to the organization can be greyed out (i.e. an organization located on a plaza building would not require physical perimeter measures such as walls, fences).

Table 3.5: Sample Framework Profile

<table>
<tr><th colspan="7">Cybersecurity Framework Profile for …….…….... Company</th></tr>
<tr><th colspan="2">CAPABILITIES</th><th>Identify</th><th>Protect</th><th>Detect</th><th>Respond</th><th>Recover</th></tr>
<tr><td colspan="2" rowspan="5">PROCEDURES</td><td>Organizational context</td><td>Access Control</td><td>Anomalies Detection</td><td>Response Planning</td><td>Recovery Planning</td></tr>
<tr><td>Asset Management</td><td>Security Awareness and Training</td><td>Detective Technology</td><td>Communication & Coordination</td><td>Disaster Recovery Planning</td></tr>
<tr><td>Risk Assessment</td><td>Data Security</td><td>Multiple Sensors Implementation</td><td>Analysis</td><td>Business Continuity Planning</td></tr>
<tr><td>Governance</td><td>Maintenance</td><td>Continuous Cyber Security Monitoring</td><td>Mitigation</td><td>Improvements</td></tr>
<tr><td>Framework Profile</td><td>Protective Technology</td><td>Detection Processes</td><td>Improvements</td><td>Communication & Coordination</td></tr>
<tr><td rowspan="5">TECHNOLOGY</td><td>Data Layer</td><td>File Management tools</td><td>Access Control, Antivirus</td><td>Antivirus</td><td>Antivirus, Antimalware</td><td>Backup & Restore</td></tr>
<tr><td>Application Layer</td><td>Change Management</td><td>Antivirus, Update/Patch, Hardening</td><td>Database monitoring</td><td>Antivirus, Antimalware, Update/Patch</td><td>Backup, Re-installation, Re-configuration,</td></tr>
<tr><td>Host Layer</td><td>Inventory tools</td><td>Antivirus, Host Firewall, Hardening</td><td>Antivirus</td><td>Antivirus, Antimalware, Update/Patch,</td><td>Re-installation, Re-configuration</td></tr>
<tr><td>Network Layer</td><td>Network reconnaissance/ discovery/monitor tools</td><td>Firewall, VPN</td><td>IDS, Firewall, Log management, SIEM</td><td>IPS, Log Analysis</td><td>Configuration Backup & Restore Alternative Communication Means</td></tr>
<tr><td>Physical Perimeter</td><td>Personnel badge, visitors' badge,</td><td>Fence, Lock, Lighting, Air-condition, UPS</td><td>CCTV, Fire Detection,</td><td>Fire Extinguisher, UPS, Air-condition</td><td>Equipment Repair</td></tr>
</table>

One of the main responsibilities of the IT manager would be designing and managing of the framework profile. IT manager should consider all the pieces of this framework, and design the optimum achievable profile to meet business needs. The aspects which may affect the framework profile design are; size and structure of the organization, business industry, size of the cyber structure, number of people, physical location and environment, available resources, strategic priorities, risk assessment.

Risk management will be one of the main drivers to design the framework profile. Below are some basics steps of risk management procedure (Refsdal et al. 2015):

1. Risk Identification: All threats and vulnerabilities that may affect the organization are identified.
2. Risk Analysis: During this phase, probability and impact analysis is conducted for every identified threats and vulnerabilities. At the end of this stage, likelihood ratings (rare, unlikely, possible, almost certain, etc.), impact ratings (insignificant, minor, major, catastrophic, etc.), and overall risk ratings (low, medium, high, etc.) are identified.
3. Risk Treatment and Security Controls: Depending on the overall risk rating, organization may decide to avoid the risk (risk elimination), accept the risk (tolerate), reduce the risk (minimize, mitigate), or transfer the risk (3rd party), and implement a proper security control, among physical, procedural or technical security controls.

Table 3.6 shows a sample risk management study organizations may utilize.

Table 3.6: Sample Risk Assessment Table

Threat	Vulnerability	Likelihood	Impact	Risk Rating	Risk Treatment	Security Control
Malware	Unpatched system	Unlikely	Minor	Medium	Eliminate	Patch the system
Hackers	No webserver firewall	Possible	Major	High	Minimize	Implement FW software
Hackers	Web Server DDoS protection	Almost certain	Major	High	Transfer	DDoS protection service from ISP
Flood	Server room in basement	Unlikely	Major	Medium	Minimize	Communicate with facility management, request additional drainage system

Another philosophy to consider during framework development is Defense in Depth strategy. Defense in Depth philosophy aims to implement multiple, overlapping technologies and procedures rather than implementing a single security solution. These overlapping protection measures target different aspects of security, such as protection against insider threats and against technical attacks. Protection solutions should also overlap in a way that eliminates any single point of failure. Looking at the reference network at Figure 3.7 it can be noticed the implementation of a NIDS, a NIPS, and a HIPS. All three of these mitigation solutions monitor for malicious traffic and can generate a warning or drop such packets. However, these solutions are deployed at different locations in the network structure to secure different areas of the network. This overlapping yet diversified security is an example of the Defense in Depth design philosophy.

