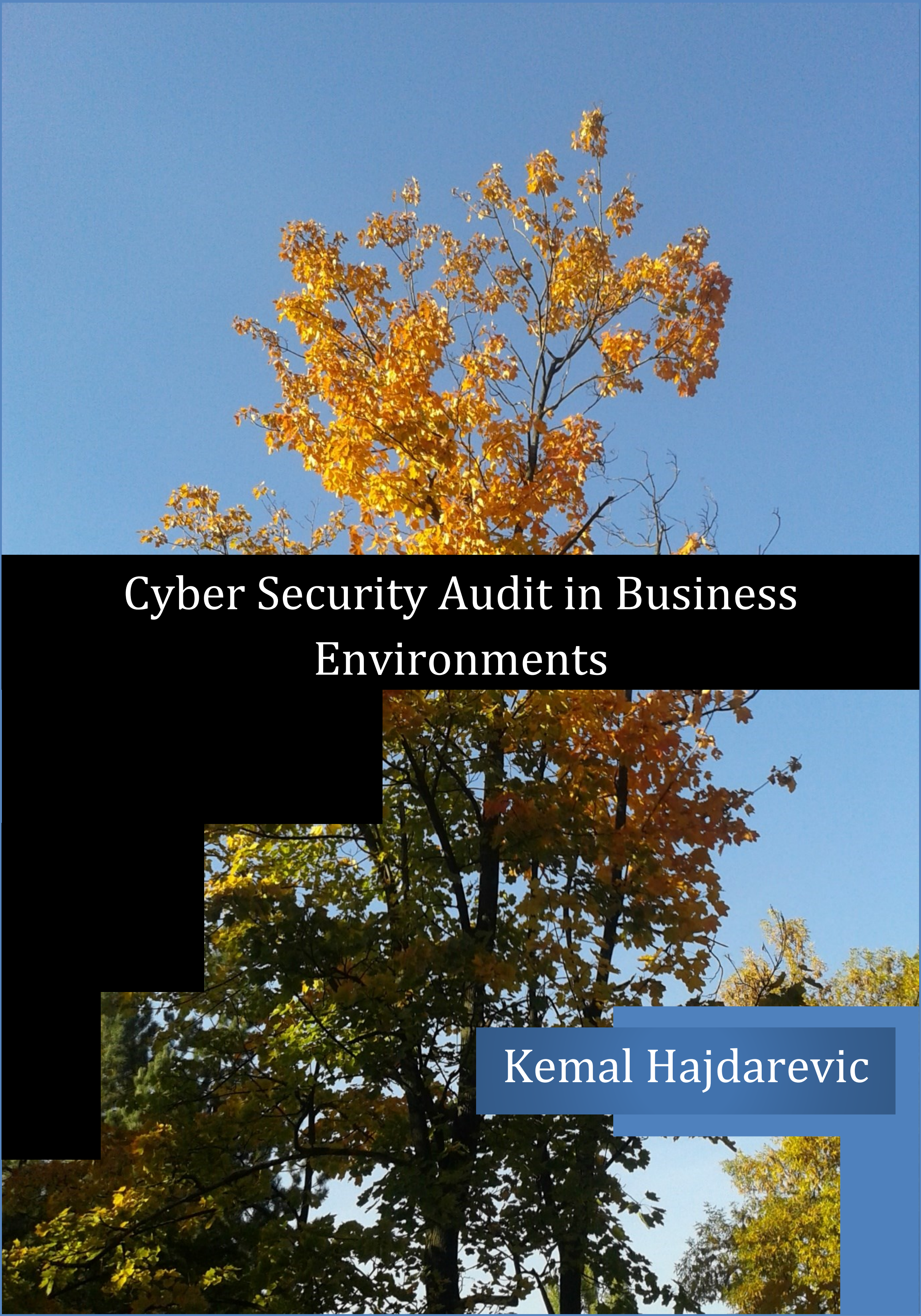
Cyber Security Audit in Business Environments



Kemal Hajdarevic

Cyber Security Audit in Business Environments

Kemal Hajdarevic

Sarajevo, 2018

Author:
Dr. Kemal Hajdarević

Proofreading
Pat Allen & Ana Tankosić

Publisher:
International Burch University

Editor-in-Chief:
Dr. Kemal Hajdarević

Reviewed by:
Prof. Dr. Colin Pattinson
Prof. Dr. Mario Spremić

DTP & Design:
Dr. Kemal Hajdarević

DTP and Prepress:
International Burch University
Circulation: Electronic document

Place of Publication: Sarajevo

Disclaimer: While every effort has been made to ensure the accuracy of the information, contained in this publication, International Burch University will not assume liability for writing and any use made of the proceedings, and the presentation of the participating organizations concerning the legal status of any country, territory, or area, or of its authorities, or concerning the delimitation of its frontiers or boundaries.

CIP - Katalogizacija u publikaciji
Nacionalna i univerzitetska biblioteka
Bosne i Hercegovine, Sarajevo
004.056:658
HAJDAREVIĆ, Kemal
Cyber security audit in business environments [Elektronski izvor] / Kemal Hajdarevic. - El. knjiga. - Sarajevo : International Burch University, 2018, XVI,160 str. : ilustr. ; 25cm About author: str. 161.
Način dostupa
(URL): http://eprints.ibu.edu.ba/3776/1/Cyber%20Security%20Audit%20in%20Business%2 0Environments_12.12.2018.pdf. - Nasl. sa nasl. ekrana. - Opis izvora dana 19. 12. 2018.
ISBN 978-9958-834-64-6
COBISS.BH-ID 26733830

Table of Contents

Author’s Preface

Everyday reports reveal numerous cyber security incidents, while many more are never uncovered due to the risk of jeopardising the reputation of the attacked systems. One definition of risk of this sort is:

“feasible determinable outcome of an activity or action subject to hazards” (Stamatelatos, 2000).

A more holistic and comprehensive definition, which is available in the NIST Special Publication 800-30 Revision 1 Guide for Conducting Risk Assessment, defines risk as:

„Adverse impact(s) that could occur... to organisational operations (including mission, functions, image, reputation), organisational assets, individuals, other organisations... due to the potential for unauthorized access, use, disclosure, disruption, modification, or destruction of information and/or information systems.“

As such, databases, as the active and passive components of computer networks and the building blocks of computer infrastructures, became a point of focus for every business in the world. Unlike 30 years ago, many households nowadays rely on Internet access and available services to support their everyday life. The Internet and World Wide Web (WWW) resources are accessible through various web browsers. The concept of web browsing can be traced back to Sir Timothy John Berners-Lee, who in March 1989 wrote a proposal in which he proposes a unique way to access web resources, using three components: Hyper Text Markup Language (HTML), Hyper Text Transfer Protocol (HTTP), and Unique Resource Locator (URL) (History of the Web, 2018).

The new and important role of computer network infrastructures, and information technologies supported by computers and computer communication networks, produced user who depend and trust in the reliability and security of their operations. Every day, media and news report on different criminal activities or misconducts in which information technology assets were involved. It is well known that high-tech companies, organisations, and banks are not the only victims of cyber-crime, but that every sphere of business and life can be subject to cyber security incidents.

Information security encompasses the field of information security, where information refers to both electronically stored or transferred information, as well as information that is written on paper or spoken in conversation.

Cyber security also has a narrower meaning that includes only information and data stored or transferred electronically. In 1948, Norbert Wiener defined cybernetics as the science of control of and communication with animals and machines (Norman J., 2018), while the term cyberspace was used by William Gibson in his 1984 book "Neuromancer" (Gibson W., 1984). In the 21st century, this term implies control of any system using technology.

In this book, cyber security is constrained to computer architectures and infrastructures, network components such as routers, switches, servers, and VOIP PBXs, as well as other active and passive devices and equipment which are part of every modern business environment.

This book is intended for cyber and information security auditors, practitioners, and students, or as supplementary documentation for students of computer communication, network administration courses, network security, ethical hacking, or network forensics courses, who have the intention to manage or be a part of cyber and information security management and audit processes.

These days, universities are trying to modernise their syllabi by creating new programs and courses that will cope with current cyber and information security challenges. However, in most cases university programs cannot change as dynamically as cyber security players in cyber arenas which demand constant changing. Students and scientists have to be aware of risks associated with fraud (English Oxford Dictionaries, 2018), different technologies, IoT devices, and the deep and dark web where criminals are at large and crime connected to the real world is happening. That is why universities in most cases still lead a losing battle when it comes to preparing information technology students for real world challenges in managing and auditing information and cyber security.

Another important goal that audit process have to accomplish, if possible, is to proactively inform stake holders regarding the state of operations, using systems of dashboards located in one place which will sound an alert in case of important cyber security issues.

Organisation of book sections

The book is divided into seven sections:

1. Introduction

2. Security of cyber and information system components

3. Cyber security landscape

4. Cyber security incident cases

5. Cyber security controls

6. Cyber security audit

7. Conclusions

While reading, it is possible to follow different tracks as proposed below.

Learning tracks

It is possible to acquire specific skills and knowledge on certain paths through different chapters in the scheme shown below.

For internal auditors, the order of reading book chapters is 1, 2, 3, 4, 5, and 6. For ethical hackers, the chapters can be read in the same order, excluding chapter 6. For network managers, the chapter order is 2, 3, and 5. Finally, for members of law enforcement agencies important chapters are 3, 4, and 5, while for Chief Information Security Officers the order of chapters to be read is 2, 3, 4, and 5.

Important definitions

Information System (IS) Security - Refers to the activities, processes, methodologies, frameworks, and standards used for the maintenance of information and information assets confidentiality, integrity, and availability. (Techopedia, 2018)

IT Controls - Refers to procedure policies that provide a reasonable assurance that information technology (IT) operations are reliable and compliant with applicable laws and regulations. (Mar S., et. al., 2012)

IT Auditing – Refers to an examination of the Information technology (IT) infrastructure controls established by management. (Mar S., et. al., 2012)

1. Introduction

Chapter abstract

Chapter goals: To present early advancements in reviewing past events, and primarily the French war campaign against Russia. To introduce core information security principles. To introduce and explain the relationship between information and cyber security. To introduce the concept of digital transformation and the risks associated with the usage of digital technology in digital transformation.

Learning outcomes: Knowledge of core principles of information security and cyber security. Cyber security assets that have to be supported through cyber security management processes.

One view on the history of documenting past events

Charles Joseph Minard (27 March 1781 – 24 October 1870) was one of the first contributors in the field of information graphics and a historian of civil engineering and statistics. Minard was working as Inspector General of Bridges and Roads (Mason B., 2017), and he is well known for his graphic work from 1869 where he presented Napoleon's disastrous military campaign against Moscow from 1812 to 1813 (Mason B., 2017). By analysing the graph shown below, it is possible to notice that Minard analysed the causes and consequences of the campaign within a single graph, which is why this document can be seen as an early sample of audit finding documentation. All findings in audit reports have to have references based on hard evidence.

As it can be read from Minard's map, the campaign started on the 24th of June 1812. The retreat from Moscow began on October 18, and ended on December 14. The graph shows the number of soldiers lost during advances to Moscow and the following return to France.

In the same graph we may find information concerning the temperature during one phase of retreat, equal to -37.5 C. This graph is probably one of the earliest flow maps containing quantitative information ever created. In literature (Maswerk, 2013), the graph is known as "*The map that made a nation cry*" because Napoleon started his campaign to Moscow with 422,000 soldiers from Niemen, France in 1812, with only 10,000 returning alive.

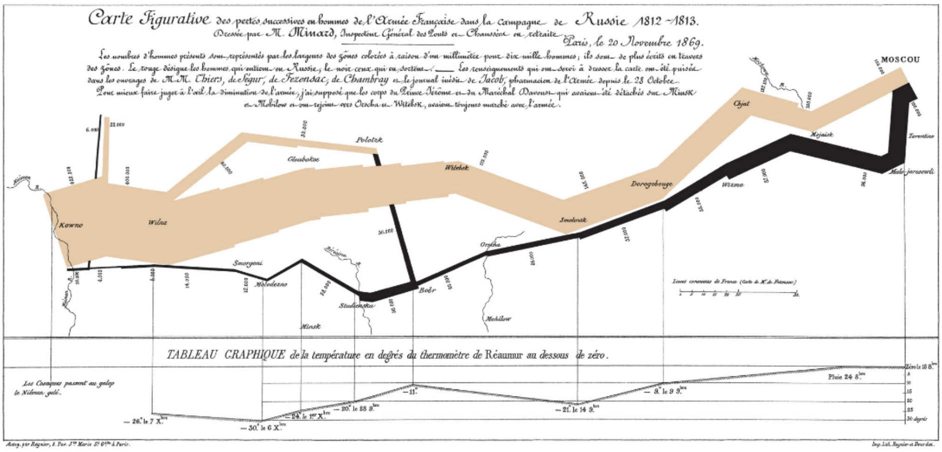

Carte Figurative des pertes successives en hommes de l'Armée Française dans la campagne de Russie 1812-1813.
Dressée par M. Minard, Inspecteur Général des Ponts et Chaussées en retraite.
Paris, le 20 Novembre 1869.
Les nombres d'hommes présents sont représentés par les largeurs des zones colorées à raison d'un millimètre pour dix mille hommes; ils sont de plus écrits en travers des zones. Le rouge désigne les hommes qui entrent en Russie, le noir ceux qui en sortent. — Les renseignements qui ont servi à dresser la carte ont été puisés dans les ouvrages de M.M. Thiers, de Ségur, de Fezensac, de Chambray et le journal inédit de Jacob, pharmacien de l'Armée depuis le 28 Octobre.
Pour mieux faire juger à l'œil la diminution de l'armée, j'ai supposé que les corps du Prince Jérôme et du Maréchal Davoust qui avaient été détachés sur Minsk et Mobilow et ont rejoint vers Orscha et Witebsk, avaient toujours marché avec l'armée.
MOSCOU
Polotzk
Gloubokoe
Witebsk
Chjat
Mojaisk
Tarantino
Malo-jarosewli
Wixma
Dorogobouge
Smolensk
Kowno
Wilna
Smorgoni
Molodezno
Minsk
Studienska
Bobr
Orscha
Mohilow
Niemen
422.000
400.000
60.000
33.000
175.000
145.000
100.000
6.000
22.000
12.000
14.000
8.000
4.000
10.000
28.000
50.000
37.000
24.000
96.000
87.000
Lieues communes de France
TABLEAU GRAPHIQUE de la température en degrés du thermomètre de Réaumur au dessous de zéro.
Les Cosaques passent au galop le Niémen gelé.
— 26° le 7 X.bre
— 30° le 6 X.bre
— 24° le 1er X.bre
— 20° le 28 9.bre
— 11°
— 21° le 14 9.bre
— 9° le 9 9.bre
Pluie 24 8.bre
Zéro le 18 8.bre
5
10
15
20
25
30 degrés
Autog. par Regnier, 8. Pas. Ste Marie St Gain à Paris.
Imp. Lith. Regnier et Dourdet.

Figure 1. Charles Joseph Minard: Napoleon's Retreat from Moscow (The Russian Campaign 1812-1813), Mason B., (2017)

That means that only 2.37% of soldiers returned alive. Up to this point, Napoleon's army was the largest army ever in the history of warfare. This graph presents a quantitative perspective of disastrous events which shows a lack of logistics, military planning, organisation, and transportation. Graph above is a presentation of many different types of data in one visual form, so the relationship between them can be seen.

From that point onwards, warfare strategists used available information and experience to avoid similar situations through better planning and organization. *Napoleon's Retreat from Moscow* looks like a non-interactive dashboard with a lot of useful information. An interactive graphic dashboard version (Maswerk, 2013) where different data reported by Minard can be analysed is available online.

Graphic maps and dashboards provide intuitive insight into multiple sets of data, facts, and information, all presented within one graphic view. By graphically documenting past events with time scales from which conclusions can be drawn, we can learn from history and available resources with the goal of preventing future unfortunate events or to improve existing activities and processes. Minard published his famous map 56 years (referenced above) after the events that changed history forever. In today's electronic or digital era we encounter activities, events, vulnerabilities, and incidents which have to be solved as soon as possible, and sometimes within minutes, hours, or days, since any unnecessary delay in time can produce serious negative consequences.

One view on digital transformation

Digital business transformation through digital technologies provides different services to a large number of people in different parts of the globe. This dominant technology creates a large dependency on digital technology in every sphere of business and life for the population at large.

Services such as *mPesa,* which started operating in 2007, allow users (20 million) mostly in Africa to exchange money and use it as a payment mechanism (Spremic, 2017).

In Sweden 95% of all transactions are performed without physical banknotes, and in Denmark from 2016 there is law that allows shops to require only electronic payment and to refuse to accept physical banknotes (Spremic, 2017).

The Netflix service, which started as a DVD movie renting company, now provides online movie rental services to more than 80 million users in more than 200 countries. Wal-Mart and Macy use the Facebook *„like"* option to decide which products will have a lower price or which products are most preferred among customers, Spremic (2017).

Airbnb is a service which allows customers to lease or rent short-term lodging, including cottages, apartments, homestays, hostel beds, or hotel rooms. More bookings are done by Airbnb than through official hotel chains. Airbnb does not have physical offices for their customers across the world. The same is true for Uber, the biggest global taxi service which is supported and run exclusively through the Internet (Spremic, 2017).

Data and information in today's business environments are the most valuable assets, immediately after the people who are responsible for managing information and maintain the security, confidentiality, integrity, and availability of information (CIA). Business sustainability depends on well-managed cyber and information security.

Whenever technology is used to improve business operations, there is risk that malicious individuals, such as cyber criminals, will attempt to harm the implemented technology.

While information security deals with the security of information, CIA treats information not only in their digital form, but in printed form as well, as well as any information that can be stored or transmitted in electronic form.

Digital transformation cyber security challenges

It was apparent that cyber security quakes were on agenda during and after the US elections which ended in January 2017. Cyber events including Hilary Clinton's leaked e-mails (Zurcher A., 2016), and the Russian influence reported by (LaFraniere S, 2018) throughout the campaign, still reverberate through the US political arena at the time when this book was in the process of writing, in the spring and summer of 2018.

Other notable cyber incidents include the Central Bangladesh Bank heist (Ruma P., 2018), which took place in February 2016, where Dridex malware was used for an attack against the local SWIFT infrastructure (Thomson I., 2016). Hackers tried to steal $951 million, succeeding in stealing around $80 million (Ruma P., 2018). The exact amount is not known, but the hackers used existing device vulnerabilities, such as operating systems which were not patched, and did not have proper antivirus intrusion detection and firewall protection.

The future will most certainly bring new unseen incidents, since we are generally only informed about incidents related to financial frauds and malicious attacks in banking industry in the news. We already witnessed incidents related to technology or military espionage and attacks on elements of vital national infrastructure, such as the attack on nuclear power plants using Stuxnet (Mueller P. and Yadegari B., 2012). It is a question of great concern what will happen in the future when food and pharmaceutical companies become the target of cyber-attacks once all tasks are automated, including, for example, the addition of chemical ingredients and determination of dosage levels.