3.5 FRAMEWORK GOVERNANCE

Once organizations develop and implement the cybersecurity framework, it is important that it should be continuously be governed as part of the business processes. Framework can be governed at three layers in the organization, it can two layers if it is a small size organization:

Medium size organizations:

a. Business Management
b. IT Management
c. IT Operations

Small size organizations:

a. Business Management
b. IT Management/Operations

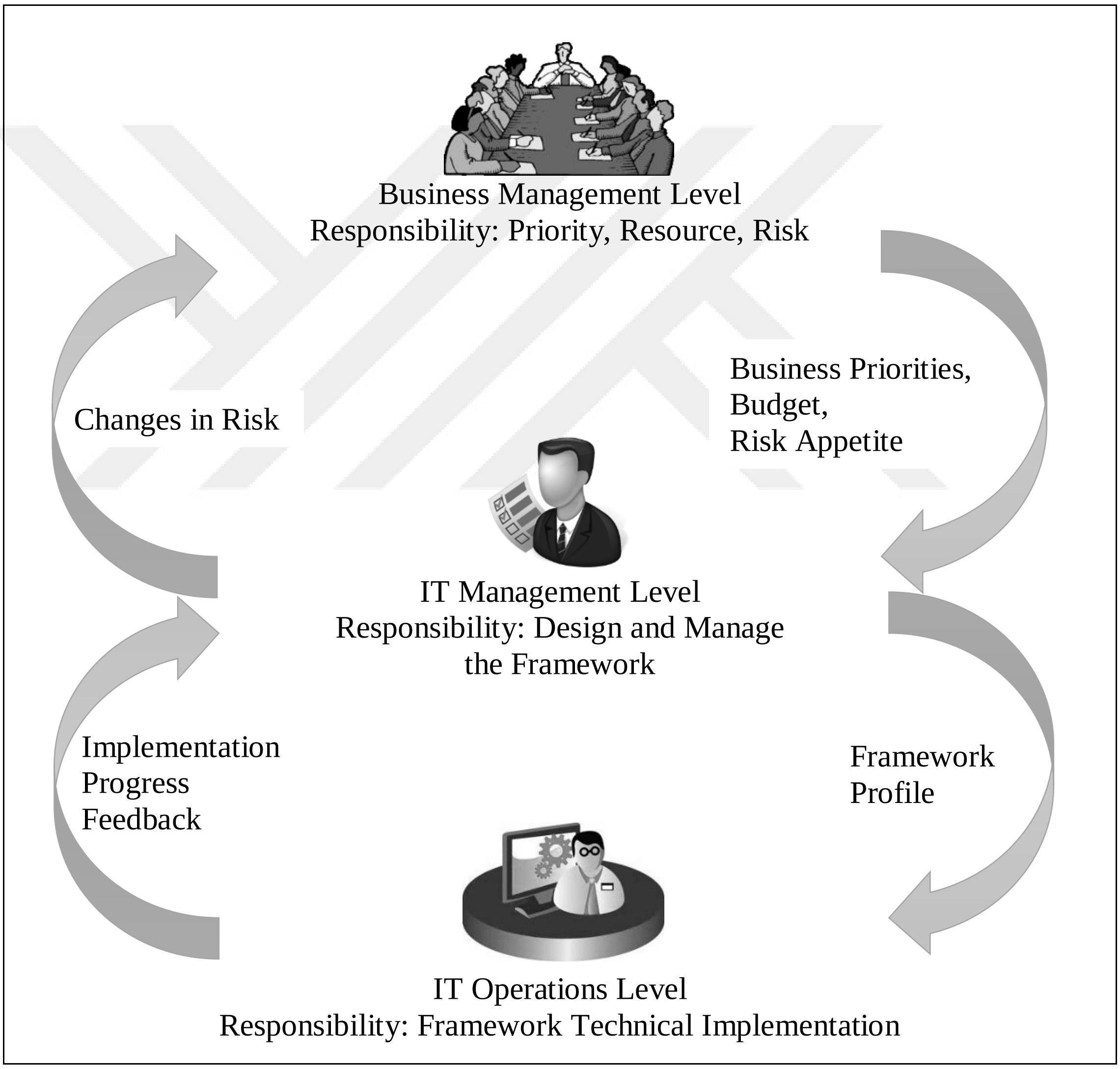
Figure 3.11 represents a common flow of framework governance within an organization.

Business Management: Depending on the size of the organization, an executive board, a CEO or the company owner (the boss) has the role of defining business priorities, available resources, and overall risk appetite. Additionally, these should be refined depending on the changes in the risk identified by IT management.

IT Management: IT management designs, develops, and manages the appropriate framework profile which fits the priorities, budget and risk appetite set by business management. Framework should be monitored and, if necessary, updated according to feedback from IT operations level regarding the implementation of the framework.

IT Operations: At this level, the framework profile designed by IT management is technically implemented by IT administrators. Any positive or negative feedback should be provided to IT management in order to have the framework profile adjusted if necessary.

Figure 3.11: Framework Governance in the Organization



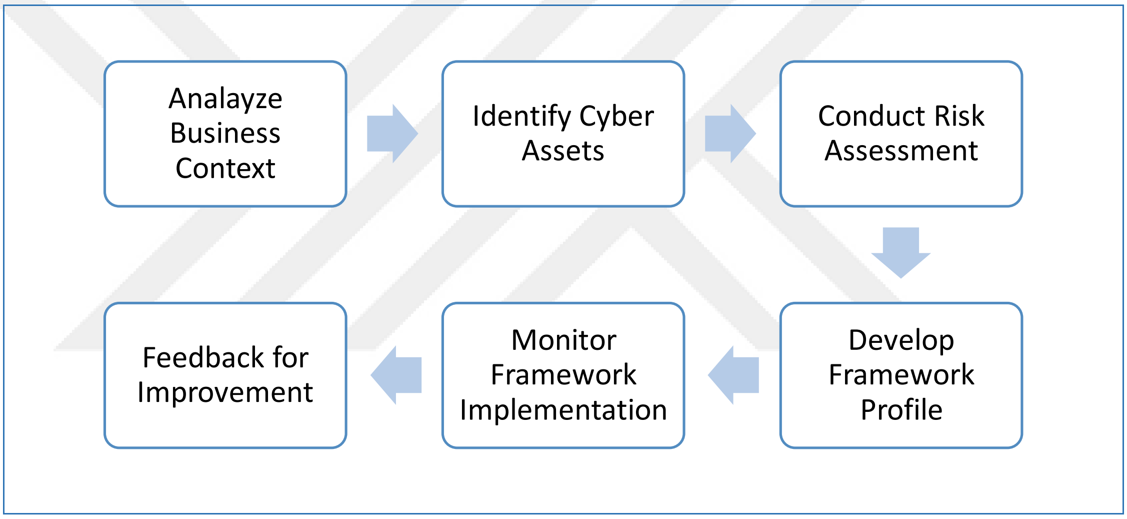
Business Management Level
Responsibility: Priority, Resource, Risk
Business Priorities,
Budget,
Risk Appetite
Changes in Risk
IT Management Level
Responsibility: Design and Manage the Framework
Implementation
Progress
Feedback
Framework
Profile
IT Operations Level
Responsibility: Framework Technical Implementation

Source: National Institute of Standards and Technology (NIST), Framework for Improving Critical Infrastructure Cybersecurity,2014, https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf

3.6 FRAMEWORK IMPLEMENTATION

As defined earlier, IT manager/administrator is the key person to design, implement and manage the framework. He/she will be the main responsible person to design, implement and maintain the framework. Although the content of the framework profile may differ depending on the business context, size, and risk assessment, steps to framework implementation for a generic small and medium size enterprise is shown at Figure 3.12.

Figure 3.12: Framework Implementation Steps


Analayze Business Context
Identify Cyber Assets
Conduct Risk Assessment
Develop Framework Profile
Monitor Framework Implementation
Feedback for Improvement

3.6.1 Analyze Business Context

As the first step, the IT manager should analyze and document the business context considering:

a. Business industry

b. Organization size

c. Organization structure and number of people

d. Physical location, facility perimeter, building, rooms

e. Environmental and natural conditions

f. Available resources

g. Business strategic priorities

3.6.2 Identify Cyber Assets

Cyber assets need to be identified to include:

a. Cyber Structure
b. Network Diagrams, connection profiles
c. Inventory of servers, workstations, mobile devices, peripheral devices
d. Inventory of software and applications
e. Organization data and sensitivity (classification) levels

3.6.3 Conduct Risk Assessment

Considering the organization context, cyber assets, potential threats, strategic priorities and available resources, a basic risk assessment should be conducted as explained in Chapter 3.4.

3.6.4 Develop Framework Profile

Considering the outcomes of previous steps, the IT manager should adjust the Reference Framework, include/adapt necessary parts, discard unnecessary parts and build the Framework Profile that fits the organization, as explained in Chapter 3.4.

3.6.5 Monitor Framework Implementation

Once the Framework Profile is developed and approved by the organization management, implementation process should be monitored by the IT Manager. Cybersecurity Implementation Dashboard at Table 3.7 enables the IT manager easily to monitor how the framework is implemented, what parts are missing, and what further improvements can be done. Implementation dashboard can also be used as a part of executive presentation to simply explain the organization managers what has been done, what needs to be done, and justify why additional resources are required to improve the framework.

Color codes are used to enable easy understanding of the table. When cells are filled in with corresponding colors, the dashboard will provide an overall status of framework implementation. Explanations of color codes as indicated in table legend are:

Implemented: The security measure is implemented as designed in framework profile.

Partially implemented: The security measure identified in framework profile is partially implemented, needs improvements.

Not implemented: The measure identified is not implemented, work is ongoing or awaiting additional resource.

Not to be implemented: The security measure is not to be implemented, either because it is not approved by the management (due to lack of resource, business continuity is expensive) or because it is not applicable due to organization context (perimeter fence will not be needed if organization is located on a floor of a business building).

It is obvious that greener in the maturity table will mean more security is provided. An example maturity table is provided at Table 3.7

Table 3.7: Sample Cybersecurity Implementation Dashboard

Cybersecurity Implementation Dashboard for ………………… Company

CAPABILITIES		Identify	Protect	Detect	Respond	Recover
PROCEDURES		🟩 Organizational context	🟧 Access Control	🟥 Anomalies Detection	🟩 Response Planning	🟩 Recovery Planning
		🟥 Asset Management	🟧 Security Awareness and Training	🟩 Detective Technology	🟧 Communication & Coordination	🟥 Disaster Recovery Planning
		🟩 Risk Assessment	🟥 Data Security	🟧 Multiple Sensors Implementation	🟥 Analysis	🟥 Business Continuity Planning
		🟩 Governance	🟩 Maintenance	🟧 Continuous Cyber Security Monitoring	🟩 Mitigation	🟧 Improvements
		🟩 Framework Profile	🟩 Protective Technology	🟧 Detection Processes	🟧 Improvements	🟧 Communication & Coordination
TECHNOLOGY	Data Layer	🟧 File Management tools	🟩 Encryption, classification, DLP, Access Control, Antivirus	🟩 DLP, Antivirus	🟩 Antivirus, Antimalware, Data wiping cleansing	🟧 Backup & Restore
	Application Layer	🟩 Change Management, Service Management	🟧 Antivirus, Update/Patch, Application whitelisting, Hardening	🟧 Database monitoring	🟩 Antivirus, Antimalware, Log Analysis, Update/Patch	🟩 Backup, Re-installation, Re-configuration,
	Host Layer	🟩 Inventory tools	🟧 Antivirus, Host Firewall, HIPS, HIDS, Hardening, Hard drive encryption	🟩 Antivirus, HIPS, HIDS, SIEM	🟧 Antivirus, Antimalware, Log Analysis, Update/Patch, Cyber forensics	🟩 Re-installation, Re-configuration
	Network Layer	🟩 Network reconnaissance/ discovery/monitor tools	🟧 Firewall, IPS, DMZ, VPN, network device hardening, encryption	🟥 IDS, IPS, Firewall, Log management, SIEM	🟧 IPS, Log Analysis	🟧 Configuration Backup & Restore Alternative Communication Means
	Physical Perimeter	🟩 Access Control, Authorized Personnel badge, visitors' badge,	🟩 Fence, Lock, Lighting, Security Guards, Air-condition, UPS	🟧 CCTV, Fire Detection,	🟩 Fire Extinguisher, UPS, Air-condition	🟥 Equipment Repair, Movement to Alternate site

🟩 Implemented 🟧 Partially Implemented 🟥 Not Implemented

The Greener The Better!!!