Attacks on any computer network infrastructure, such as food processing facilities, could be conducted via communication channels, servers, data bases, and applications.

These kinds of attacks can severely affect human health or even cause deaths. As such, we realise the danger of underestimating risks associated with cyber and information security, especially by individuals responsible for security. While key persons and top management in most working environments will most probably be able to recognise the importance of cyber and information security as one of the top strategic goals, when it comes to real world situations there are many existing problems and challenges.

The nature of information is such that it can exist in different forms, or it can be communicated using different communication channels. Information can be written on paper, stored on hard disks in data bases, or transferred via wired or wireless communication channels.

Purpose of this book

The purpose of this book is to provide insight into cyber security landscapes, and it is intended for students, teachers, administrators, information security auditors, forensic staff, security consultants/professionals, professional penetration testers, and everyone else who plans to use it for ethical reasons.

This book can be used as a review manual for cyber and information security, or as supplemental documentation related to computer security, digital forensics, and ethical hacking courses. The book is also necessary in areas where it is important to monitor the performance and compliance of information systems, and to report the status to management or regulatory bodies in the form of a specific type of operational feedback.

Feedback is a well-known term and mechanism from the 18th century, used in different fields including engineering (mechanical, electrical, electronic, software), dynamical systems, climate science, control theory, finance and economy, biology, social science, and even medicine as a self-regulated mechanism. Ramaprasad (1983) defines it as:

“Information about the gap between the actual level and the reference level of a system parameter“

Business environments are supported by computer and network infrastructures that are used for collaboration, data processing, internal and external communication, reporting, and many other purposes. As such, cyber and information security auditors have to be aware of approaches presented here which can make their jobs easier.

This book can also be used as a quick reference guide in addition to other referenced sources for practitioners who are delegated or are in the process of information system, cyber, and information security audit. It can be used as supplemental material for students of computer communications and network management courses, information management system courses, system and network administration courses, and cyber and network security courses.

In essence, this book is for cyber security specialists who want to learn more about the process of auditing, using available standards and controls applicable to today's architectures with active components such as switches and routers. While university programs offer technical knowledge about cyber and information security management through courses, there is a clear need to educate students about the organisational aspects and functions which include auditing.

This book can be used as supplemental material for students and practitioners to grasp the scope of expertise they will need, and to understand what standards, methods, and tools can be used to successfully perform future tasks in cyber and information security arena, with a particular focus on auditing tasks.

The focus of this book is on principles of auditing, applicable standards, controls, and risk management processes. Another contribution of this book is the visualisation of trends and the presentation of the current state of the field of auditing.

Cyber security

Cyber security is limited to electronically stored data or information, as well as data and information which is transferred through communication channels, real time operational instructions, network devices, communications links, servers ant other similar devices which stores and transports the data.

The management of information security covers cyber related information, as well as physical media such as paper and spoken word. As shown in the figure below, cyber security is considered a subset of information security.

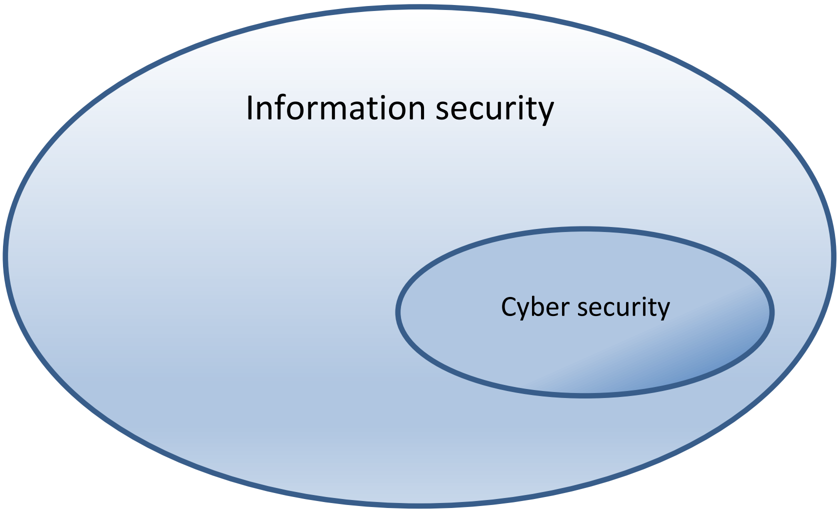


Figure 2. Cyber and information security realm

Cyber security management

Cyber security management is possible through implementation and constant monitoring and improvement check-ups. Check-ups can be implemented in various forms using the existing standards.

As we saw from the well-known cases in the media, the root of many cyber and information security incidents stems from basic administrative flaws such as unpatched operating systems, unimplemented antivirus solutions, or cheap unmanaged switches separating network traffic.

It is a common mistake on the part of the management to believe that information security is only information technology (IT) security or that cyber security is something that only IT experts have to handle. The real-life cases show us that more broader approaches, methods, and standards have to be considered, implemented, and used. A successful response to cyber security threats has to involve key players and decision makers who can contribute to cyber security in key areas.

For cyber security management, IT related activities are key to cyber and information security management for the whole organisations. IT supports data infrastructures through communication signalisation (which can be wired or wireless), with passive (cables, trunks and patch cabinets) and active network components (such as switches and routers), data bases, files, applications, media servers, or clouds.

Unmanaged access rights, weak network controls, weak antimalware update policy, no Bring Your Own Device (BYOD) policy, no cryptographic controls, no media disposal or Universal Serial Bus (USB) policy, will all likely jeopardise organisation security.

Information security has several additional responsibilities for information assets to manage, including:

- Human resources security that would include security issues during the hiring, employment, and termination process. It should include cyber and information security awareness programs for employees and third parties.
- Physical security that would include security of physical perimeters around information processing facilities. The focus of physical security should be physical access rights, video surveillance, and physical alarm systems.
- Legal issues that would include licensing and intellectual rights.
- Common affairs that would include tendering processes, utility concerns such as power supplies from the electric grid, redundant power supplies that would include UPSs, generators, fuel supplies, equipment services, and water and gas supplies.

Summary

Cyber security is a subset of information security that deals with the security of information stored in digital form and transferred over communication links. A great part of information security related standards deals with cyber security issues.

Almost daily, media reports reveal cyber security related incidents. By learning from history, we can conclude that we will see an increase in incidents of this type, especially as more services and users use digital technology in everyday work and life.

Knowledge acquired

The difference between information and cyber security, information and key cyber areas of management. Digital transformation challenges related to cyber security.

Review questions

1. Explain the difference between information and cyber security?
2. What are the key areas of information security?

Further readings

- Digital transformation: online guide to digital business transformation https://www.i-scoop.eu/digital-transformation/
- The Cyber Security Management System: A Conceptual Mapping, SANS Institute InfoSec Reading Room https://www.sans.org/reading-room/whitepapers/basics/cyber-security-management-system-conceptual-mapping-591
- What Is Cybersecurity? https://www.cisco.com/c/en/us/products/security/what-is-cybersecurity.html

2. Security of cyber and information system components

Chapter abstract

Chapter goals: To present Shannon's communication model, as well as the essential network standards related to the ISO OSI referenced model and the TCP/IP suite. To define network topologies, and present network communication devices, network types, and network terminal devices. To present network services and associated protocols, to explain core network management principles, and to explore the purpose of active and passive monitoring.

Learning outcomes: Knowledge of core principles in computer communications and operation of active computer communication network devices, protocols, and services. Essential knowledge concerning network management processes.

Network components and infrastructure

Network infrastructures in terminal devices such as client computers, laptops, smart phones, and servers, provide a large number of users access to different services. All these infrastructures are supported by active and passive devices such as modems, hubs, bridges, switches, routers, firewalls, intrusion detection and prevention systems, and other communication devices and communication links that guarantee reliable and secure communication. For an internal auditor it is important to understand and have enough knowledge of available technology to be able to conduct audits and identify the points of improvement for audited systems.

Network reliability requirements

With the goal of providing reliable network support, network operations have to satisfy specific requirements to be able to support everyday business functions such as:

Interoperability, which means that different network technologies have to be interconnected.

Availability, which means that the network architecture and services have to be available 24-7-365.

Flexibility, which means that new network segments can be added and expanded as new needs are introduced.

Manageability, which means that networks can be well managed from a single point of management.

Communication model

The client–server model is one of the most common communication models available, drawing roots from Shannon and Weaver's communication model presented in the 1940's (Shannon & Weaver, 1949).

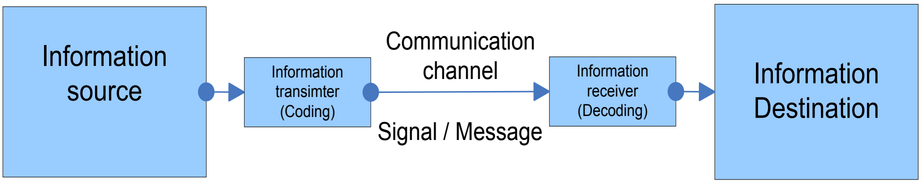


Figure 3. Shannon's communication model

This model contains communicative highlights components such as information source and information destination as the most important parts of communication. With the goal of transmitting information from source to destination, a communication channel (wired or wireless) with transmitters and receivers implemented as hardware or software components is needed. All these components are the building blocks of the core communication model relevant for today's communications.

OSI reference model and TCP/IP suite

The TCP / IP protocol is the standard Internet protocol used, and the latest version of the TCP/IP protocol is version 6 (IPv6, 2018), but version 4 is still widely in use.

TCP/IP protocol suite

In the late 1960s, the United States Department of Defence financed a project known as ARPANET (Featherly K., 2018) with the goal of developing communication protocols which would enable computers to communicate. The initial network started working in 1969, with a set of protocols. In 1974, specifications for the TCP protocol were published, and they were tested in the following years as the fourth version of TCP/IP (Pelkey, 2007). In 1977, first tests were conducted between Stanford and University College of London (TCP/IP Internet Protocol, 1981).

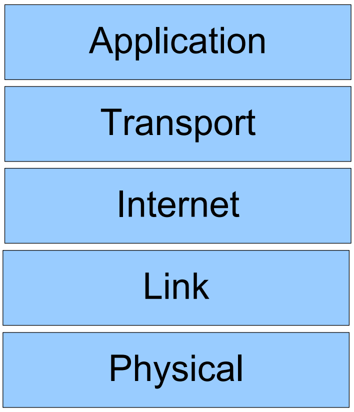


Figure 4. TPC / IP protocol suite layers

ISO / OSI reference model

The idea of standardizing computer protocols was initiated in the 1970s when two bodies for the establishment of international standards independently began working on their reference models. These were the *International Standardisation Organisation* (ISO) and the *International Telegraph and Telephone Consultative Committee* (CCITT acronym, French version of the name) (Pelkey , (2007) Chapter 9 Standards: 1979-1984.

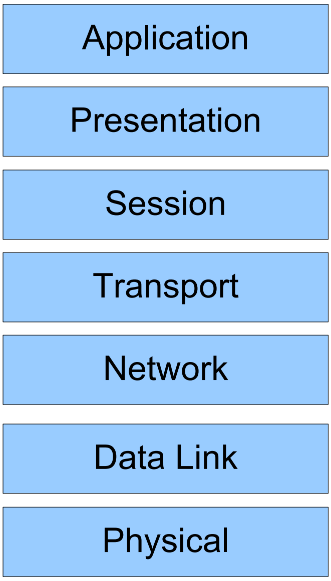


Figure 5. ISO / OSI reference model

The two documents which were created by these two bodies were merged in 1983 and published in 1984 under the name The Basic Reference Model for Open Systems Interconnection. ISO named their version of the standard ISO 7498 (ISO 7498:1984, 1984) and CCITT named it ITU-T (*Telecommunications Standardization Sector of the International Telecommunication Union*) x.200 (x.200, 1995).

The goal of this model was to provide a fundamental design for future protocols which will be used for international communication for the industrial, educational, and commercial purposes.

This model never fully came to life as, unlike TCP/IP, it was not practically implemented in the real world of communications. The OSI reference model is used as a model for educational purposes in order to understand the general principles of the protocol used for computer communications. The OSI reference model has seven layers, as is shown in the figure above.

Network topologies

An important aspect of computer networks is network architecture. Within network architecture, the physical layout of computer networks is called network topology.

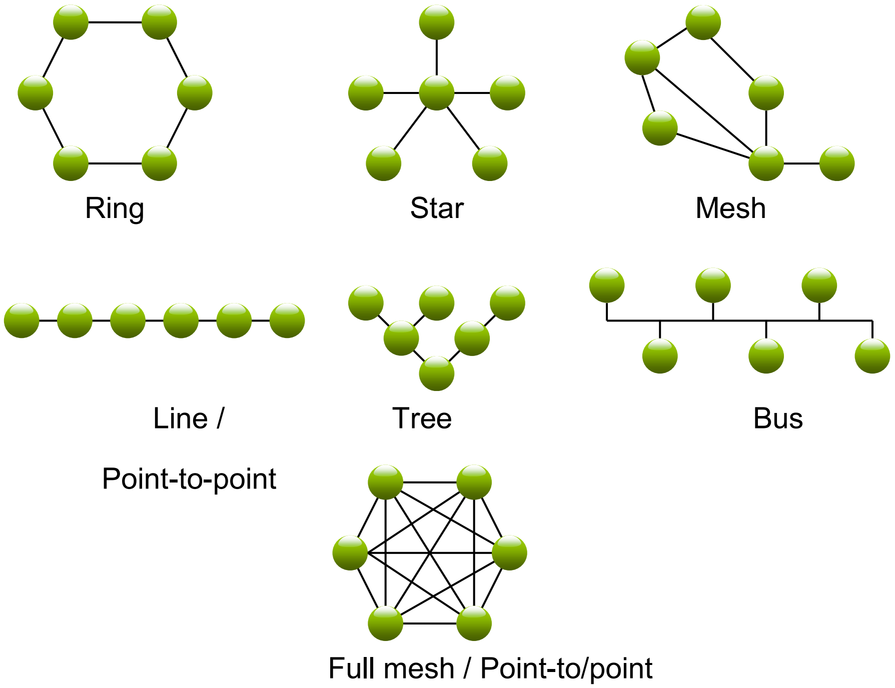


Figure 6. Network topologies

Network topology determines how the network and the networked devices are interconnected. While network topology was primarily used as a hardware setting, with computer networks and Internet, different applications were developed which use elements from physical topologies, such as client-server and peer-to-peer applications.

Client – Server Communication model

This model represent the earliest Internet building blocks where on the service side there was a server, and on the user side was a client.

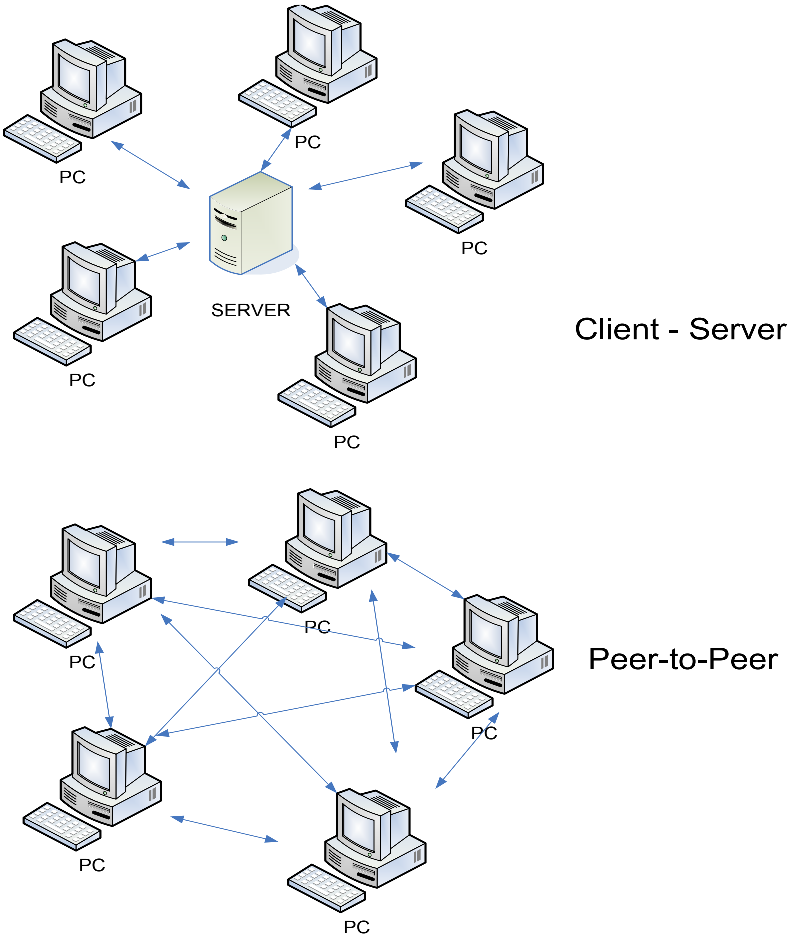


Figure 7. Client-Server and Peer-to-Peer communication models

Peer-to-Peer communication model

The Peer-to-Peer (P2P) model was originally concerned with how computer hardware and computer communication were interconnected.

Infrastructure and ad-hoc communication model

With the arrival of wireless communication, two types of communication models were introduced.

The first one is **infrastructure,** where a wireless access point is needed as a gateway for users to use network resources such as the Internet. In this way, the network is configured in a hierarchical infrastructure.

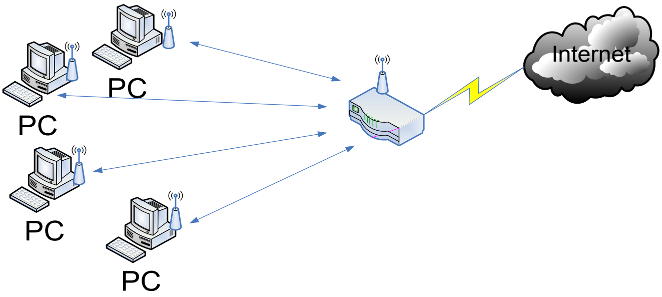


Figure 8. Infrastructure of the wireless communication model

The **ad-hoc** model is used so that devices are interconnected with each other in point-to-point topology.

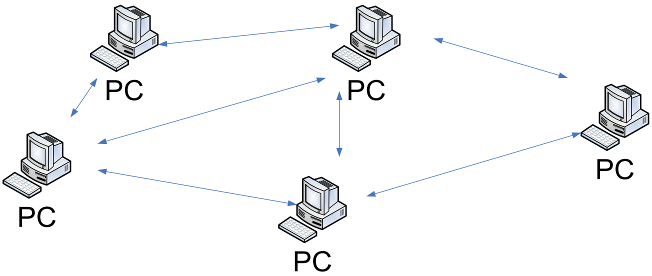


Figure 9. Ad-hoc wireless communication model

Network communication media

A communication channel is needed to transfer data from a sender to a receiver over certain communication media. Communication media can be wired or wireless.