3.6.6 Feedback for Improvement

Cybersecurity is not an end state to achieve but a business enabler to be included in continuous organization processes. IT Managers should continuously monitor the implementation, stay alert for any deficiencies, consider any feedback available, and integrate if necessary. Any changes in business context, risk assessment, threats, physical environment and available resources should be communicated with executives and incorporated in the Framework Profile. There is always room for improvement, IT managers should always look for opportunities to improve the cybersecurity posture of the organization.

4. FRAMEWORK IMPLEMENTATION SAMPLES

This chapter provides sample framework implementations basing on different organizational scenarios. Scenarios will follow the framework implementation steps explained in section 3.6.

4.1 SCENARIO-1

This scenario will explain development and implementation of the cybersecurity framework for a mid-size company. The company is an IT company which provides consultancy and training services to its customers.

4.1.1 Analyze Business Context

a. Business industry: Company is in IT service industry. It does not sell IT goods or products, but provides consultancy support to its customers. It also has training facilities and provides several level IT trainings to customers or trainees.

b. Organization size: It can be considered as a mid-size company considering its number of employees, facilities, business relations and annual income.

c. Organization structure and number of people: The company has 55 employees; 3 executive level people, 2 executive assistants, 3 personnel in administrative management department, 2 in financial department, 2 security/reception personnel, 8 IT experts providing consultants to customers, 17 IT trainers, 18 IT outsourced experts employed as consultants or trainers when necessary. The company also hosts up to 80 trainees on its premises during course times.

d. Physical location, facility perimeter, building, and rooms: The company is located on a building of its own, on a street at the city center where there other business building next to it. The building has 5 floors, 1st floor as the entrance and reception, 2nd floor management offices, 3rd floor IT consultant and trainer offices, 4th floor hosts four training classes 20 trainee capacity per class, 5th floor as cafeteria. There are several security cameras operating in the building floors. Building entrance has a strengthened door which is locked after working hours. Office rooms are provided with standard door locks. Server room is equipped with air conditioner, fire system and UPS, and has a secure door, with door lock and fingerprint authentication.

e. Environmental and natural conditions: There are frequent power cuts in the region due to high consumption, the company utilizes power generator and UPS system to prevent power issues. Being located in a crowded business area, building fire risk is assessed as high. Flood risk is medium, and earthquake risk is assessed as high.

f. Available resources: Due to IT expert employees, the company has good manpower and knowledge resource to provide cybersecurity capability. The company can spare enough budget for reasonable cybersecurity investments.

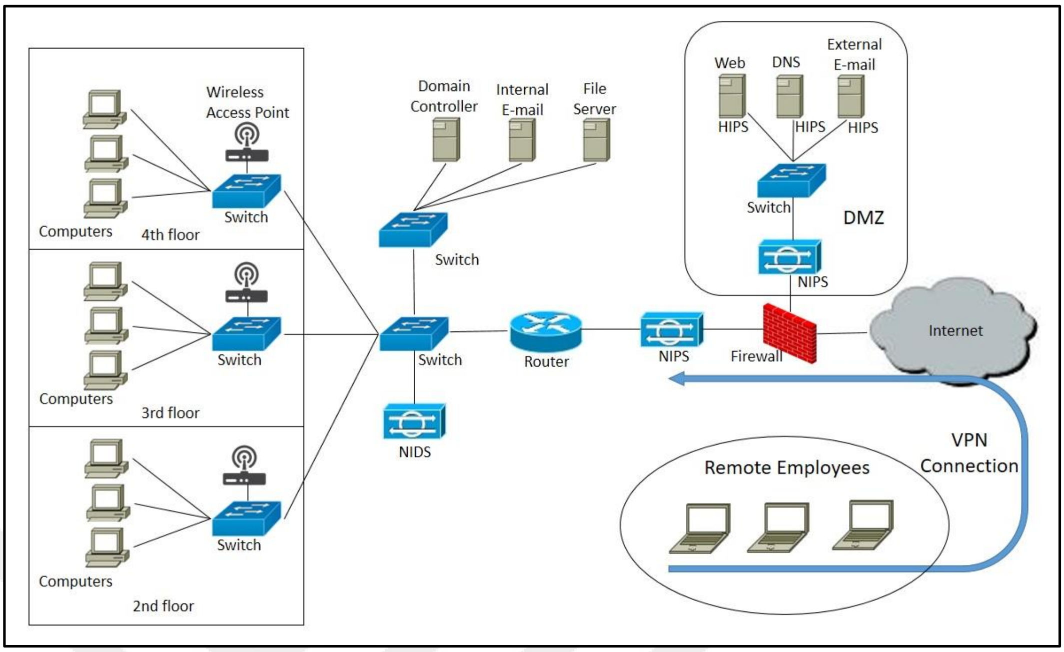
g. Business strategic priorities: Main priority for the company is to provide consultancy to its customers and to conduct training for trainees. Although cybersecurity is not the main priority, maintaining a decent level an organizational cybersecurity is aimed to meet company goals.

4.1.2 Identify Cyber Assets

a. Cyber Structure: Company has a LAN to provide IT services, with several servers, and switches and wireless access point for the connection of computers in each floor. Company hosts its own web server and e-mail server on its network in a safe DMZ. The network is connected to the internet behind a firewall. There are also laptops used by company consultants remotely connecting the company network via VPN connection.

b. Network Diagrams, connection profiles: Company network diagram and connections are provided in Figure 4.1.