Wired communication media

Wired communication media that can be used consists of copper based pairs, coaxial cables, or fibre optic cables.

Twisted pairs made of copper are used for WAN and LAN technologies. These cables are produced as Unshielded Twisted Pairs (UTP) and Shielded Twisted Pairs (STP). Coaxial cables, called thin net and thick net, can be used to transfer data. Because copper cables are prone to electromagnetic interference, STPs with a metal shield around twisted pairs are used to reduce external noise. With the goal of providing higher frequencies and data transfer speeds, different categories of twisted pair cables are introduced, which allows for high data rate transfer over Ethernet segments as shown in the table below.

CATEGORY	SHIELDING	TRANSMISSION SPEED 100 METERS SEGMENT	FREQUENCY
Cat 3	UTP	10 Mbps	16 MHz
Cat 5	UTP	10/100 Mbps	100 MHz
Cat 5e	UTP	1000 Mbps / 1 Gbps	100 MHz
Cat 6	UTP / STP	1000 Mbps / 1 Gbps	250 MHz
Cat 6a	STP	10000 Mbps / 10 Gbps	500 MHz
Cat 7	STP	10000 Mbps / 10 Gbps	600 MHz

Table 1. Ethernet cable performance (Ethernet, 2018)

Enhanced twisted pair categories and electronics allow higher frequencies and faster data rates as is shown in Table 2.

Experimental Ethernet	1973	2.94 Mbit/s over coaxial cable (coax) bus
Ethernet II	1982	10 Mbit/s over thick coax.
IEEE 802.3	1983	10BASE5 10 Mbit/s over thick coax.
802.3a	1985	10BASE2 10 Mbit/s over thin Coax
802.3e	1987	1BASE5 or StarLAN
802.3i	1990	10BASE-T 10 Mbit/s over twisted pair
802.3j	1993	10BASE-F 10 Mbit/s over Fiber-Optic
802.3u	1995	100BASE-TX, 100BASE-T4, 100BASE-FX
802.3y	1998	100BASE-T2 100 Mbit/s
802.3z	1998	1000BASE-X Gbit/s Ethernet over Fiber-Optic at 1 Gbit/s
802.3ab	1999	1000BASE-T Gbit/s Ethernet over twisted pair at 1 Gbit/s
802.3ae	2002	10 Gigabit Ethernet over fiber
802.3an	2006	10GBASE-T 10 Gbit/s
802.3aq	2006	10GBASE-LRM 10 Gbit/s Ethernet over multimode fiber
802.3bm	2015	100G/40G Ethernet for optical fiber
802.3bp	2016	1000BASE-T1 – Gigabit Ethernet over a single twisted pair
802.3bs	2017	200GbE (200 Gbit/s) over single-mode
802.3bw	2015	100BASE-T1 – 100 Mbit/s Ethernet over a single twisted pair
802.3by	2016	Optical fiber, twinax and backplane 25 Gigabit Ethernet[6]
802.3bz	2016	2.5GBASE-T and 5GBASE-T – 2.5 Gigabit

Table 2. Ethernet standards (Ethernet IEEE 802.3 Standards, 2018)

Fibre optic cables are used for faster and more reliable communication than with twisted pairs. There are two types of fibre optic cables: single-mode and multi-mode.

Single-mode cables use lasers as the source of light for data transmission while multimode cables use light emitting diode (LED) as a source of light. Single mode cables provide faster communication data rates.

Wireless communication media

For wireless communication Radio Frequency (RF), laser, or infra-red signals can be used.

Weaknesses associated with communication media

Below presented are the weaknesses associated with technology used as communication media. Radio communication and copper based communication media are weaker than fiber optic media because of their physical characteristics.

Technology	Weakness
Coaxial Cable	Easy to Tap Distance sensitive Difficult to modify
Twisted pair	Easy to Tap Easy to splice Cross talk interference
Fiber Optics	
Microwave radio and Radio links	Easy to Tap Interference Noise
Satellite radio link	Easy to Tap interference Noise

Table 3. Communication media weaknesses

Network communication devices

Because network mechanisms such as protocols provide reliable end to end communication, their functions are delivered through all seven layers in the case of the ISO/OSI model, or five layers in the TCP/IP protocol suite.

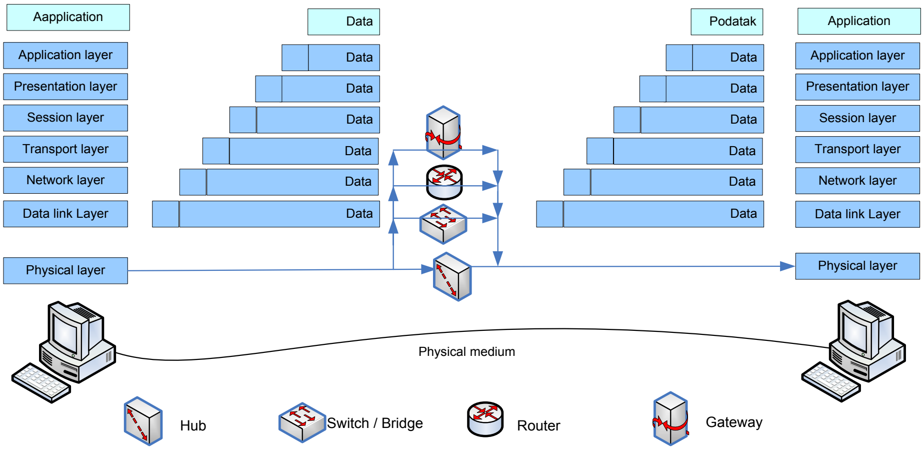


Figure 10. Encapsulation process and communication devices on layers

Every layer of the TCP/IP protocol suite (Figure 4.) has a unique task and that is why special devices were developed to support specific tasks at specific communication layers.

Hubs

Hubs are devices that regenerate and amplify received frames (Protocol Data Unit -PDU at data link layer (InetDaemon, 2018)) and then send them to all device ports. This device is considered as a device which operates on a physical level.

Bridges

Bridges are devices responsible for interconnecting different network technologies, such as IEEE 802.3 and IEEE 802.5, and different network segments with different physical media, such as copper cable networks with coaxial cable networks. Bridges are devices that collect knowledge using internal media access control MAC (InetDaemon, 2018) address tables, which helps them distinguish which device is part of which network segment, thus limiting unnecessary traffic in-between network segments. These devices cannot limit collisions in the network, but can send notifications about existing collisions.

Switches

Switches are, in essence, multiport bridges, and they operate on both the physical and data link level. While early bridges were computers with appropriate software, switches are hardware devices able to provide connections for many computers, where they can send frames in full-duplex mode. Switches separate network segments into different collision domains. They do this using MAC addresses (InetDaemon, 2018) to forward frames, and their major task is to forward and filter traffic.

For network monitoring purposes, a switch can be configured to forward all traffic to one specific port called the SPAN port. Traffic gathered in this way can be analysed frame by frame or can be used to create usage statistics for a specific protocol, application, and other network management purposes explained in later chapters.

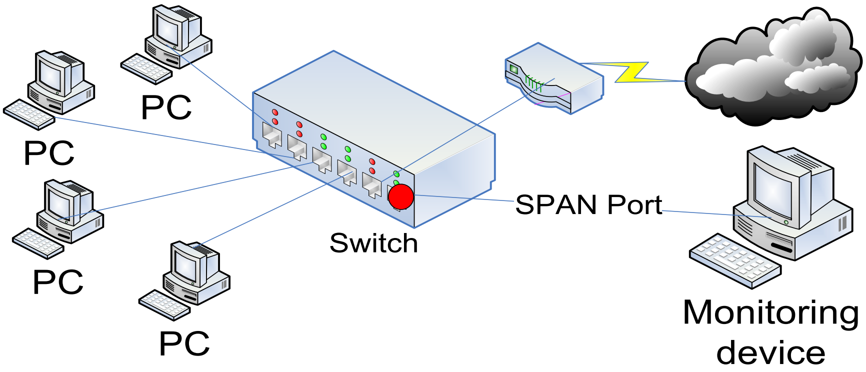


Figure 11. Typical SPAN port deployment in a simplified network diagram

Network TAPs

A Network Terminal Access Point (TAP) is a specialized device used to intercept network communication for the purposes of analysis known as „*traffic analysis*“. It is a device dedicated to intercepting network traffic. At minimum it has three ports: a port for incoming traffic, a port for outgoing traffic, and a port to attach the computer which is used to capture and analyse network traffic.

This device is usually placed on network segments, such as backbones, where major network traffic flows, so that all traffic can be captured or monitored. Specialized traffic analysis software, such as Wireshark (2018) for wired networks and Kismet for wireless networks together with Wireshark (2018), can be used. The usage is explained in later chapters of the book.

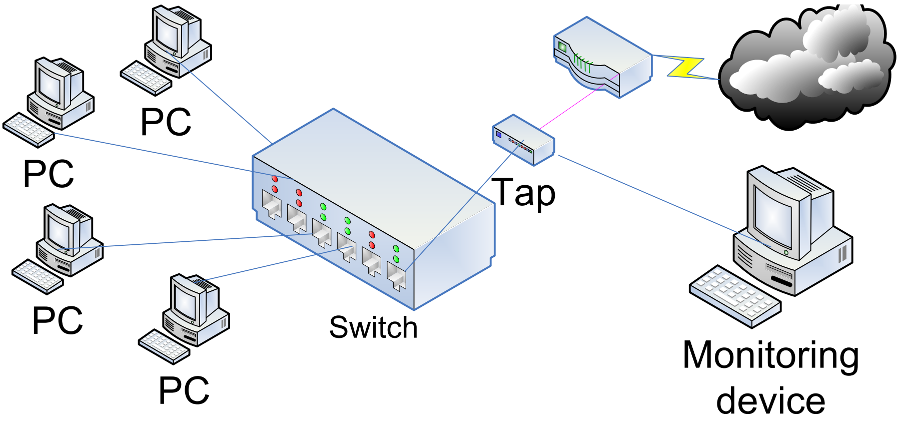


Figure 12. Typical Tap location in network

A network TAP device that can be placed on a UTP network and Fibre optic network segments is shown in the figure below. This specific device has two ports where two monitoring devices can be attached.

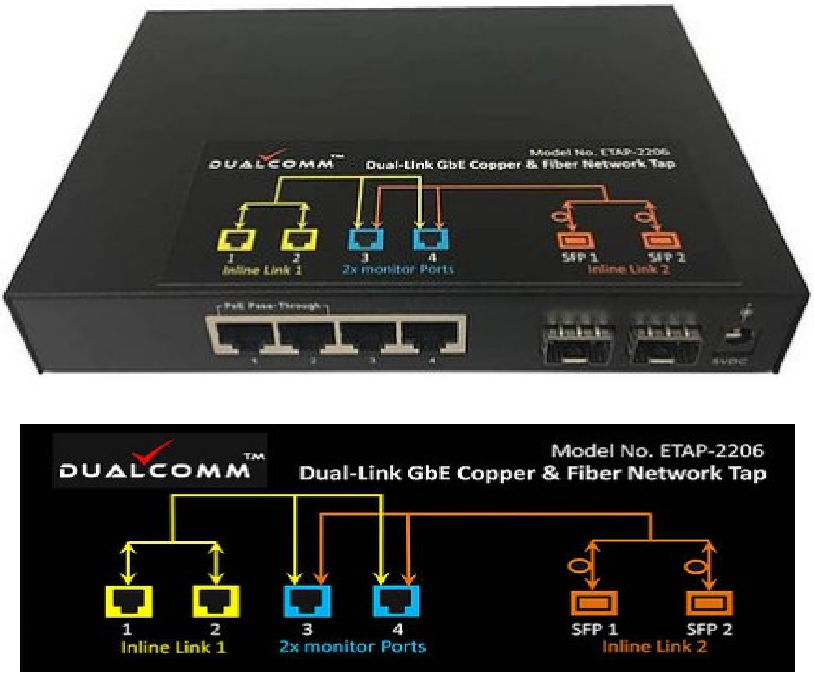


Figure 13. Network TAP, Dualcomm (2018)

Routers

Routers are devices that operate on the network or IP level, as they separate network segments into multiple broadcast domains. Routers operate with logical or IP addresses.

They are equipped with software that allows routers to work with routing protocols which route routed protocols and manage routes so that packets can reach their destinations.

Firewalls

Firewalls are devices which, when deployed between different network segments, are seen as network devices, whereas if they are deployed on client computers, they are called personal firewalls. Their goal is to protect local resources from security breaches.

The primary task of firewalls is to limit access to sensitive internal resources, monitor and record communication, encrypt packets, and provide end-to-end encryption using Virtual Private Networks (VPN) (CISCO, 2018).

There are different types of firewalls (CISA, 2015, pp.368), including packet filtering firewalls, stateful firewalls, application based firewalls which can be implemented through screened-host firewalls, dual-homed firewalls, and hardware based appliances.

Intrusion detection and prevention systems

Firewall intrusion, detection, and prevention systems (IDS/IPS) can be implemented as network-based or host-based systems. The logic which can use these devices includes signature-based, statistical-based, or neural networks as mechanisms for the detection of malicious activities.

IDS/IPS is considered an additional mechanism for detecting malicious attempts against protected and valuable network resources.

These systems have sensors and detection logic that is used to detect malicious activities.

VOIP and PBX

Voice over IP is becoming a dominant form of technology, replacing old PSTN analogue services available from 1920s onwards. VOIP is well-known for its Internet application, using different VOIP services, such as Skype or Viber.

The VOIP private box exchange (PBX) are computer-based switches which are installed at organisation premises with the purpose of switching telephone calls in and out of the organisation.

Network types

There are different classification types for computer communication networks, but the most common is one that recognises coverage for interconnected devices.

BAN

Body area networks that are limited to one meter, and are typically wireless technology used to connect smart phones with smart watches, and sensors inside wearables such as clothes or shoes.

PAN

Personal area networks are limited to 10 meters, and are used to connect nearby devices, such as Bluetooth enabled devices.

LAN

A typical local area network segment spans 100 meters, but can be extended up to 400 meters using hubs, bridges, and switches, and even further using routers. Wireless LAN (WLAN) can be used to connect access points below 100 meters, but using point links these networks can be interconnected over tens of kilometres.

SAN

Storage area networks (SAN) or network area storage (NAS) are used to provide data storage on LANs for users. These devices can be configured to have locally managed users or they can incorporate an already available authentication scheme.

WAN

A Wide area network is considered a network which is used to connect all type of IT devices across a wide area in different regions in a country or even between countries. Internet is usually referred to as a WAN network

A special type of WAN is wireless LAN (WLAN), which uses wireless technology to interconnect communication sites within same town.

MAN

Metropolitan area network is used to interconnect LANs across a city to connect different buildings of, for example, a university campus with parts of the university located in the same town on fiscally different location.

Network terminal devices

Network terminal devices are devices where communication ends. They are also a well-known part of Claud Shannon's communication model (Businesstopia, 2018), called sending-receiving stations.

Supercomputers

Supercomputers are computers dedicated to a specific problem or application where huge processing power is needed. The need dictates the high prices of these computer systems, and as such they are mostly used by research or military organisations.

Mainframes

Mainframes are computers which are used by thousands of users, and which usually have dedicated operating systems. Usually these computers support multiprocessor architectures.

High-end and midrange servers

These servers use operating systems such as UNIX, Linux, and Windows. They are cheaper than mainframes, but share some capabilities of mainframes.

Supercomputers, mainframes, and servers have to be located in air-conditioned rooms with uninterruptable power supply (UPS), electric generators, and redundant power supply from independent supply grids which are apart from the primary power grid. It is because all critical components have to be available all the time if possible.

Personal computers

Personal Computers are designed for single users. They use microprocessor architecture with almost all the components that servers have, such as a hard disk and multiprocessors, but with weaker performances than servers. They are used for word processing, access to common business applications, and network resources such as printing services or intranet.

Thin client computers

Thin client computers have limited hardware capacity, and are often without hard disks. They use network storage from servers or dedicated network area storage devices. They are, much like personal computers, used for personal use to common applications.

Laptop computers

Laptops are smaller, lightweight personal computers, suitable to be carried in a suitcase.

Smartphones and handheld computers

Smartphones, tablets, and other handheld computers are devices lighter than laptops with high processing power, usually without keyboards to make for easier carrying. They can be used as telephones, organisers, PCs, tablets, as means of communication, voice messages, or as a VOIP communicator using Skype, Viber, and other similar tools.

IoT

Internet of Things describes all devices connected to the Internet which are not considered as conventional as PC, laptop, or smartphones. These devices are, for example, IP cameras, VOIP telephones, and even household devices, such as refrigerators, which have an Internet connection that allows users to interact with the devices.

Network services

Network services enables network users to access network resources as they are locally available. They run as daemons on Linux/Unix platforms, or as a service on Windows platforms.

NFS

Network File Systems (NFS) allows users of computer networks to access files over network resources.

DHCP

Dynamic Host Configuration Protocols (DHCP) enable devices which do not have manually configured IP addresses to obtain an IP address, subnet masks, default gateways, and IP address DNS servers from the DHCP service which can be located on the server or on another device, such as a router.

Client devices have to be configured as a DHCP client which initial DHCPs discover as a broadcast request to which available DHCP servers reply with the offer of an IP address, subnet mask, default gateway, or DNS addresses. After that, the client requests one of the offered addresses, and the DHCP acknowledge the given and accepted set of addresses.

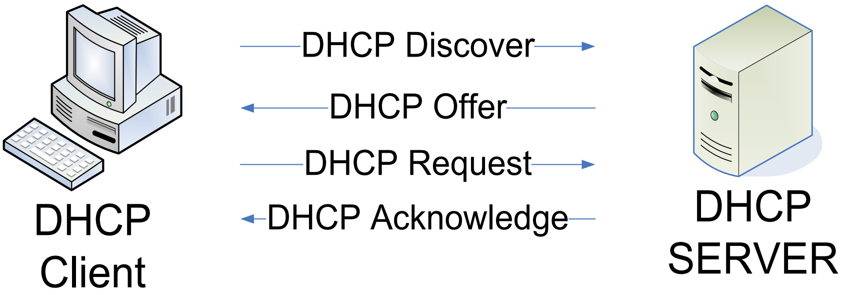


Figure 14. Simple DHCP architecture and modus operandi

E-mail

E-mail service provides the service of exchanging e-mail messages on intranets and Internet using SMTP, IMAP, and POP3 protocols. Common server programs send mail on Unix/Linux servers or MS Exchange servers. A typical email architecture contains three types of agents (an agent in this context is the software which provides a specific function for somebody):

Mail User Agent (MUA)

MUA is software installed on end-user devices or accessed as a web service (webmail such as Gmail), which is used to read and compose emails

Mail Transfer Agent (MTA)

MTA is software on the server side of the application which receives emails from MUA and checks with MDA if the recipient is in the local mail address box. If not , the email is sent to another receiving MTA based on the DNS name and the resolved IP address. All emails are transferred using the Simple Mail Message Protocol (SMTP) which uses TCP port 25.