Figure 4.1: Scenario-1 Company Network Diagram



c. Inventory of servers, workstations, mobile devices, peripheral devices: Company cyber inventory is prepared to include servers (physical/virtual), computers, mobile devices, peripheral devices, switches, routers, wireless equipment, and security devices (firewall, IPS, IDS, etc.)

d. Inventory of software and applications: Software and application inventory is prepared to maintain updates, upgrades and to provide license management.

e. Organization data and sensitivity (classification) levels:

i. Confidential: Confidential information of other firms/organizations which are provided consultancy by the company. Company financial data, documentation and agreements.

ii. Restricted: Training material and documentation.

iii. Unclassified: Non-sensitive information which can be shared with customers or trainees.

4.1.3 Conduct Risk Assessment

Risk assessment table is utilized for the identification and analysis of threats, vulnerabilities, likelihood and impact of threats, risk rating. After the analysis, risk treatment and security controls to be applied are identified. Risk assessment table for Scenario-1 company is provided at Table 4.1.

Table 4.1: Scenario-1 Risk Assessment Table

Threat	Vulnerability	Likelihood	Impact	Risk Rating	Risk Treatment	Security Control
Remote consultant connections	Company consultants remotely connecting the company network	Likely	Major	High	Eliminate	Implement VPN solution for the remote connection of the consultants.
Trainee access to confidential information	Trainees can access company network	Likely	Moderate	Medium	Eliminate	Trainee workstations to be installed on a separate training VLAN.
Frequent power cuts in the region	Company services needs to run 24/7	Almost certain	Major	High	Eliminate	Implement power generator for the whole building, and UPS for the critical servers and computers.
Malware	Unpatched system	Unlikely	Minor	Low	Eliminate	Patch the system
Hackers	Company web site is hosted on company web server	Unlikely	Major	Medium	Minimize	Web server in DMZ, behind a firewall and HIPS implemented.
Hackers	Web Server DDoS protection	Almost certain	Major	High	Transfer	DDoS protection service will be procured from Internet Service Provider
Storm, Rain, Flood	Server room damage	Unlikely	Moderate	Medium	Minimize	Server room is on 3rd floor, no threat is assessed due to flood. Room windows to be strengthened against storm, rain.

4.1.4 Develop Framework Profile

Framework profile for the Scenario-1 company is provided at Table 4.2.

Table 4.2: Framework Profile for Scenario-1 Company

Cybersecurity Framework Profile for Scenario-1 Company						
CAPABILITIES		**Identify**	**Protect**	**Detect**	**Respond**	**Recover**
PROCEDURES		Organizational context	Access Control	Anomalies Detection	Response Planning	Recovery Planning
		Asset Management	Security Awareness and Training	Detective Technology	Communication & Coordination	Disaster Recovery Planning
		Risk Assessment	Data Security	Multiple Sensors Implementation	Analysis	Business Continuity Planning
		Governance	Maintenance	Continuous Cyber Security Monitoring	Mitigation	Improvements
		Framework Profile	Protective Technology	Detection Processes	Improvements	Communication & Coordination
TECHNOLOGY	Data Layer	File Management tools	Access Control, Antivirus	Antivirus	Antivirus, Antimalware	Backup & Restore
	Application Layer	Change Management	Antivirus, Update/Patch	Database monitoring	Antivirus, Antimalware, Update/Patch	Backup, Re-installation, Re-configuration,
	Host Layer	Inventory list	Antivirus, Host Firewall, Hardening, HIPS	Antivirus	Antivirus, Antimalware, Update/Patch,	Re-installation, Re-configuration
	Network Layer	Network reconnaissance/ discovery/monitor tools	Firewall, VPN	IDS, NIPS, Firewall	IPS, Log Analysis	Configuration Backup & Restore
	Physical Perimeter	Access Control, Authorized Personnel badge, trainees'/visitors' badge	Door lock, Lighting, Security Guards, Air-condition, UPS	CCTV, Breach Alarm System, Fire Detection	Fire Extinguisher, UPS, Air-condition	Equipment Repair

4.1.5 Monitor Framework Implementation

Implementation of the company cybersecurity implementation can be monitored utilizing the dashboard at Table 4.3. This Implementation dashboard can also be used as a part of executive presentation.

Table 4.3: Implementation Dashboard for Scenario-1 Company

Cybersecurity Implementation Dashboard for Scenario-1 Company						
CAPABILITIES		**Identify**	**Protect**	**Detect**	**Respond**	**Recover**
PROCEDURES		🟩 Organizational context	🟨 Access Control	🟩 Anomalies Detection	🟨 Response Planning	🟨 Recovery Planning
		🟩 Asset Management	🟨 Security Awareness and Training	🟩 Detective Technology	🟩 Communication & Coordination	🟥 Disaster Recovery Planning
		🟩 Risk Assessment	🟩 Data Security	🟥 Multiple Sensors Implementation	🟩 Analysis	🟥 Business Continuity Planning
		🟩 Governance	🟩 Maintenance	🟨 Continuous Cyber Security Monitoring	🟨 Mitigation	🟩 Improvements
		🟩 Framework Profile	🟨 Protective Technology	🟩 Detection Processes	🟩 Improvements	🟩 Communication & Coordination
TECHNOLOGY	Data Layer	🟩 File Management tools	🟩 Access Control, Antivirus	🟩 Antivirus	🟩 Antivirus, Antimalware	🟨 Backup & Restore
	Application Layer	🟨 Change Management	🟩 Antivirus, Update/Patch	🟥 Database monitoring	🟩 Antivirus, Antimalware, Update/Patch	🟩 Backup, Re-installation, Re-configuration,
	Host Layer	🟩 Inventory list	🟨 Antivirus, Host Firewall, Hardening, HIPS	🟩 Antivirus	🟩 Antivirus, Antimalware, Update/Patch,	🟩 Re-installation, Re-configuration
	Network Layer	🟨 Network reconnaissance/ discovery/monitor tools	🟩 Firewall, VPN	🟩 IDS, NIPS, Firewall	🟨 IPS, Log Analysis	🟩 Configuration Backup & Restore
	Physical Perimeter	🟨 Access Control, Authorized Personnel badge, trainees'/visitors' badge	🟩 Door lock, Lighting, Security Guards, Air-condition, UPS	🟩 CCTV, Breach Alarm System, Fire Detection	🟩 Fire Extinguisher, UPS, Air-condition	🟨 Equipment Repair