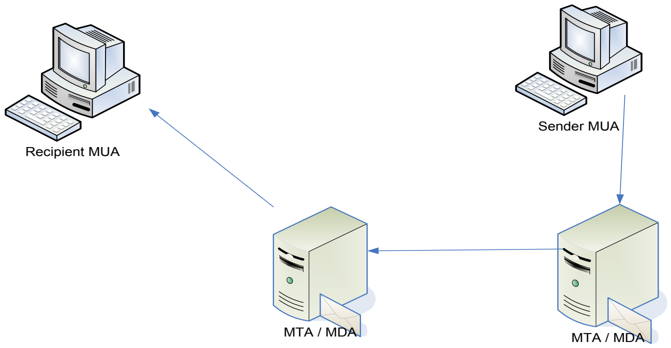


Figure 15. Simple MUA, MTA, MDA architecture

Mail Delivery Agent (MDA)

MDA is software responsible for delivering emails to local mailboxes, so that local users can use MUA to access emails. Mails accessed by MUA to MDA use POP3 or IMAP protocols.

Print service

Print services allow users to use network printers in the organisation in accordance with the given promotions. This type of service provides better management of resources from a single management point. Printers are of communicating via IP, and all status messages such as low toner or paper can be sent directly to administrators, so that problems of missing resources can be resolved proactively. Users of print services can choose which printer they want to use, such as black and white or colour printers.

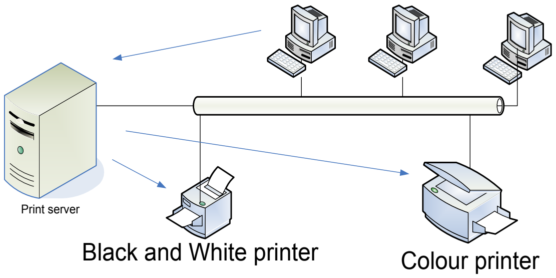


Figure 16. Simple network printing service

Print servers allow the storage of printed files for a specific amount of time so that documents can be printed later, again, or to check what was already printed.

RAS

Remote Access Service (RAS) provides direct access to local network resources to authorized users. This access was popular from the beginning of the computer network era when access was provided with WAN technologies, usually via Public Switched Telephone Networks (PSTN), and later with Integrated Switched Telephone Networks (ISDN).

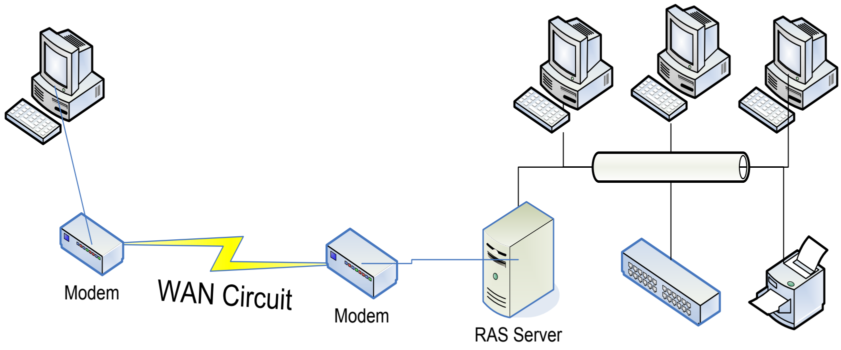


Figure 17. Simple RAS architecture

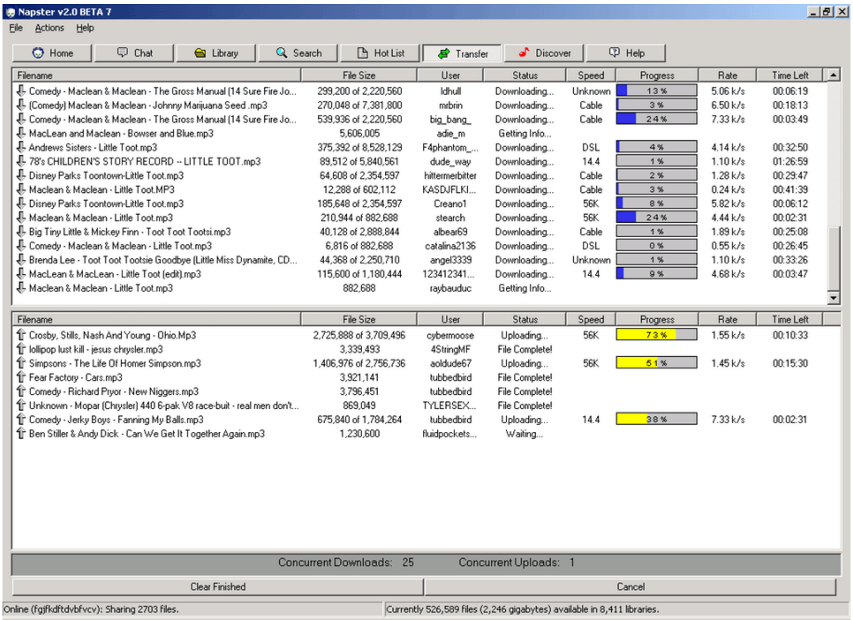
Nowadays, due to available Internet connections, the Internet and VPNs are a common way of securely connecting to remote networks.

Directory services

Directory service provides user authentication and access to network resources such as shared files, directories, printers, applications, and other network resources.

Peer-to-Peer services and applications

With the expansion of the Internet, P2P models were used with common applications that share files, such as music, videos, and other resources. One of the pioneering peer-to-peer (P2P) file sharing services was Napster (2018), established in 1999.



Filename	File Size	User	Status	Speed	Progress	Rate	Time Left
Comedy - Maclean & Maclean - The Gross Manual (14 Sure Fire Jo...	299,200 of 2,220,560	ldhull	Downloading...	Unknown	13 %	5.06 k/s	00:06:19
(Comedy) Maclean & Maclean - Johnny Marijuana Seed .mp3	270,048 of 7,381,800	mrbrin	Downloading...	Cable	3 %	6.50 k/s	00:18:13
Comedy - Maclean & Maclean - The Gross Manual (14 Sure Fire Jo...	539,936 of 2,220,560	big_bang_	Downloading...	Cable	24 %	7.33 k/s	00:03:49
MacLean and Maclean - Bowser and Blue.mp3	5,606,005	adie_m	Getting Info...				
Andrews Sisters - Little Toot.mp3	375,392 of 8,528,129	F4phantom_...	Downloading...	DSL	4 %	4.14 k/s	00:32:50
78's CHILDREN'S STORY RECORD -- LITTLE TOOT.mp3	89,512 of 5,840,561	dude_way	Downloading...	14.4	1 %	1.10 k/s	01:26:59
Disney Parks Toontown-Little Toot.mp3	64,608 of 2,354,597	hittermerbitter	Downloading...	Cable	2 %	1.28 k/s	00:29:47
Maclean & Maclean - Little Toot.MP3	12,288 of 602,112	KASDJFLKI...	Downloading...	Cable	3 %	0.24 k/s	00:41:39
Disney Parks Toontown-Little Toot.mp3	185,648 of 2,354,597	Creano1	Downloading...	56K	8 %	5.82 k/s	00:06:12
Maclean & Maclean - Little Toot.mp3	210,944 of 882,688	stearch	Downloading...	56K	24 %	4.44 k/s	00:02:31
Big Tiny Little & Mickey Finn - Toot Toot Tootsi.mp3	40,128 of 2,888,844	albear69	Downloading...	Cable	1 %	1.89 k/s	00:25:08
Comedy - Maclean & Maclean - Little Toot.mp3	6,816 of 882,688	catalina2136	Downloading...	DSL	0 %	0.55 k/s	00:26:45
Brenda Lee - Toot Toot Tootsie Goodbye (Little Miss Dynamite, CD...	44,368 of 2,250,710	angel3339	Downloading...	Unknown	1 %	1.10 k/s	00:33:26
MacLean & MacLean - Little Toot (edit).mp3	115,600 of 1,180,444	123412341...	Downloading...	14.4	9 %	4.68 k/s	00:03:47
Maclean & Maclean - Little Toot.mp3	882,688	raybauduc	Getting Info...				

Filename	File Size	User	Status	Speed	Progress	Rate	Time Left
Crosby, Stills, Nash And Young - Ohio.Mp3	2,725,888 of 3,709,496	cybermoose	Uploading...	56K	73 %	1.55 k/s	00:10:33
lollipop lust kill - jesus chrysler.mp3	3,339,493	4StringMF	File Complete!				
Simpsons - The Life Of Homer Simpson.mp3	1,406,976 of 2,756,736	aoldude67	Uploading...	56K	51 %	1.45 k/s	00:15:30
Fear Factory - Cars.mp3	3,921,141	tubbedbird	File Complete!				
Comedy - Richard Pryor - New Niggers.mp3	3,796,451	tubbedbird	File Complete!				
Unknown - Mopar (Chrysler) 440 6-pak V8 race-buit - real men don't...	869,049	TYLERSEX...	File Complete!				
Comedy - Jerky Boys - Fanning My Balls.mp3	675,840 of 1,784,264	tubbedbird	Uploading...	14.4	38 %	7.33 k/s	00:02:31
Ben Stiller & Andy Dick - Can We Get It Together Again.mp3	1,230,600	fluidpockets...	Waiting...				

Concurrent Downloads: 25 Concurrent Uploads: 1

Online (fgjfkdftdvbfvcv): Sharing 2703 files.

Currently 526,589 files (2,246 gigabytes) available in 8,411 libraries.

Figure 18. Napster (2018)

Napster was specialized in sharing mp3 music files and had about 80 million registered users. According to (Lamont T., 2013) *"The digital music revolution started with Napster"* but the service was closed in 2001 due to a lawsuit for illegal sharing of copyrighted materials.

FTP

File Transfer Protocol (FTP) is used to store or retrieve files and folders from and to FTP servers.

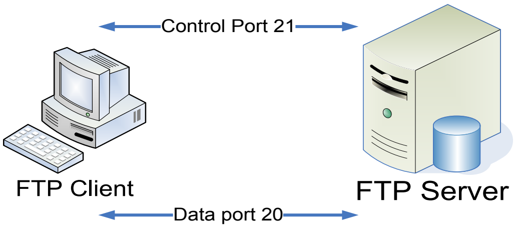


Figure 19. Simple FTP architecture

FTP uses TCP protocols with two ports, 20 and 21. FTP is most frequently used to transfer username and password in clear text if additional encryption is not used.

Telnet

Telnet is a service used to access remote devices via TCP/IP using TCP port 23.

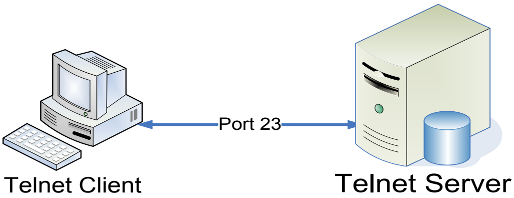


Figure 20. Simple Telnet architecture

It allows for two-way bidirectional communication. The protocol was developed in 1969 and is still used today by many communication and terminal devices.

VPN

Virtual Private Networks provide confidentiality and integrity of data over unsecured networks, such as Internet, by providing point-to-point data encryption.

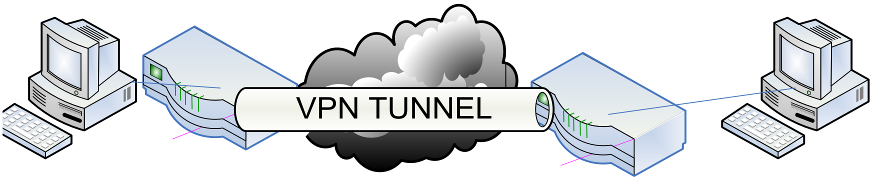


Figure 21. Simplified VPN connection

Communication ports used

Every service that acts as a server in the client/server architecture has a predefined port, i.e. a specific service use which the client application can use to connect.

Application / Service	Acronym	Port
Simple Network Management Protocol	SNMP	161, 162
Domain Name System	DNS	53
Hypertext Transfer Protocol	HTTP	80
Simple Mail Transfer Protocol	SMTP	25
Post Office Protocol	POP3	110
Telnet	Telnet	23
Dynamic Host Configuration Protocol	DHCP	67
File Transfer Protocol	FTP	20, 21

Table 4. Applications / Services and standard ports used

Network management

Network management provides capabilities of reactively and proactively maintaining network components. ISO published a standardized approach to network management which contains the architecture and modelling known as the ISO model and *Telecommunications Management Network* (TMN) framework (Overview of TMN Recommendations, 2001) for network management (Sahin T. et. al., 1988). There is also the IETF IP Performance Management (IPPM) (IPPM, 2018) Working Group (WG) which developed a number of standards and metrics for IP-based networks. In essence, there are two types of network monitoring which are part of network management: passive and active network monitoring. These two approaches are complementary. However, when performing passive monitoring, active monitoring should be turned off, because it will otherwise produce additional network traffic. Using both approaches, monitoring results are more accurate.

Passive monitoring

Passive monitoring can be done using SPAN ports and Tap devices to capture/sniff and analyse network traffic using software such as Wireshark (2018).

Another way of gathering valuable information is by using Simple Network Management Protocols (SNMP) to poll devices such as routers, switches, and servers that have installed SNMP agents with the Management Information Base for information on traffic, such as the number of IP, TCP, and UDP packets.

It is possible to configure devices to send trap messages when specific events occur. Netflow is a passive monitoring mechanism which is able to provide the network manager with valuable statistical information.

RMON is also a passive monitoring mechanism which is used to manage devices on network segments with limited bandwidth capacities.

Active monitoring

The IETF IP Performance Management (IPPM, 2018) Working Group (WG) was formed in 1997 with the task of developing metrics as Key Performance Indicators (KPI) and standards for active monitoring in the performance management of IP networks

History of network management

Three major organisations ISO, IETF, IETF, developed approaches and protocols specific for network management with the different focus to reach specific goals. Each organisation set up their own goals presented below in each row of the table.

ISO	ITU-T	IETF
Powerful Management	Define management architecture only	Simple Management
Object Oriented	Using OSI protocol (CMIP & CMIS)	Variable Oriented
Reliable transport	Out-of-band exchanged Management Information	Unreliable transport

Table 5. ISO, ITU-T, IETF basic principles

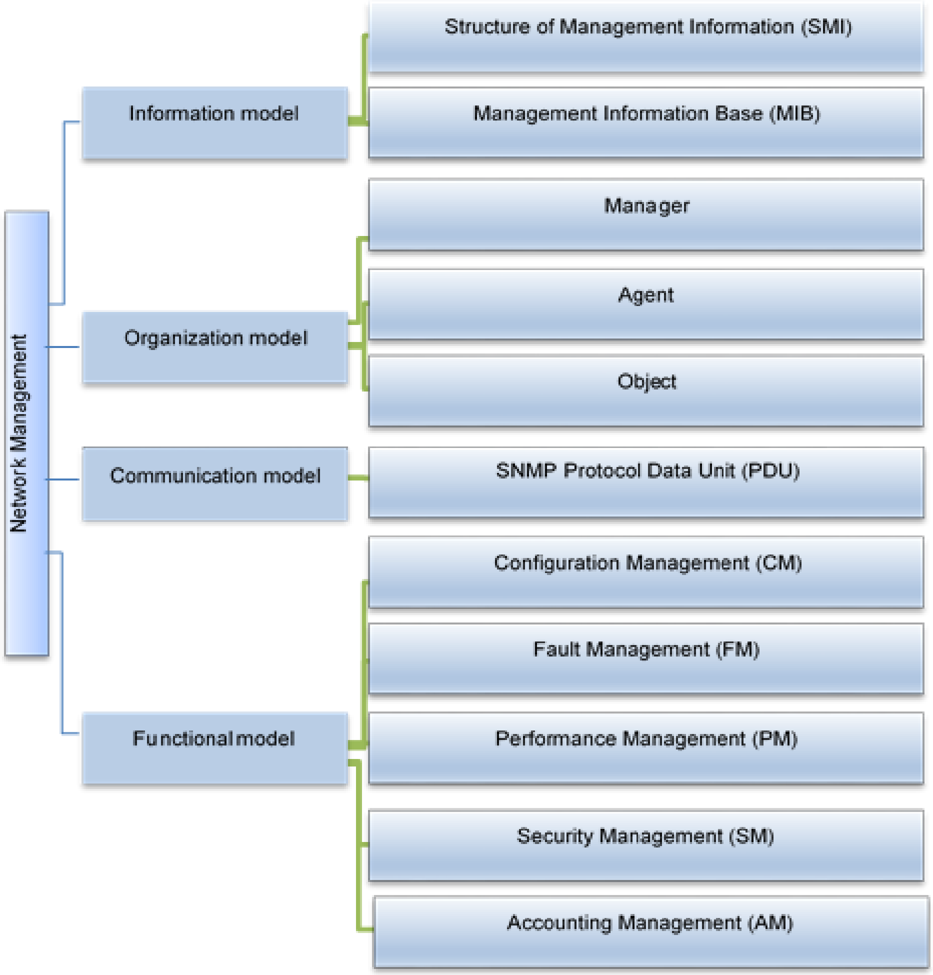
ISO developed model and framework for network management based on five functional areas: Fault, Configuration, Accounting, Performanse, and Security (FCAPS). Based ond FCAPS model, newer FAB model is defined in the Business Process Framework (eTOM, 2018).

ITU-T developed Telecommunications Management Network (TMN) for managing open systems in a communications network. Goal was to automate process of detecting and resolving problems in telecommunication networks.

IETF defined set of standards that defined SNMP and application layer protocol, data objects, and database schema.

OSI model and framework for network management

This model recognises five areas of functional management: Fault, Configuration, Accounting, Performance, and Security (FCAPS) (Nuangjamnong C, 1998).



Network Management
Information model
Organization model
Communication model
Functionalmodel
Structure of Management Information (SMI)
Management Information Base (MIB)
Manager
Agent
Object
SNMP Protocol Data Unit (PDU)
Configuration Management (CM)
Fault Management (FM)
Performance Management (PM)
Security Management (SM)
Accounting Management (AM)

Figure 22. Network Management history IETF, ISO Network Management architecture and model (Nuangjamnong C, 1998).

Additionally, it proposes an organisation model which contains a manager, an agent, and an object. OSI FCAPS model turned out to be used for education purposes just as ISO OSI communication model.

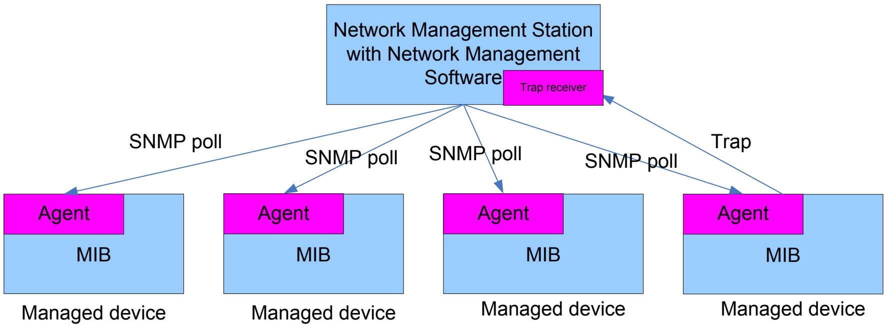


Figure 23. Network Management architecture using SNMP, (Nuangjamnong C, 1998).

The communication protocol used for *Telecommunications Management Network* (TMN) is the Simple Network Management (SNMP) protocol which can access SNMP agents on devices such as switches, routers, servers, and personal computers. SNMP agents send their queries locally to the Management Information Base (MIB) which contains information on running services, applications, status of connections, and other useful information.

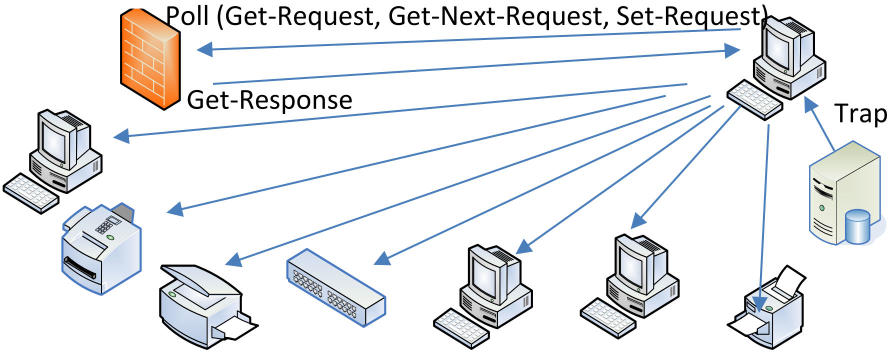


Figure 24. Network Management surrounding

A Network management station (NMS) with the appropriate network management software uses SNMP protocols to periodically poll data from managed resources or to receive traps if the predefined event occurs on the managed device.

Using SNMP protocols equipped with command sets, NMS can collect information from MIB using different commands. SNMP uses UDP and port 161 for poll requests, and port 162 for Traps.

Rmon Groups (1.3.6.1.2.1)	
Statistic Group (1)	Traffic Matrix Group (6)
History Group (2)	Filter Group (7)
Alarms Group (3)	Capture Group(8)
Hosts Group (4)	Events Group (9)
Host Top N Group (5)	

Table 6. RMON Groups (Cisco Remote Monitoring, 2018)

As mentioned, when it comes to networks with limited bandwidth capacities, RMON is used to minimize the SNMP poll impact on bandwidth resources. This mechanism allows periodic access to already locally prepared reports about reports, most frequently used protocols/application/devices and network resources, and other useful information.

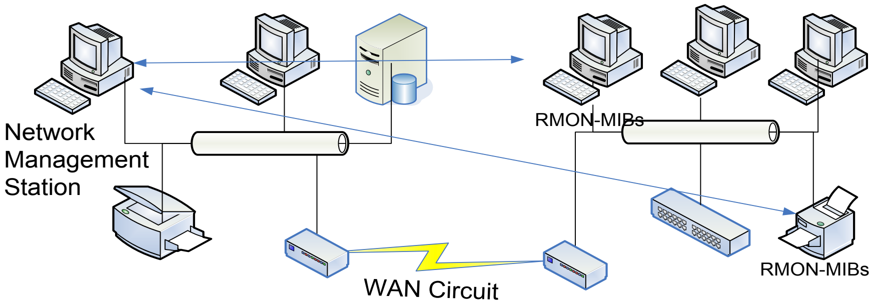
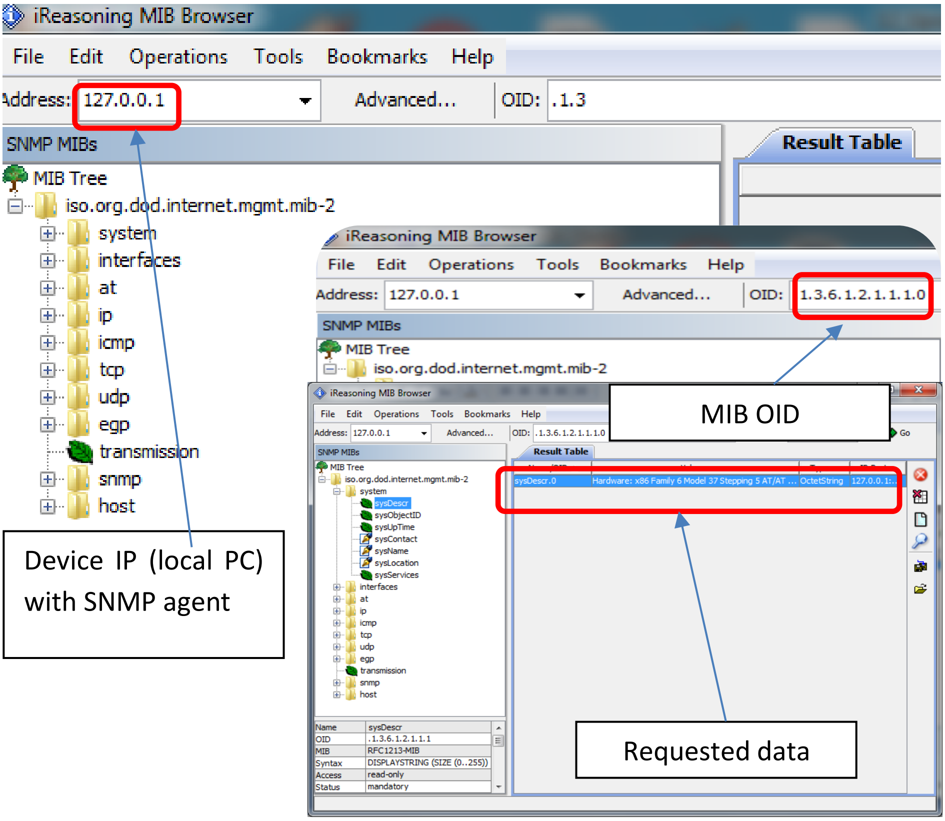


Figure 25. Simple RMON architecture

SNMP version 3 is equipped with the following set of commands: get, getnext, set, getresponse, trap, getbulk, notification, inform, report.



Address: 127.0.0.1 OID: .1.3

Address: 127.0.0.1 OID: 1.3.6.1.2.1.1.1.0

Address: 127.0.0.1 OID: .1.3.6.1.2.1.1.1.0

sysDescr.0	Hardware: x86 Family 6 Model 37 Stepping 5 AT/AT ...	OctetString	127.0.0.1:..

Name	sysDescr
OID	.1.3.6.1.2.1.1.1
MIB	RFC1213-MIB
Syntax	DISPLAYSTRING (SIZE (0..255))
Access	read-only
Status	mandatory

Figure 26. Example query using iReasoning MIB Browser

Information in MIBs can be accessed using different tools. The lightest ones are MIB query tools such as iReasoning, (shown above) which is used for querying the system description of the local PC.

Summary

Cyber and information components and infrastructures which use the TCP/IP protocol suite provide common services such as VOIP, NFS, DHCP, E-mail, Print, RAS, and Directory services. Services are supported by different network technologies such as BAN, PAN, LAN, SAN, WAN, and MAN. Network infrastructures are built using network communication devices such as Hubs, Bridges, Switches, Routers, PBX and Firewalls, and protected using intrusion detection and prevention systems. All network devices can be managed by implementing network management solutions such as the ISO *Telecommunications Management Network* (TMN) model and an appropriate framework for network management.

Knowledge acquired

In this chapter, the reader can gain knowledge about network topologies, network media, protocols and services, and network devices and their interoperation. The reader can also learn about network management purposes and activities that can help in day-to-day network operations meant to support cyber security.

Review questions

1. Explain the difference between active and passive monitoring?
2. What is a TAP device and what is it used for?
3. What is a SPAN port and what is it used for?
4. Define the network functional model, and explain each management area?
5. Explain the difference between polls and traps?
6. What is a communication port?
7. Describe weaknesses associated with communication media?
8. Explain the role of MUA, MTA, and MDA in e-mail communication?

9. Explain the difference between HUB and Switch operations?

10. Explain the difference between infrastructure and the ad-hoc wireless communication model?

11. What is network topology?

Further readings

- ISO/IEC 27000 family - Information security management systemshttps://www.iso.org/isoiec-27001-information-security.html

- TCP/IP vs. OSI: What's the Difference Between the Two Models? https://community.fs.com/blog/tcpip-vs-osi-whats-the-difference-between-the-two-models.html

- Network Topology https://study.com/academy/lesson/how-star-topology-connects-computer-networks-in-organizations.html

- Communication Media (Data Communications and Networking) http://what-when-how.com/data-communications-and-networking/communication-media-data-communications-and-networking/

- Communication device https://www.computerhope.com/jargon/c/communication-devices.htm

- Network Taps, Regenerator Taps, and Tap Aggregators https://www.ixiacom.com/products/network-taps-regenerators-and-aggregators

- What Is a Firewall? https://www.cisco.com/c/en/us/products/security/firewalls/what-is-a-firewall.html

- What is IDS and IPS? https://www.juniper.net/us/en/products-services/what-is/ids-ips/

- Network Management System: Best Practices White Paper

https://www.cisco.com/c/en/us/support/docs/availability/high-availability/15114-NMS-bestpractice.html

- What's on Your Network? The Need for Passive Monitoring http://www.tomsitpro.com/articles/network_monitoring-netflow-it_security-networking-snmp,2-561-2.html

3. Cyber security landscape

Chapter abstract

Chapter goals: To explain core information security principles, to define cyber security incidents and motivations, to present common cyber security threats, to define cybercrime, to present different malicious software and distinguish passive from active attacks, to explain what is fraud and present the deep and dark web, and to present tools used, such as TOR, and their operations. Finally, to explain penetration testing principles and ethical hacking techniques and tools.

Learning outcomes: Acquiring knowledge of information security and understanding the aspect of information security related to cyber security. Raising awareness of cyber threats and possible mitigations and strengthening organisation resilience using ethical hacking techniques.

Fundamental aspects of cyber and information security

The fundamental aspects of information security are usually divided into Confidentiality, Integrity, Availability, Authenticity, and Non-Reputability. Because information can be stored and transferred in different shapes, its security depends on the security of tools, utilities, people, hardware, software, and means of transfer. All of them are considered information assets, and are subject to fundamental security aspects. As stated in the introduction, ISO 27000 27000 (ISO 27001:2013, ISO 27005:2008, and other) standards consider Confidentiality, Integrity, Availability as the fundamental aspects of information security, whereas some other formal approaches and authors (Vigila et al., 2015) consider

Authenticity, and Non-Reputability as important aspects for managing information security.

Information security core principle	**Description**
Confidentiality	Information assets can be electronic, non-electronic, or spoken. Information can be stored or can be transferred over communication links. In any state, the confidentiality of information can be jeopardized if not protected.
Integrity	Information can be changed or destroyed by an unauthorized person or information assets can be destroyed. This is connected to integrity principles of information security. That is why all information transferred over communication lines and stored on hard disks and other media has to be protected so that integrity is guaranteed by technical and organisational mechanisms and internal controls.
Availability	Information and information assets have to be protected so that they are available for access and use. Information processing facilities have to be protected so that the business is resilient to minor and major possible outbreaks due to internal or external impacts.
Authenticity	Authenticity has to guarantee the truthfulness of the origin of information.
Non-Repudiation	This principle is related to the authenticity of information so that the creator originator of specific information cannot deny that specific information originates from a specific person.

Table 7. Information security core principles (ISO 27001:2013 and Vigila et al., 2015)

Cyber security incidents and motivations

Financial theft, access to resources, competitive advantage (economic, political), personal grievances, vengeance, intellectual or other curiosity, mischief, personal or group attention (CNSCENTER, 2000), and fraud, are some of the most common reasons for cyber and information security criminals to conduct their criminal acts. In all attacks, it is clear that the attackers have a specific goal which depends on motivations. Attackers have dangerous and destructive goals of stealing money and data, or destroying the victim's data and other digital resources, as well as some less dangerous goals motivated by curiosity, intellectual challenge, or learning about system resources

Because of potential destructive consequences, every attempt or preparation for attack has to be seriously considered by examining all the early indicators of unpatched equipment, uncontrolled areas of infrastructure, lack of monitoring logs, or unexpected events in the area of administration.

Many organisations can survive cyber and information security attacks due to their nature and position explained below, but many privately owned companies are not that lucky and their businesses get terminated or seriously damaged. On a personal level, it is almost certain that individuals responsible for cyber and information security will be object of disciplinary or other legal action.

Common cyber threats

It is clear that cyber threats affect different victims, including individuals, corporations, and critical and vital national infrastructures. There are different types of threats used for different purposes.

Cybercrime is a connected criminal activity which uses digital technology to commit criminal activity such as ransomware, data theft, and virus creation and distribution. These types of attacks are performed by individuals or groups.

Cyber industrial espionage is performed against corporations and institutions with the goal of stealing data and producing damage.

Cyber warfare is usually conducted on critical state infrastructure, including such examples as the Stuxnet (2010), (Mueller P. and

Yadegari B., 2012) virus, or attacks on Iranian or Estonia's critical national infrastructure (Iasiello E, 2013).

Malicious software – history and types

As explained by Microsoft, (2003) malware is short for malicious software which includes viruses, macro viruses, worms, Trojans, logic bombs, ransomware, rogue adware, adware, and spyware.

Malwares are created to infect as many computer resources as possible, to perform specific tasks such as stealing data, deleting data, or even stealing money. Malicious software has its roots in automated organisations proposed in John von Neumann's article, "*Theory of self-reproducing automata*"(Von Neumann, J., and Burks, Arthur W., 1966)

A **Virus** is malicious program able to replicate itself with the goal of infecting other files after it is executed. Viruses can affect computer systems in different ways, such as file deletion, change, or sending spam mails. The concept of self-replicating software was proposed "Theory of self-reproducing automata"*(Von Neumann, J., and Burks, Arthur W., 1966)*

Macro viruses appeared in mid-nineties with the goal of infecting Microsoft files created in Word, Excel, and other Microsoft created documents.

Worm, as a term connected to computers, was first mentioned in The Shockwave Rider, written by John Brunner (Brunner J., 1975). Brunner used the word "worm" for a program which can propagate through a computer network by itself. The first worm that was spread over the Internet was created by Robert Morris (Eisenberg T.et al, 1989).

Below is a table created based on Wikipedia (2018) with a short history of software related to malicious software.

1949	John von Neumann's article on the "Theory of self-reproducing automata“ published.
1971	Experimental self-replicating program *The Creeper*.
1973	Michael Crichton movie *Westworld* mentions the concept of a computer virus.
1974	*The Rabbit* (or Wabbit) virus
1975	ANIMAL
1981	*Elk Cloner*
1983	The term "virus" is coined by Frederick Cohen in describing self-replicating computer programs.
1986	The Brain boot sector virus is released.
1987	Vienna virus, Lehigh virus, Jerusalem virus, SCA virus, Christmas Tree EXEC,
1988	The Morris worm, created by Robert Tappan Morris,
1989	Ping-Pong virus, CyberAIDS and Festering Hate Apple ProDOS AIDS Trojan, the first known ransomware, Ghostball,
1990	Vienna and Cascade, Form viruses,
1992	The Michelangelo virus
1993	Leandro or Leandro & Kelly and Freddy Krueger
1994	OneHalf
1995	The first Macro virus, called "Concept"
1996	"Ply" Boza, Laroux, Staog the first Linux virus attacks Linux machines
1998	CIH virus
1999	The Happy99 worm, The Melissa, The ExploreZip worm, The Kak worm
2000	The ILOVEYOU worm, The Pikachu
2001	The Anna Kournikova, Sadmind worm, The Sircam worm, The Code Red worm, The Nimda worm, The Klez worm
2002	The Simile virus, Mylife
2003	The SQL Slammer worm, Graybird is a trojan horse, ProRat trojan horse, and worms: The Blaster, The Welchia (Nachi), The Sobig, Swen worm, The Sober, Agobot, Bolgimo
2004	Bagle, The MyDoom worm, The Netsky worm, The Witty worm, The Sasser worm, Caribe or Cabir, Nuclear RAT backdoor trojan, Vundo, or the Vundo Trojan, Bifrost, Santy,
2005	Zotob, The Zlob Trojan
2006	The Nyxem worm, OSX/Leap-A or OSX/Oompa-A, Brontok, Starbucks,Stration or Warezov worm
2007	Storm Worm, Zeus
2008	Mocmex is a trojan, Torpig Trojan horse, Rustock.C, Bohmini.Ar trojan, The Koobface computer worm, Computer worm Conficker
2009	W32.Dozer, Daprosy Worm, Source code for MegaPanzer
2010	Waledac botnet, The Psyb0t worm is discovered, Alureon Trojan, Stuxnet, a Windows Trojan, "VBMania", Kenzero
2011	SpyEye and Zeus, The Morto worm, the ZeroAccess rootkit, Duqu is a worm
2012	May: Flame or Flamer, sKyWIper, and Skywiper, Shamoon NGRBot
2013	The CryptoLocker Trojan horse, The Gameover ZeuS Trojan, Linux.Darlloz
2014	The Regin Trojan horse
2015	The BASHLITE, Linux.Wifatch
2016	Ransomware Locky, Tiny Banker Trojan, Mirai
2017	The WannaCry ransomware attack, The Petya (malware) attack, Kedi RAT (Remote Access Trojan)
2018	Spectre and Meltdown Flaws

Table 8. Short timeline of major malicious software appearance based on Wikipedia (2018) information

Trojan is a program that was first created in 1975 as a non-malicious program. In 1989 the first known ransomware Trojan was created (Lord N., 2018). In the late nineties, Trojan was used to create backdoors on computer systems which were then used by attackers to exploit systems and system resources.

Spyware are programs that infect computer systems and collect information about user behaviour with the goal of offering products or steal data such as usernames, passwords, and bank account details.

Logic bombs can be software on their own or incorporated into existing applications. They are software that accomplishes malicious intents when specific conditions are met. A typical example would be when a disgruntled programmer incorporates malicious software into the existing organisation's application that deletes files or do other harm to organisation's information technology resources when the following criteria in the database is met: „programmer's name and surname“ is locked as a result of termination from the company (CISA 2015, pp. 349).

Ransomware is a malware that encrypts user's files and on behalf of the attacker request ransom to be paid for a key to decrypt the encrypted files Cowing J. (2015).