🟩 Implemented 🟨 Partially Implemented 🟥 Not Implemented

4.1.6 Feedback for Improvement

Company IT Manager will continuously monitor the implementation, stay alert for any deficiencies, consider any feedback available, and integrate if necessary. Any changes in company business context, risk assessment, threats, physical environment and available resources will be communicated with executives and incorporated in the Framework Profile and monitored by the Implementation Dashboard.

4.2 SCENARIO-2

This scenario will explain development and implementation of the cybersecurity framework for a small-size firm. The firm is an accounting firm which provides accounting, tax and financial consultancy services to its customers.

4.2.1 Analyze Business Context

a. Business industry: Firm is in accounting service sector. It provides accounting, tax, and financial consultancy services to its customers.

b. Organization size: It can be considered as a small-size firm considering its number of employees, facilities, business relations and annual income.

c. Organization structure and number of people: The firm has 13 employees; 2 executive level people, 2 assistants, 1 personnel in administrative management, 1 IT manager, 7 accountants.

d. Physical location, facility perimeter, building, and rooms: The firm is located on the 3rd floor of a business plaza, occupying an office area with 5 office rooms. Building physical perimeter security is provided by plaza management, with security guards and security cameras. There are several security cameras operating in the building managed by the plaza management. The firm has its secure door separating the firm are from the rest of the floor, and its own security cameras for its office rooms. Office rooms are provided with standard door locks. Servers are located in a cabinet in the IT manager office, there is UPS inside the cabinet. Whole building is equipped with air conditioner, fire extinguisher system and power generator.

e. Environmental and natural conditions: No flood is expected in the area, building is built strong against earthquakes, no environmental or natural threats assessed to the firm. Plaza building is equipped with power generators.

f. Available resources: The firm has limited financial resource to spare for cyber expenses. There is only one IT personnel managing the firm cyber services, including cybersecurity requirements. Some required cyber services are outsourced as necessary.

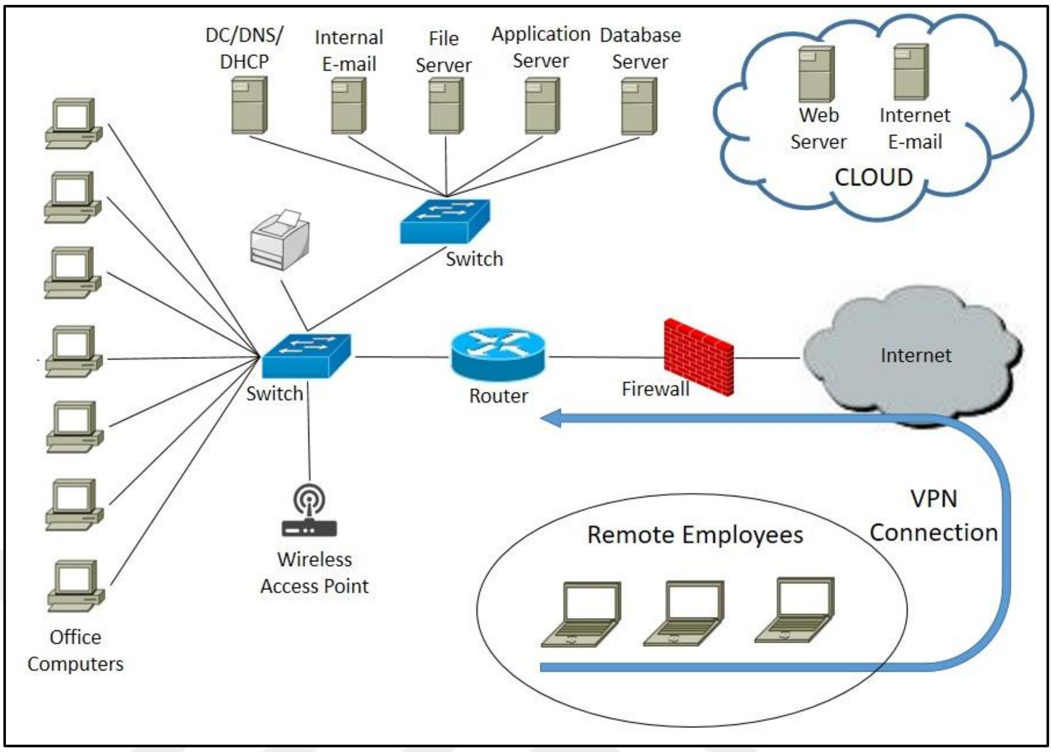
g. Business strategic priorities: Main priority for the company is to provide accounting, tax and financial consultancy to its customers. Although cybersecurity is not the main priority for the firm, keeping the accounting application software and the firm website available for the customers has great importance for the firm to maintain its business goals.

4.2.2 Identify Cyber Assets

a. Cyber Structure: The firm has a small size LAN to provide IT services, with servers, a switch and a wireless access point for the connection of computers in office. Firm hosts application and database servers for accounting purposes. Firm website is hosted by a third party hosting company, exchange server is also outsourced. The firm network is connected to the internet behind a firewall. There are also laptops used by firm accountants remotely connecting the firm network via VPN connection when they are visiting customers.

b. Network Diagrams, connection profiles: Firm network diagram and connections are provided in Figure 4.2.