Passive and Active attacks

Passive attacks are used to intercept communication between two ending nodes which participate in communication. Passive attacks are different across wired and wireless networks, since for wired networks a tap device which is physically placed on a network segment is needed to the capture packets, whereas for wireless networks appropriate software and hardware with antenna is needed. The goal of passive attacks is gathering specific information, such as passwords and data in transit. That is why the main objective of passive attacks is to target confidentiality of information in transit (CISA 2015, pp 380).

Active attacks include active actions meant to harm specific systems by intruding in or interrupting system operations. Whilst the goal of passive attack is to jeopardize confidentiality only, active attacks target integrity (change of data and information), availability, and confidentiality as well (CISA 2015, pp. 350).

Masquerading

Masquerading is an active type of attack by presenting the identity of somebody else with the goal of accessing resources in an unauthorised way by impersonating people or machines (CISA, 2015. pp 350).

Man in the middle attacks

Man in the middle attacks (MITM) target the communication between two communicating entities by secretly relaying and possibly altering that communication. In MITM, the attacker is attempting to play an active part in the communication (CISA 2015, pp. 349).

Message modification

Message modification is an active type of attack where the attacker changes the content of the message, such as a bank invoice or payment transaction (CISA 2015, pp. 350).

Eavesdropping

Eavesdropping is a passive type of attack where the attacker gathers information from network with the goal of acquiring data related to login and password sessions (usernames and passwords), e-mail content, and keystrokes. This type of activity provides the attacker with credentials to access sensitive resources (CISA 2015, pp. 348).

Intrusion attacks

Intrusion attacks are active types of attacks where the goal is to make an active impact on the targeted system, such as to find system passwords and manipulate (change or steal) data.

Packet reply

This type of attack has attributes of both active and passive attacks. It is conducted by listening (sniffing) to the network traffic and recording it, which is the passive aspect of the attack. The active aspect of the attack is to send the recorded network traffic, usually for the purpose of authentication, sending encrypted passwords, and to continue to use authenticated sessions avoiding decrypting passwords (CISA 2015, pp. 350).

Spoofing

Attackers use this method to masquerade their presence on the network as somebody else by falsifying data, such as the IP address, to gain privileges or data such as passwords (CISA 2015, pp. 349).

Pharming

This type of attacks redirects requests from a web site to other web sites which were prepared by the attacker. For example, a web site which looks like the exact or genuine web site of the attacked person's client web site. The attacker's intention is to steal user's credentials such as username and password. This type of attack is possible through changing local host files or DNS settings (CISA 2015, pp. 350).

War dialling

In War dialling, the attacker is checking the availability of modems that can be reached through Remote Access Systems (RAS) available via Public Switched Telephone Networks (PSTN), Integrated Switched Digital Networks (ISDN), and through remote access devices such as modems and routers.

War driving

Similar to War dialling, except this type of attack is used for attacking wireless networks by using equipment (laptop, wireless antenna, software) and vehicles to gather information on weak encryption and open wireless access networks by driving around buildings and other physical objects (CISA 2015, pp. 351).

War walking

An identical type of attack as war driving where instead of using a vehicle, the attacker walks around a building with the equipment for identification of vulnerable access points (CISA 2015, pp. 351).

War chalking

War chalking is the process of marking buildings and physical objects to notify of open wireless networks. Purpose of war chalking is to notify other users who wants to use wireless access to the Internet at no cost (CISA 2015, pp. 351). .

Code injection

Code injection relies on program errors which, when they receive data or code from the attacker, change the course of execution. There are different types of code injection techniques, such as SQL injection, HTML script injection, Dynamic evaluation vulnerabilities, Object injection, Remote file injection, Format Specifier Injection, and Shell injection.

Interrupt attacks

These types of attacks are used to insert specific and malicious routines in running operating systems using system calls to interrupt other operating system executions (CISA 2015, pp. 349).

DoS, DDoS, flood attacks

These kinds of attacks have the goal to disrupt or block all communication to and from the attacked network.

Denial-of-service attack (DoS attack) is an active type of cyber-attack with the goal of making the targeted system temporarily unavailable. . A typical approach is to flood the targeted network with large amounts of packets or misuse the TCP/IP stack with syn flood attacks that misuse the vulnerability of the three-way handshake mechanism. Typical attacks include ICMP ping flood, Smurf attack, Syn flood attack, and Teardrop attack.

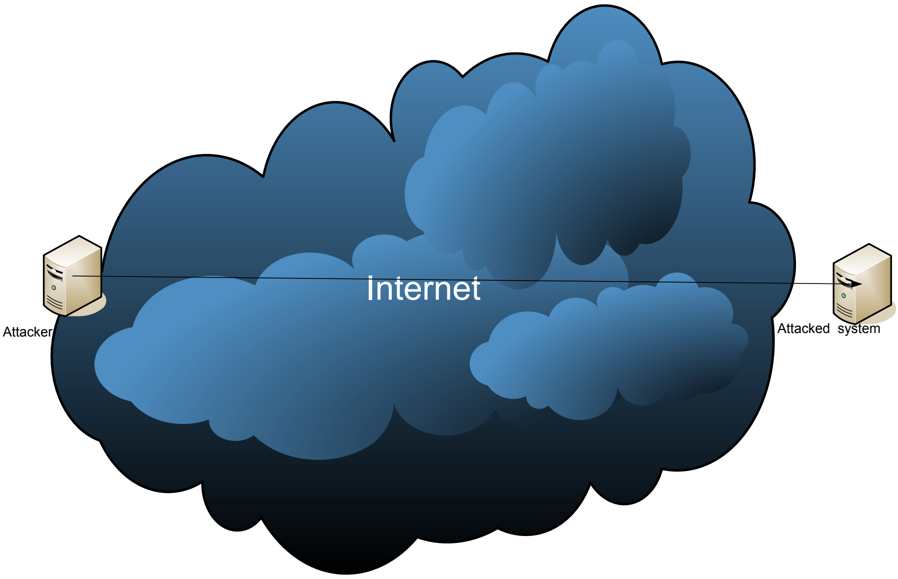


Figure 27. DoS attack

A special type of DoS attack is permanent DoS or PDoS or plashing, with the goal of damaging hardware and in this way prolonging the recovery of the attacked system.

Distributed Denial-of-service attack (DDoS attack) is a special type of DoS attack where many machines on the Internet are used to amplify the strength of the attack. Machines used to amplify the attack are called agents or botnets.

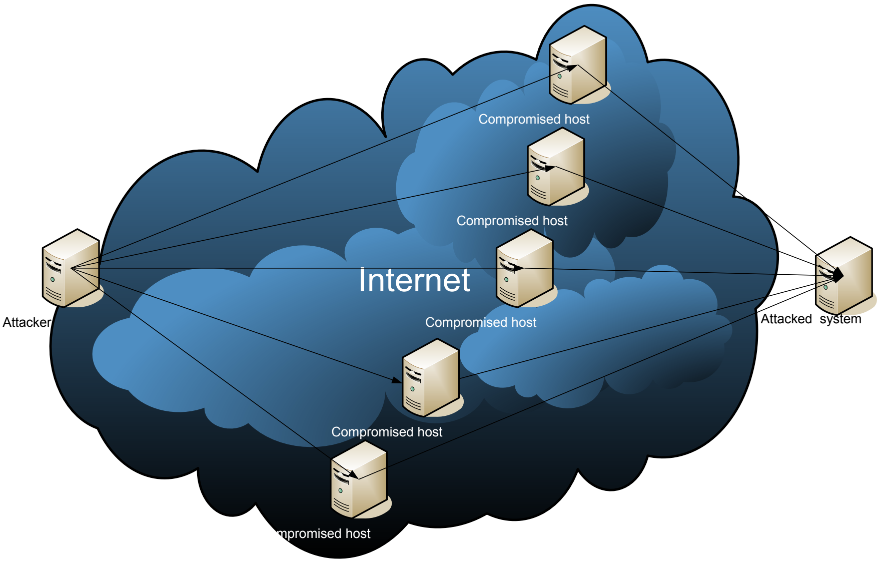


Figure 28. DDoS attack

Flood attacks

Flooding the network with large amounts of traffic disables the communicative channels of the attacked network, and as such, these attacks are DoS or DDoS variants.

Protocol specific attacks

Due to a weak protocol design and implementations during a course of time, different types of attacks were launched.

DNS attacks

Most prominent attacks on DNS services include DNS spoofing or hijacking, DNS rebinding, DNS Denial-of-service attack, and DNS Amplification attacks.

DNS attacks are common ground or starting point for other types of attacks because DNS services provide users with vectors and directions of communication similar to routing protocols. The difference is that DNS is easier to attack because it relies on end-user insecurity such as unpatched operating systems, un-updated antivirus software, weak firewall and/or intrusion detection policies, and/or lack of network segmentation.

ARP attacks

ARP protocol are part of the TCP/IP protocol suite of Ethernet types of network, which is used by network operating systems to determine the MAC address of a device’s IP address so that communication on the LAN segment can be initiated and finished with the communication peer.

When initiating IP communication, the computer needs the MAC address of the device so that the sending and receiving device can communicate using data link layers. Once the initiating computer learns the MAC address of the computer with which communication is needed, as is the case when using DNS service on DNS servers, communication continues using IP protocols.

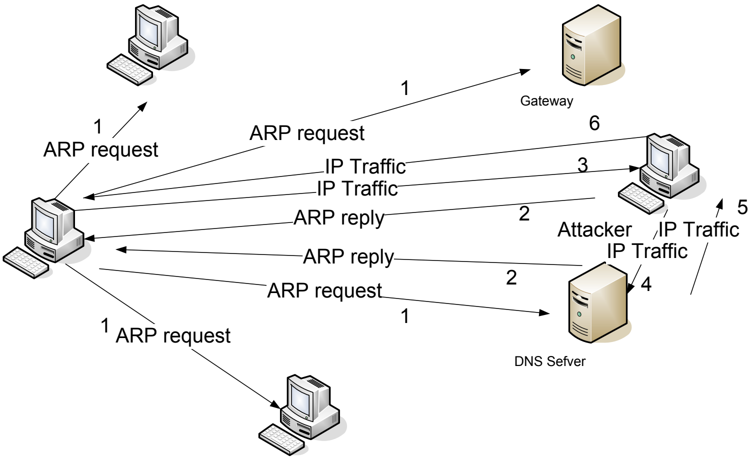


Figure 29. ARP operation and ARP attack

Attackers use techniques called ARP spoofing, ARP poison routing, or ARP cache poisoning, which is a subtype of MITM attacks which are used to send ARP replies to confuse the communication initiator and to “persuade” the communication initiator that traffic should pass via the attacker’s computer. Implementing this scenario, the attacker is able to record traffic and get passwords, credit card numbers, and even change user data in packets.

DHCP attack

As previously explained, the DHCP service provides dynamic IP addresses. Attackers install malicious software on infected computers or use other techniques or even hardware to offer IP addresses to computers that require the IP address. The malicious DHCP service and server where it is installed is called a rogue DHCP server attack. The attacker sends the victim an IP address, subnet address, default gateway address, and IP addresses of DNS and WINS servers, which allows the attacker to hijack all communication initiated from the victim’s computer.

Alteration attacks

This kind of attack is used to modify data or program codes, thus affecting the integrity of data.

Botnets

Botnets are networks of compromised computers running malicious software to amplify attacks such as DDoS, spam, and other massive types of attacks.

Fraud

Fraud is defined by the Oxford dictionary as: “wrongful or criminal deception intended to result in financial or personal gain”

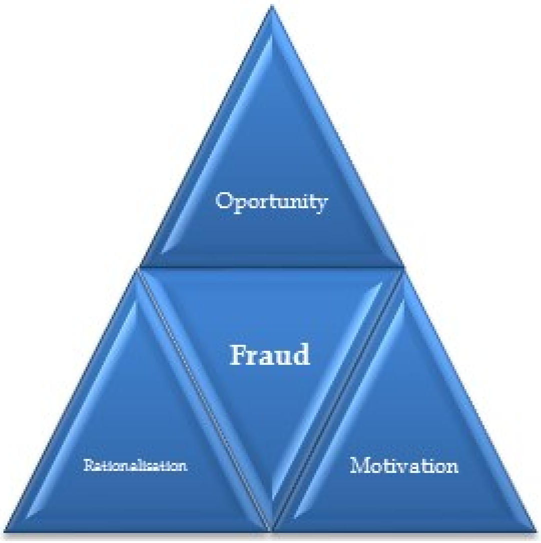


Figure 30. Fraud triangle

Opportunity to commit fraud is created by the following conditions: misuse of privileges and entrance into the system, lack of established monitoring activities, collaboration between co-workers, and established four eyes controls, as well as keeping access rights through changing organisation positions (Sandwith L. 2006).

Rationalisation represents another part of the fraud triangle. It is based on a self-morally defensible justification for fraud which could be in the form of medical or social programs available for all citizens (Sandwith L. 2006).

Motivation or pressure to commit fraud, as the third part of the triangle arises when there is a need for additional income, expensive health interventions, nursing care, and previously un-detected frauds (Sandwith L. 2006).

Salami

This type of a fraud attack uses the technique of taking small amounts of money from accounts and sending it to other accounts which usually belongs to attackers. This type of attack is common in banking institutions (CISA, 2015, pp. 350.).

Phishing

Phishing is cyber fraud whose goal is identity theft. This type of attack is performed when criminals send messages which seem genuine to victims (their bank e-mail address, or other legitimate organisation addresses) persuading them to submit confidential information such as credentials or other information (CISA, 2015, pp.349).

Deep Web, Dark Web

Search engines such as Google, Bing, YouTube, Wikipedia, and other similar services, represent available Internet resources which are used for legitimate purposes. On the other hand, resources available through the Deep and Dark Web (2018) are generally considered illegal, offensive, and in focus and interest of law enforcement agencies for detecting, preventing, and documenting criminal activities.

Deep Web

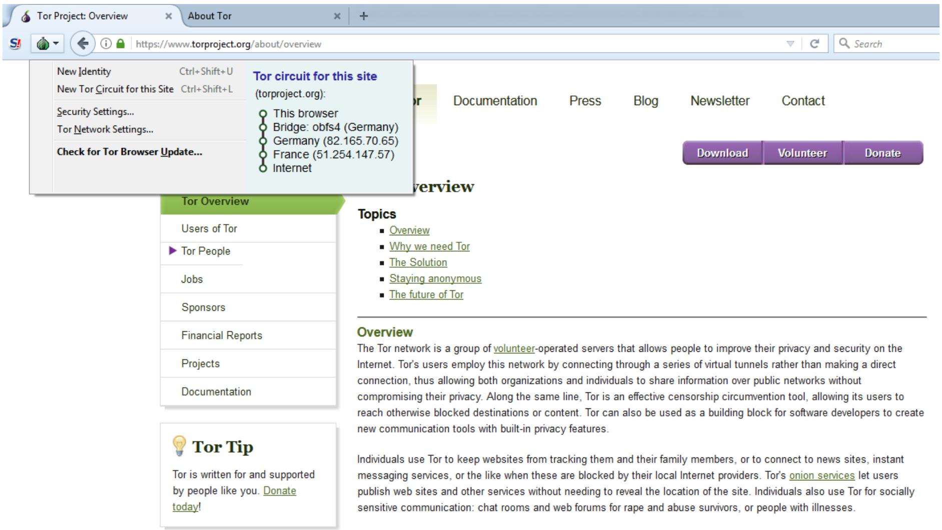
The phenomenon known as Deep Web contains illegal information such as web sites with medical records, published scientific reports, and papers stored and transferred from services which require a special fee for accessing those files.

Dark Web

The Dark Web is a part of the Internet used for drug trafficking, illegal information, political protests, and private communications usually supported with certain types of browsers such as The Onion Router (TOR, 2018) which encrypts traffic.

Dark Net

The Dark web uses Dark Net to transfer data and route traffic over the Internet. This network uses hidden services available only through web browsers such as TOR. As explained on the TOR website, TOR protects its users against "*traffic analysis*."



Tor circuit for this site
(torproject.org):

- This browser
- Bridge: obfs4 (Germany)
- Germany (82.165.70.65)
- France (51.254.147.57)
- Internet

Overview

Topics

- Overview
- Why we need Tor
- The Solution
- Staying anonymous
- The future of Tor

Overview

The Tor network is a group of volunteer-operated servers that allows people to improve their privacy and security on the Internet. Tor's users employ this network by connecting through a series of virtual tunnels rather than making a direct connection, thus allowing both organizations and individuals to share information over public networks without compromising their privacy. Along the same line, Tor is an effective censorship circumvention tool, allowing its users to reach otherwise blocked destinations or content. Tor can also be used as a building block for software developers to create new communication tools with built-in privacy features.

Individuals use Tor to keep websites from tracking them and their family members, or to connect to news sites, instant messaging services, or the like when these are blocked by their local Internet providers. Tor's onion services let users publish web sites and other services without needing to reveal the location of the site. Individuals also use Tor for socially sensitive communication: chat rooms and web forums for rape and abuse survivors, or people with illnesses.

Tor Tip

Tor is written for and supported by people like you. Donate today!

Figure 31. TOR (2018)

Figure 31. shows TOR's automatic configuration for using proxy servers before the web request reaches the Internet.

Many sources claim that TOR was developed by the United States National Security Agency (NSA) (Lee T. B. 2013) to provide covert communication for activists in countries with censored Internet. However, it was used against NSA when WikiLeaks (Lee T. B. 2013) published a great amount of data which were transferred using TOR.

TOR as a technology is used as a service for anonymous communication by many on the Internet.

TOR operation

TOR operates through three steps explained on the TOR support web-site.

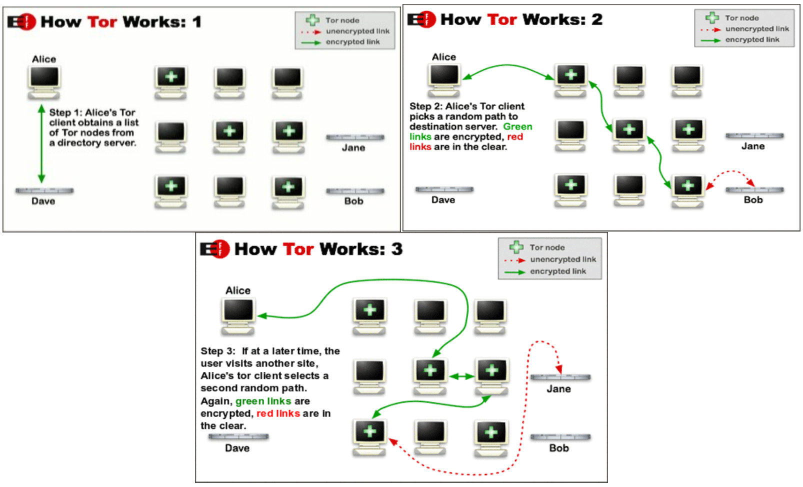

How Tor Works: 1
Tor node
unencrypted link
encrypted link
Alice
Step 1: Alice's Tor client obtains a list of Tor nodes from a directory server.
Jane
Dave
Bob
How Tor Works: 2
Tor node
unencrypted link
encrypted link
Alice
Step 2: Alice's Tor client picks a random path to destination server. Green links are encrypted, red links are in the clear.
Jane
Dave
Bob
How Tor Works: 3
Tor node
unencrypted link
encrypted link
Alice
Step 3: If at a later time, the user visits another site, Alice's tor client selects a second random path. Again, green links are encrypted, red links are in the clear.
Jane
Dave
Bob

Figure 32. TOR modus operandi, TOR (2018)

In the initial phase, the local TOR browser searches for TOR nodes from the directory server. Afterwards, it selects a random path for each request. Communication between TOR nodes is encrypted, while only the final hop (communication the between TOR node and the requested destination) is not encrypted.

This type of operation was used before in P2P communication where resources from other nodes were used by Napster (2018), Gnutela (Mitchell B. 2018), Donkey (2018), and other similar tools.

Penetration testing, ethical hacking, and intrusions

Intrusion attacks on a critical infrastructure are common security problems in the cyber space. Critical infrastructures must be on the Internet to offer services to users. Because of that, it is necessary to test critical infrastructures against potential intrusion attacks as they would be performed in reality. These types of security tests are called penetration testing and ethical hacking, and are performed by ethical hackers.

Ethical hackers, known as white hat hackers, are security professionals who know how to find and exploit vulnerabilities in different systems. They must have same technical knowledge and skills as malicious hackers, better known as black hat hackers.

Ethical hackers use skills in a legitimate and lawful way to try to find vulnerabilities and propose improvements before black hat hackers can get there and try to break in.

Penetration testing and ethical hacking became very important for organisations because they improve security. As such, educational institutions designed courses in an attempt to teach their students ethical hacking skills. One of the best known ethical hacking programs is the Certified Ethical Hacker (CEH, 2018) certification scheme developed by EC-Council, which is an organisation headquartered in Albuquerque, New Mexico available at https://www.eccouncil.org.

Penetration tests follow similar or same steps as real intrusions. There are three major approaches to penetration testing (CEH, 2018) explained below.

White box – in this approach, an ethical hacker has access to a lot of information, such as IP addresses, running services, and operating systems, available applications, etc.

Grey box – some of the information is not given to the ethical hacker, but rather it is left for the test team in order to discover information needed for intrusion.

Black box – no information is given to the ethical hacker, but it is his task to discover information needed for intrusion.

Common intrusion steps, techniques, and tools

Figure 33. shows that in the time scale, there are more points which come before successful intrusion. This knowledge can be used to detect intrusion attempts and stop intrusion. It is very important to know that there were months of cyber-attack preparations in cases explained in previous sections. Preparation points could be detected earlier if proper malware protection, intrusion detection, fraud detection, and event monitoring activities exist.

In order to protect the local system, it is clearly important that early signs of malicious attempts be recognised. Bejtlich (2004) suggests common points in time when cyber-attacks could be recognised.

Reconnaissance is used to gain knowledge of the targeted system state which includes but is not limited to hardware platforms, operating systems, open ports, and running services.

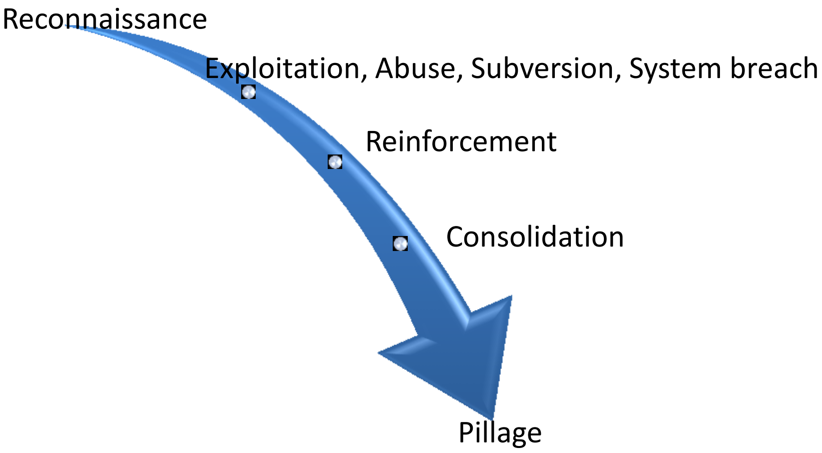


Figure 33. Common steps of intrusion attacks (Bejtlich, 2004)

Performing ethical hacking, penetration testing, or executing a cyber-attack is a similar act to engaging in war. Following this logic, it is crucial to gain knowledge on strengths and weaknesses of the targeted system.

Network port scanning and war driving for wireless networks (a technique known as war dialling in the modem communication era) provide information for attackers or ethical hackers about open and closed ports, versions of operating systems, encryption used for wireless networks, and used certificates.

During the reconnaissance phase, attackers collect valuable information on the security state of any system. This phase in ethical hacking terminology uses methods such as footprinting, port scanning, and enumeration. In this phase, collected data can reveal system vulnerabilities which can be used against the system. The main aim of this is to improve the approach used by the attacker with which system vulnerabilities can be exploited.

Tool	Function
groups.google.com	Search for posting technical or non-technical newsgroups.
Whois (whois.net or arin.net)	Can be used as IP address gathering tool.
SamSpade (http://www.majorgeeks.com)	Application for gathering domain information.
White Pages (www.whitepages.com)	Retrieve phone and address information
OWASP Zed Attack Proxy (ZAP) (https://www.owasp.org/)	Discovers web server information and possible vulnerabilities.

Table 9. Short timeline of major malicious software appearance Reconnaissance and foot printing tools

In the reconnaissance phase, the attacker or the ethical hacker uses non-intrusive and intrusive methods to gather information of physical and logical location of the targeted system.

Furthermore, the tester or attacker gains knowledge on open ports, operating systems, and available resources, such as shares on the network, user names, groups assigned on the network, and the last time the user logged on.

Sometime, an organisation's (which is object of recognisance and footprinting) web-site can reveal phone numbers, responsible persons, employees' biographies, as well as the e-mail address format which can be used to guess e-mail addresses of other employees.

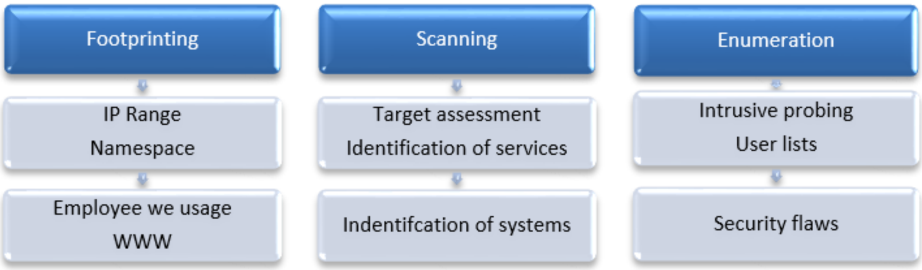
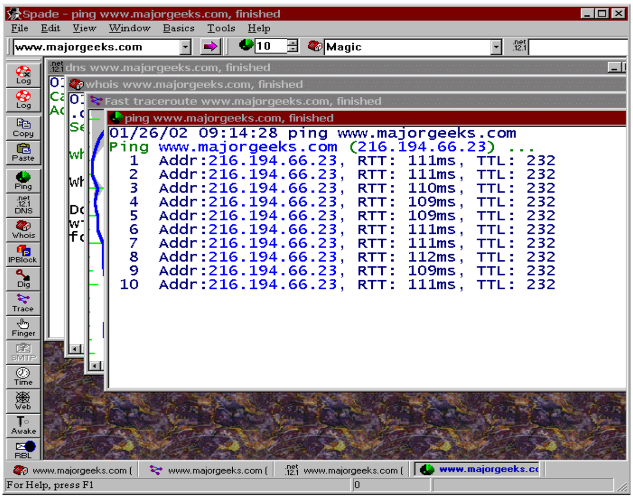


Figure 34. Reconnaissance phases (CEH, 2018)

The SampSpade (2018) tool can be used to investigate Zone Transfer, SMTP Relay Check, Scan Addresses, Crawl website, Browse web, Fast and Slow Traceroute, S-Lang command, Decode URL, and Parse e-mail headers. It can give an attacker information about users and a system or particular host which is object of the attack, or it can be used to examine a server or web site security on the Internet.

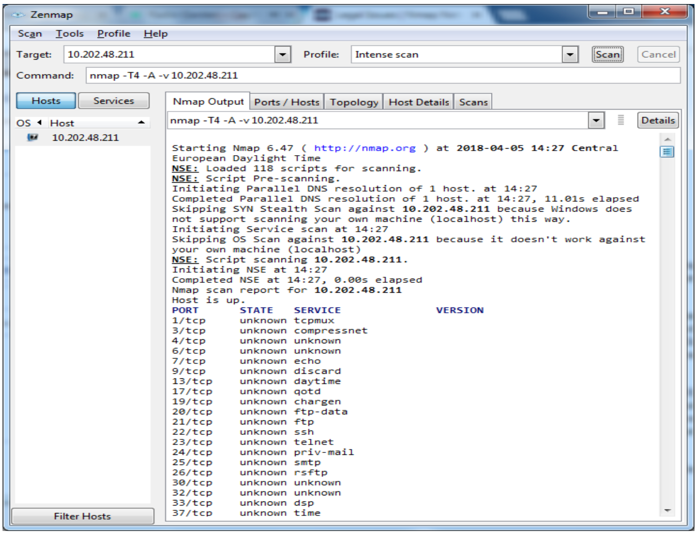


```
01/26/02 09:14:28 ping www.majorgeeks.com
Ping www.majorgeeks.com (216.194.66.23) ...
  1   Addr:216.194.66.23, RTT: 111ms, TTL: 232
  2   Addr:216.194.66.23, RTT: 111ms, TTL: 232
  3   Addr:216.194.66.23, RTT: 110ms, TTL: 232
  4   Addr:216.194.66.23, RTT: 109ms, TTL: 232
  5   Addr:216.194.66.23, RTT: 109ms, TTL: 232
  6   Addr:216.194.66.23, RTT: 111ms, TTL: 232
  7   Addr:216.194.66.23, RTT: 111ms, TTL: 232
  8   Addr:216.194.66.23, RTT: 112ms, TTL: 232
  9   Addr:216.194.66.23, RTT: 109ms, TTL: 232
 10   Addr:216.194.66.23, RTT: 111ms, TTL: 232
```

Spade - ping www.majorgeeks.com, finished
File Edit View Window Basics Tools Help
www.majorgeeks.com
10
Magic
dns www.majorgeeks.com, finished
whois www.majorgeeks.com, finished
Fast traceroute www.majorgeeks.com, finished
ping www.majorgeeks.com, finished
Log
Log
Copy
Paste
Ping
DNS
Whois
IPBlock
Dig
Trace
Finger
SMTP
Time
Web
Awake
RBL
For Help, press F1

Figure 35. SamSpade (2018)

Another tool used for reconnaissance purposes is Nmap/Zenmap (2018), available for Linux and Windows systems.



Target: 10.202.48.211
Profile: Intense scan
Command: nmap -T4 -A -v 10.202.48.211

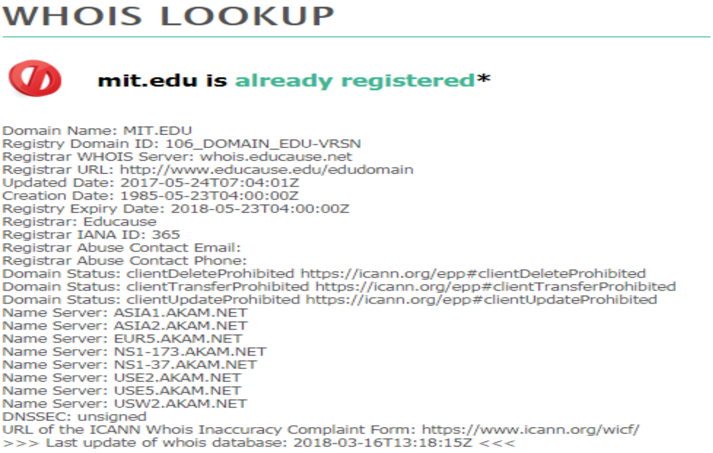
```
nmap -T4 -A -v 10.202.48.211

Starting Nmap 6.47 ( http://nmap.org ) at 2018-04-05 14:27 Central
European Daylight Time
NSE: Loaded 118 scripts for scanning.
NSE: Script Pre-scanning.
Initiating Parallel DNS resolution of 1 host. at 14:27
Completed Parallel DNS resolution of 1 host. at 14:27, 11.01s elapsed
Skipping SYN Stealth Scan against 10.202.48.211 because Windows does
not support scanning your own machine (localhost) this way.
Initiating Service scan at 14:27
Skipping OS Scan against 10.202.48.211 because it doesn't work against
your own machine (localhost)
NSE: Script scanning 10.202.48.211.
Initiating NSE at 14:27
Completed NSE at 14:27, 0.00s elapsed
Nmap scan report for 10.202.48.211
Host is up.
PORT      STATE   SERVICE             VERSION
1/tcp     unknown tcpmux
3/tcp     unknown compressnet
4/tcp     unknown unknown
6/tcp     unknown unknown
7/tcp     unknown echo
9/tcp     unknown discard
13/tcp    unknown daytime
17/tcp    unknown qotd
19/tcp    unknown chargen
20/tcp    unknown ftp-data
21/tcp    unknown ftp
22/tcp    unknown ssh
23/tcp    unknown telnet
24/tcp    unknown priv-mail
25/tcp    unknown smtp
26/tcp    unknown rsftp
30/tcp    unknown unknown
32/tcp    unknown unknown
33/tcp    unknown dsp
37/tcp    unknown time
```

Figure 36. Nmap / Zenmap (2018)

Google site groups.google.com can be used as a tool to find corporate employees' information.

Whois is a commonly used tool for gathering IP addresses and domain information that attackers can use.



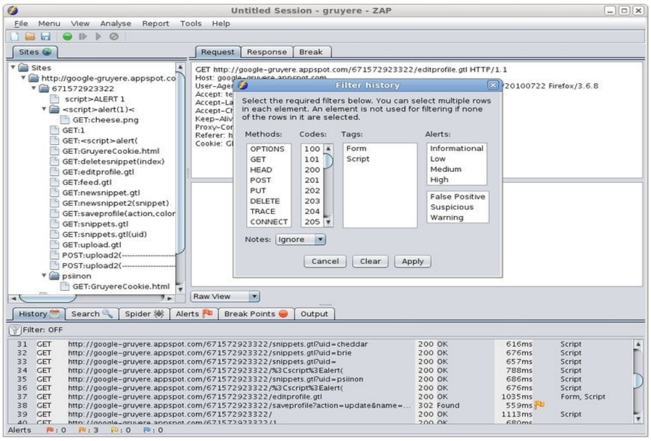
WHOIS LOOKUP

mit.edu is already registered*

```
Domain Name: MIT.EDU
Registry Domain ID: 106_DOMAIN_EDU-VRSN
Registrar WHOIS Server: whois.educause.net
Registrar URL: http://www.educause.edu/edudomain
Updated Date: 2017-05-24T07:04:01Z
Creation Date: 1985-05-23T04:00:00Z
Registry Expiry Date: 2018-05-23T04:00:00Z
Registrar: Educause
Registrar IANA ID: 365
Registrar Abuse Contact Email:
Registrar Abuse Contact Phone:
Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited
Name Server: ASIA1.AKAM.NET
Name Server: ASIA2.AKAM.NET
Name Server: EUR5.AKAM.NET
Name Server: NS1-173.AKAM.NET
Name Server: NS1-37.AKAM.NET
Name Server: USE2.AKAM.NET
Name Server: USE5.AKAM.NET
Name Server: USW2.AKAM.NET
DNSSEC: unsigned
URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
>>> Last update of whois database: 2018-03-16T13:18:15Z <<<
```

Figure 37. Whois output for www.mit.edu

ZAP (2018) can be used to discovered web server information and find possible vulnerabilities and weaknesses.



```
GET http://google-gruyere.appspot.com/671572923322/editprofile.gtl HTTP/1.1
Host: google-gruyere.appspot.com
User-Agen                                  20100722 Firefox/3.6.8
Accept: te
Accept-La
Accept-Ch
Keep-Aliv
Proxy-Co
Referer: h
Cookie: G
```

Filter history

Select the required filters below. You can select multiple rows in each element. An element is not used for filtering if none of the rows in it are selected.

Methods:	Codes:	Tags:	Alerts:
OPTIONS	100	Form	Informational
GET	101	Script	Low
HEAD	200		Medium
POST	201		High
PUT	202		False Positive
DELETE	203		Suspicious
TRACE	204		Warning
CONNECT	205		

Notes: Ignore

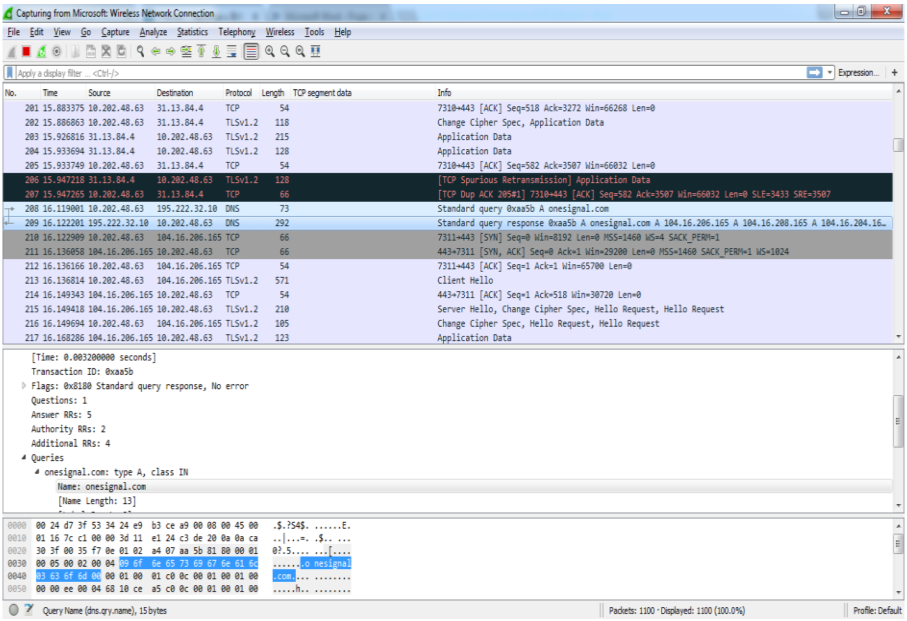
Cancel Clear Apply

Filter: OFF

```
31  GET  http://google-gruyere.appspot.com/671572923322/snippets.gtl?uid=cheddar       200 OK      616ms   Script
32  GET  http://google-gruyere.appspot.com/671572923322/snippets.gtl?uid=brie          200 OK      676ms   Script
33  GET  http://google-gruyere.appspot.com/671572923322/snippets.gtl?uid=              200 OK      657ms   Script
34  GET  http://google-gruyere.appspot.com/671572923322/%3Cscript%3Ealert(             200 OK      788ms   Script
35  GET  http://google-gruyere.appspot.com/671572923322/snippets.gtl?uid=psiinon       200 OK      686ms   Script
36  GET  http://google-gruyere.appspot.com/671572923322/%3Cscript%3Ealert(             200 OK      676ms   Script
37  GET  http://google-gruyere.appspot.com/671572923322/editprofile.gtl                200 OK     1035ms   Form, Script
38  GET  http://google-gruyere.appspot.com/671572923322/saveprofile?action=update&name=...  302 Found   559ms
39  GET  http://google-gruyere.appspot.com/671572923322/                               200 OK     1113ms   Script
40  GET  http://google-gruyere.appspot.com/671572923322/1                              200 OK      680ms
Alerts  : 0  : 3  : 0  : 0
```

Figure 38. ZAP (2018)

All gathered information can be used for social engineering purposes or the technical exploitation phase for the next phase of the attacks.