Figure 4.2: Scenario-2 Firm Network Diagram



c. Inventory of servers, workstations, mobile devices, peripheral devices: Firm cyber inventory is prepared to include servers (physical/virtual), computers, mobile devices, peripheral devices, switch, routers, wireless equipment, and the firewall.

d. Inventory of software and applications: Software and application inventory is prepared to maintain updates, upgrades and to provide license management.

e. Organization data and sensitivity (classification) levels:

i. Confidential: Confidential information of other firms/organizations which are provided accountancy and consultancy by the firm. Firm financial data, documentation and agreements.

ii. Unclassified: Non-sensitive information which can be shared with customers.

4.2.3 Conduct Risk Assessment

Risk assessment table is utilized for the identification and analysis of threats, vulnerabilities, likelihood and impact of threats, risk rating. After the analysis, risk treatment and security controls to be applied are identified. Risk assessment table for Scenario-2 firm is provided at Table 4.4.

Table 4.4: Scenario-2 Risk Assessment Table

Threat	Vulnerability	Likelihood	Impact	Risk Rating	Risk Treatment	Security Control
Remote accountant connections	Company accountants remotely connecting the firm network	Likely	Major	High	Eliminate	Implement VPN solution for the remote connection of the accountants.
Availability of the accounting application is critical	High availability for the accounting application service is required.	Likely	Major	High	Eliminate	Redundant server copies to be implemented on the cloud.
Malware	Unpatched system	Unlikely	Minor	Low	Eliminate	Patch the system
Hackers	Company web site is critical for firm business.	Likely	Major	Medium	Transfer	Web server security is provided by hosting company.
Hackers	Web Server DDoS protection	Almost certain	Major	High	Transfer	DDoS protection service will be procured from Internet Service Provider
Environmental Threats	Damage to cyber assets	Unlikely	Minor	Low	Minimize	No major environmental threats to firm cyber assets due to building structure.

4.2.4 Develop Framework Profile

Framework profile for the Scenario-1 company is provided at Table 4.2.

Table 4.5: Framework Profile for Scenario-2 Firm

Cybersecurity Framework Profile for Scenario-2 Firm						
CAPABILITIES		**Identify**	**Protect**	**Detect**	**Respond**	**Recover**
PROCEDURES		Organizational context	Access Control	Anomalies Detection	Response Planning	Recovery Planning
		Asset Management	Security Awareness and Training	Detective Technology	Communication & Coordination	Business Continuity Planning
		Risk Assessment	Data Security	Continuous Cyber Security Monitoring	Mitigation	Improvements
		Framework Profile	Protective Technology	Improvements	Improvements	Communication & Coordination
TECHNOLOGY	Data Layer	File Management tools	Access Control, Antivirus	Antivirus	Antivirus, Antimalware	Backup & Restore
	Application Layer	Change Management	Antivirus, Update/Patch	Database monitoring	Antivirus, Antimalware, Update/Patch	Backup, Re-installation, Re-configuration,
	Host Layer	Inventory list	Antivirus, Hardening	Antivirus	Antivirus, Antimalware, Update/Patch,	Re-installation, Re-configuration
	Network Layer	Network reconnaissance/discovery/monitor tools	Firewall, VPN	Firewall	Log Analysis	Configuration Backup & Restore
	Physical Perimeter	Access Control, Authorized Personnel badge, visitors’ badge	Door lock, Lighting, UPS	CCTV, Fire Detection	Fire Extinguisher, UPS	Equipment Repair

4.2.5 Monitor Framework Implementation

Implementation of the firm cybersecurity implementation can be monitored utilizing the dashboard at Table 4.6. This Implementation dashboard can also be used as a part of executive presentation.

Table 4.6: Implementation Dashboard for Scenario-2 Firm

Cybersecurity Implementation Dashboard for Scenario-2 Firm						
CAPABILITIES		**Identify**	**Protect**	**Detect**	**Respond**	**Recover**
PROCEDURES		🟩 Organizational context	🟩 Access Control	🟨 Anomalies Detection	🟨 Response Planning	🟩 Recovery Planning
		🟩 Asset Management	🟩 Security Awareness and Training	🟩 Detective Technology	🟩 Communication & Coordination	🟨 Business Continuity Planning
		🟨 Risk Assessment	🟨 Data Security	🟨 Continuous Cyber Security Monitoring	🟩 Mitigation	🟩 Improvements
		🟩 Framework Profile	🟨 Protective Technology	🟩 Improvements	🟩 Improvements	🟩 Communication & Coordination
TECHNOLOGY	Data Layer	🟩 File Management tools	🟩 Access Control, Antivirus	🟩 Antivirus	🟩 Antivirus, Antimalware	🟩 Backup & Restore
	Application Layer	🟩 Change Management	🟩 Antivirus, Update/Patch	🟥 Database monitoring	🟩 Antivirus, Antimalware, Update/Patch	🟥 Backup, Re-installation, Re-configuration,
	Host Layer	🟩 Inventory list	🟨 Antivirus, Hardening	🟩 Antivirus	🟨 Antivirus, Antimalware, Update/Patch,	🟩 Re-installation, Re-configuration
	Network Layer	🟨 Network reconnaissance/ discovery/monitor tools	🟩 Firewall, VPN	🟩 Firewall	🟥 Log Analysis	🟨 Configuration Backup & Restore
	Physical Perimeter	🟨 Access Control, Authorized Personnel badge, visitors' badge	🟩 Door lock, Lighting, UPS	🟩 CCTV, Fire Detection	🟩 Fire Extinguisher, UPS	🟥 Equipment Repair

🟩 Implemented 🟨 Partially Implemented 🟥 Not Yet Implemented

4.2.6 Feedback for Improvement

Company IT Manager will continuously monitor the implementation, stay alert for any deficiencies, consider any feedback available, and integrate if necessary. Any changes in company business context, risk assessment, threats, physical environment and available resources will be communicated with executives and incorporated in the Framework Profile and monitored by the Implementation Dashboard.

5. CONCLUSION

It is clear that, small and medium size organizations need more help on implementing cybersecurity than large size organizations, due to increasing threats, complex security solutions and limited resources. This framework can be used to aid the small and medium size enterprises to understand their cyber structure, current threats, and figure out what they can do in order to obtain a decent level of cybersecurity posture.

It is not possible to develop a one-size-fits-all solution, this framework is designed to be flexible, so that organizations can build and implement the appropriate framework profile which fits the organization's needs, cyber structure, business objectives and risk appetite.

It is highly important to keep in mind that, cyber threats are increasing and evolving every day, and security measures should increase and evolve as such. The solutions defined in this study may not include all current security measures and can not last forever. In addition to the security solutions provided in this study, another important takeaway should be the developed "framework approach". This is a living document, organizations should seek opportunities to incorporate newly introduced technologies and threats to keep the framework up to date. For instance, cloud technology is becoming widely used as a cyber structure, the organizations utilizing cloud solutions are encouraged to upgrade this framework and integrate the cyber threats and security measures to meet their updated requirements.

REFERENCES

Books

Merkow, M.S. & Breithaupt, J., 2014. *Information security: principles and practices.* Second Edition. Indiana: Pearson IT Certification

Humphreys, T., 2016. *Implementing the ISO/IEC 27001 ISMS standard*. Second Edition. Boston : Artech House.

Campbell, T., 2016. *Practical Information Security Management : A Complete Guide to Planning and Implementation.* New York: Apress

Caroll, J., 1996. *Computer Security*. 3rd ed. Newton, MA: Butterworth-Heinemann

Refsdal, A., Solhaug, B. & Stolen K., 2015. *Cyber-Risk Management*. London:Springer

Probst, C.W., Hunker, J., Gollmann, D. & Bishop, M., 2010. *Insider threats in cyber security*. London:Springer

Periodicals

Safa, N.S., Solms, R.V., & Furnell, S., 2016. Information security policy compliance model in organizations. *Computers & Security*. **56**, pp. 70-82.

Osborn, E., & Simpson A., 2017. On small-scale IT users' system architectures and cyber security: A UK case study. *Computers* & *Security.* **70**, pp. 27-50

Other Publications

Turkish Statistical Institute-TUIK, The Small and Medium Size Enterprise Statistics 2016, http://www.tuik.gov.tr/PdfGetir.do?id=21540 [accessed 25 Feb 2018]

Turkish Government Official Newspaper, Regulation on the definition, composition, and classification of small and medium size enterprises, 2012, http://www.resmigazete.gov.tr/eskiler/2012/11/20121104-11.htm , [accessed 25 Feb 2018]

UK Government, Department for Business, Innovation & Skills, Business population estimate for the UK and regions: 2017 statistical release, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/663235/bpe_2017_statistical_release.pdf , [accessed 25 Feb 2018]

Rapid7 LLC, [no date]. *The Most Common Types of Cyber Security Attacks*, [online]. https://www.rapid7.com/fundamentals/types-of-attacks [accessed 14 Feb 2018]

McDowell M., 2013. *Understanding Denial-of-Service Attacks,* [online]. https://www.us-cert.gov/ncas/tips/ST04-015 [accessed 14 Feb 2018].

National Institute of Standards and Technology (NIST), Framework for Improving Critical Infrastructure Cybersecurity, 2014, https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf [accessed 14 Feb 2018], p.7.

Rapid7 LLC, [no date]. *What is a man-in-the-middle attack?*, [online]. https://www.rapid7.com/fundamentals/man-in-the-middle-attacks [accessed 14 Feb 2018]

Sasneh R., 2016. *10 Easy Ways To Spot a Phishing Attack,* [online]. https://www.techwyse.com/blog/internet-marketing/easy-ways-to-spot-phishing-attack [accessed 15 Feb 2018].

Nayak, G.N. & Samaddar, S.G., 2010. Different flavours of Man-In-The-Middle attack, consequences and feasible solutions. *2010 3rd International Conference on Computer Science and Information Technology*. 9-11 July 2010 Chengdu, China: IEEE, p.5

Krebs M., 2015. *Clone wars – How to secure yourself from an evil hotspot,* [online]. http://lancomwire.com/clone-wars-how-to-secure-yourself-from-an-evil-hotspot [accessed 16 Feb 2018].

Keycdn 2017. *What Is DNS Spoofing?,* [online]. https://www.keycdn.com/support/dns-spoofing [accessed 16 Feb 2018]

Hidayatullah S., 2010. *Man in the middle attack prevention strategies,* [online]. http://www.computerweekly.com/tip/Man-in-the-middle-attack-prevention-strategies [accessed 16 Feb 2018].

Patsis G., 2013. *Integrating people, process and technology,* [online]. https://www.scmagazineuk.com/integrating-people-process-and-technology/article/545841 [accessed 16 Feb 2018].

Lord, N., 2017, What is Data Loss Prevention (DLP)? A Definition of Data Loss Prevention [Online], Data Insider, https://digitalguardian.com/blog/what-data-loss-prevention-dlp-definition-data-loss-prevention , [accessed 18 Feb 2018].

Bradley, T., 2018, Introduction to Intrusion Detection Systems (IDS) [Online], Lifewire, https://www.lifewire.com/introduction-to-intrusion-detection-systems-ids-2486799, [accessed 24 Feb 2018]

Verizon, 2017 Data Breach Investigations Report 10th Edition, [online], https://www.ictsecuritymagazine.com/wp-content/uploads/2017-Data-Breach-Investigations-Report.pdf , [accessed 20 Feb 2018]