Capturing from Microsoft: Wireless Network Connection
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...
+

```
No.   Time      Source          Destination     Protocol Length TCP segment data  Info
  201 15.883375 10.202.48.63    31.13.84.4      TCP        54                     7310→443 [ACK] Seq=518 Ack=3272 Win=66268 Len=0
  202 15.886863 10.202.48.63    31.13.84.4      TLSv1.2   118                     Change Cipher Spec, Application Data
  203 15.926816 31.13.84.4      10.202.48.63    TLSv1.2   215                     Application Data
  204 15.933694 31.13.84.4      10.202.48.63    TLSv1.2   128                     Application Data
  205 15.933749 10.202.48.63    31.13.84.4      TCP        54                     7310→443 [ACK] Seq=582 Ack=3507 Win=66032 Len=0
  206 15.947218 31.13.84.4      10.202.48.63    TLSv1.2   128                     [TCP Spurious Retransmission] Application Data
  207 15.947265 10.202.48.63    31.13.84.4      TCP        66                     [TCP Dup ACK 205#1] 7310→443 [ACK] Seq=582 Ack=3507 Win=66032 Len=0 SLE=3433 SRE=3507
  208 16.119001 10.202.48.63    195.222.32.10   DNS        73                     Standard query 0xaa5b A onesignal.com
  209 16.122201 195.222.32.10   10.202.48.63    DNS       292                     Standard query response 0xaa5b A onesignal.com A 104.16.206.165 A 104.16.208.165 A 104.16.204.16…
  210 16.122909 10.202.48.63    104.16.206.165  TCP        66                     7311→443 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
  211 16.136058 104.16.206.165  10.202.48.63    TCP        66                     443→7311 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM=1 WS=1024
  212 16.136166 10.202.48.63    104.16.206.165  TCP        54                     7311→443 [ACK] Seq=1 Ack=1 Win=65700 Len=0
  213 16.136814 10.202.48.63    104.16.206.165  TLSv1.2   571                     Client Hello
  214 16.149343 104.16.206.165  10.202.48.63    TCP        54                     443→7311 [ACK] Seq=1 Ack=518 Win=30720 Len=0
  215 16.149418 104.16.206.165  10.202.48.63    TLSv1.2   210                     Server Hello, Change Cipher Spec, Hello Request, Hello Request
  216 16.149694 10.202.48.63    104.16.206.165  TLSv1.2   105                     Change Cipher Spec, Hello Request, Hello Request
  217 16.168286 104.16.206.165  10.202.48.63    TLSv1.2   123                     Application Data
```

```
    [Time: 0.003200000 seconds]
    Transaction ID: 0xaa5b
  ▷ Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 5
    Authority RRs: 2
    Additional RRs: 4
  ◢ Queries
    ◢ onesignal.com: type A, class IN
        Name: onesignal.com
        [Name Length: 13]
```

```
0000  00 24 d7 3f 53 34 24 e9  b3 ce a9 00 08 00 45 00   .$.?S4$. ......E.
0010  01 16 7c c1 00 00 3d 11  e1 24 c3 de 20 0a 0a ca   ..|...=. .$.. ...
0020  30 3f 00 35 f7 0e 01 02  a4 07 aa 5b 81 80 00 01   0?.5.... ...[....
0030  00 05 00 02 00 04 09 6f  6e 65 73 69 67 6e 61 6c   .......o nesignal
0040  03 63 6f 6d 00 00 01 00  01 c0 0c 00 01 00 01 00   .com.... ........
0050  00 00 ee 00 04 68 10 ce  a5 c0 0c 00 01 00 01 00   .....h.. ........
```

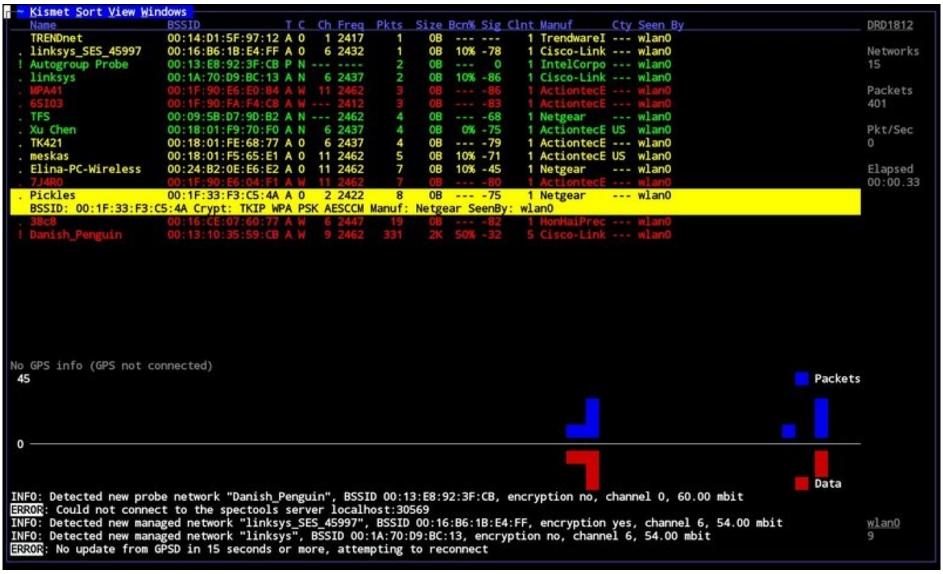
Query Name (dns.qry.name), 15 bytes
Packets: 1100 · Displayed: 1100 (100.0%)
Profile: Default

Figure 39. Wireshark window with captured traffic

Tools such as **Wireshark** (2018) can be used to sniff network traffic from wired network segments closed using Tap devices or Switches and SPAN ports.

Wireless networks, compared to wired networks, make surveying network traffic easier. This is because there is no possibility to physically protect the network flow, and the only protection is the encryption mechanism. Based on the historical overview, weak implementations of encryption mechanisms lead to vulnerabilities exploited by attackers.

Software such as Kismet (2018) in combination with Wireshark (2018) can be used to analyse captured wireless traffic.



```
  Name                  BSSID              T C  Ch Freq  Pkts  Size Bcn% Sig Clnt Manuf       Cty Seen By
  TRENDnet              00:14:D1:5F:97:12 A 0   1 2417     1    0B  --- ---    1 TrendwareI --- wlan0
. linksys_SES_45997     00:16:B6:1B:E4:FF A 0   6 2432     1    0B  10% -78    1 Cisco-Link --- wlan0
! Autogroup Probe       00:13:E8:92:3F:CB P N --- ----     2    0B  ---   0    1 IntelCorpo --- wlan0
. linksys               00:1A:70:D9:BC:13 A N   6 2437     2    0B  10% -86    1 Cisco-Link --- wlan0
. MPA41                 00:1F:90:E6:E0:B4 A W  11 2462     3    0B  --- -86    1 ActiontecE --- wlan0
. 6SI03                 00:1F:90:FA:F4:C8 A W --- 2412     3    0B  --- -83    1 ActiontecE --- wlan0
. TFS                   00:09:5B:D7:9D:B2 A N --- 2462     4    0B  --- -68    1 Netgear    --- wlan0
. Xu Chen               00:18:01:F9:70:F0 A N   6 2437     4    0B   0% -75    1 ActiontecE US  wlan0
. TK421                 00:18:01:FE:68:77 A 0   6 2437     4    0B  --- -79    1 ActiontecE --- wlan0
. meskas                00:18:01:F5:65:E1 A 0  11 2462     5    0B  10% -71    1 ActiontecE US  wlan0
. Elina-PC-Wireless     00:24:B2:0E:E6:E2 A 0  11 2462     7    0B  10% -45    1 Netgear    --- wlan0
. 7J4R0                 00:1F:90:E6:04:F1 A W  11 2462     7    0B  --- -80    1 ActiontecE --- wlan0
. Pickles               00:1F:33:F3:C5:4A A 0   2 2422     8    0B  --- -75    1 Netgear    --- wlan0
  BSSID: 00:1F:33:F3:C5:4A Crypt: TKIP WPA PSK AESCCM Manuf: Netgear SeenBy: wlan0
. 38c8                  00:16:CE:07:60:77 A W   6 2447    19    0B  --- -82    1 HonHaiPrec --- wlan0
! Danish_Penguin        00:13:10:35:59:CB A W   9 2462   331    2K  50% -32    5 Cisco-Link --- wlan0

No GPS info (GPS not connected)

INFO: Detected new probe network "Danish_Penguin", BSSID 00:13:E8:92:3F:CB, encryption no, channel 0, 60.00 mbit
ERROR: Could not connect to the spectools server localhost:30569
INFO: Detected new managed network "linksys_SES_45997", BSSID 00:16:B6:1B:E4:FF, encryption yes, channel 6, 54.00 mbit
INFO: Detected new managed network "linksys", BSSID 00:1A:70:D9:BC:13, encryption no, channel 6, 54.00 mbit
ERROR: No update from GPSD in 15 seconds or more, attempting to reconnect
```

Figure 40. Kismet (2018)

System hacking or exploitation phase include abuse, subversion, or system breach which comes after the reconnaissance stage (foot printing, port scanning, and enumeration) because reconnaissance phase has to provide enough information for **abuse**.

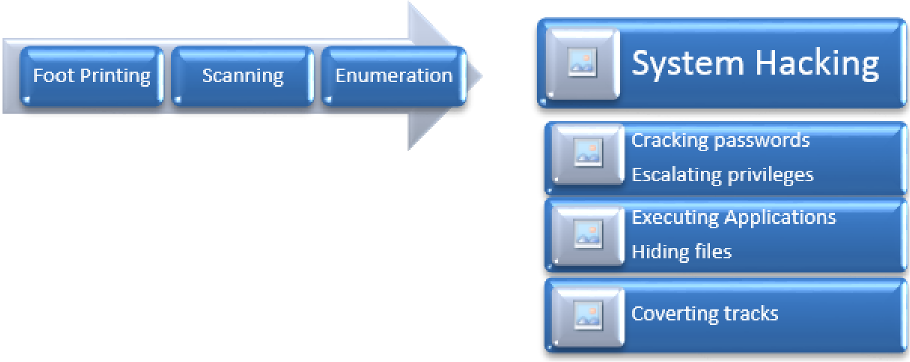
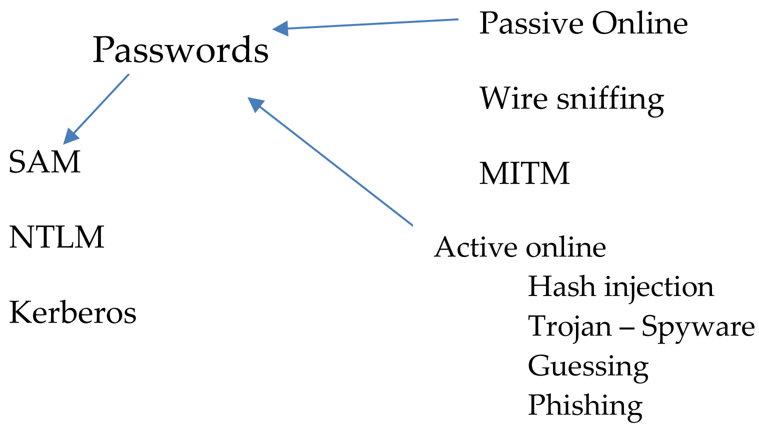


Figure 41. System hacking steps (CEH, 2018)

In the abuse stage, an attacker is able to log on to legitimate services by utilizing previously used techniques such as brute force or password cracking. Password cracking is one of the earliest hacking techniques for accessing privileges.



Passwords

Passive Online

Wire sniffing

MITM

SAM

NTLM

Kerberos

Active online

Hash injection

Trojan – Spyware

Guessing

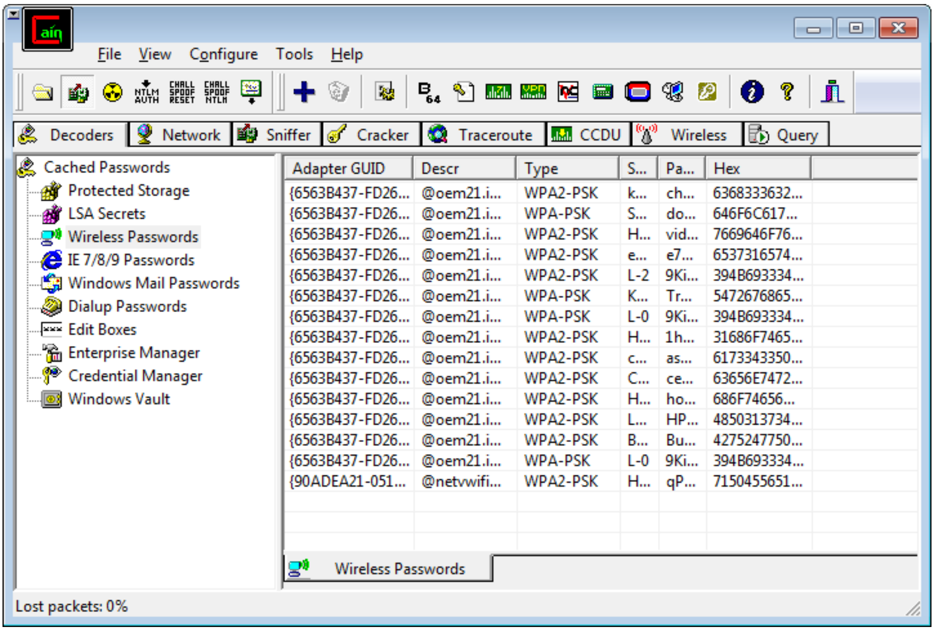
Phishing

Figure 42. Password cracking techniques (CEH, 2018)

Passwords have to be stored somewhere in order to authenticate users. They are encrypted for security reasons. One approach towards identifying one's password represents stealing the password or entire password files for decryption. This process is known as password cracking.

Password cracking can be used as a password strength checking tool in ethical hacking, technical testing, or for audit purposes.

Common tool used in this approach are John the Ripper (2018), Cain & Abel (2018), and other similar tools.



Adapter GUID	Descr	Type	S...	Pa...	Hex
{6563B437-FD26...	@oem21.i...	WPA2-PSK	k...	ch...	6368333632...
{6563B437-FD26...	@oem21.i...	WPA-PSK	S...	do...	646F6C617...
{6563B437-FD26...	@oem21.i...	WPA2-PSK	H...	vid...	7669646F76...
{6563B437-FD26...	@oem21.i...	WPA2-PSK	e...	e7...	6537316574...
{6563B437-FD26...	@oem21.i...	WPA2-PSK	L-2	9Ki...	394B693334...
{6563B437-FD26...	@oem21.i...	WPA-PSK	K...	Tr...	5472676865...
{6563B437-FD26...	@oem21.i...	WPA-PSK	L-0	9Ki...	394B693334...
{6563B437-FD26...	@oem21.i...	WPA2-PSK	H...	1h...	31686F7465...
{6563B437-FD26...	@oem21.i...	WPA2-PSK	c...	as...	6173343350...
{6563B437-FD26...	@oem21.i...	WPA2-PSK	C...	ce...	63656E7472...
{6563B437-FD26...	@oem21.i...	WPA2-PSK	H...	ho...	686F74656...
{6563B437-FD26...	@oem21.i...	WPA2-PSK	L...	HP...	4850313734...
{6563B437-FD26...	@oem21.i...	WPA2-PSK	B...	Bu...	4275247750...
{6563B437-FD26...	@oem21.i...	WPA-PSK	L-0	9Ki...	394B693334...
{90ADEA21-051...	@netvwifi...	WPA2-PSK	H...	qP...	7150455651...

Figure 43. Cain & Abel (2018) captured traffic

Subverting phase of system mechanisms has the goal to perform actions needed for escalating privileges which go into the **reinforcement stage**.

In the **reinforcement** stage, an attacker is able to use additional privileges by installing Trojans and opening backdoors for easier access, which is then used in the **consolidation** phase that leads to **pillage**, where attackers steal sensitive data and misuse other system privileges, hiding files, and covering tracks.

Summary

The cyber and information security landscape is changing constantly, and old threats become more sophisticated, while criminal motivations remain the same. The aforementioned passive and active attacks are realised through specially crafted intrusion attacks, code injection, DoS and DDoS, man in the middle attacks, malicious software, hacking tools, fraud, and phishing. Efforts in securing the infrastructure can be invested through testing security via performing common intrusion steps as part of penetration testing, and ethical hacking techniques explained in this chapter.

Knowledge acquired

In this chapter, it is possible to learn about ethical hacking steps and tools, cyber security threats and different attacks on application and communication protocols, and malware threats and the history of malware.

Review questions

1. Explain common steps of intrusion attacks.
2. What is ethical hacking?
3. What is TOR?
4. Explain what is the Deep and Dark Web.
5. Explain the elements of the fraud triangle.
6. Explain ARP, DHCP, DNS attacks.
7. Explain the difference between DoS and DDoS attacks.
8. Explain the difference between Virus and Trojan.
9. What is system hacking?
10. What tools can be used for traffic sniffing on wireless and wired networks?
11. What are password cracking techniques?
12. Name and explain three approaches for penetration testing.

13. What is fraud?

14. Explain common cyber threats.

15. What is spoofing?

Further readings

- Cyber Attacks – What are the Financial Impacts? https://www.countercept.com/our-thinking/how-much-should-you-care-about-cybersecurity/
- Six Cyber Threats to Really Worry About in 2018 https://www.technologyreview.com/s/609641/six-cyber-threats-to-really-worry-about-in-2018/
- A Brief History of Malware — Its Evolution and Impact https://www.lastline.com/blog/history-of-malware-its-evolution-and-impact/
- The Difference Between Passive & Active Attacks on a Computer https://www.techwalla.com/articles/the-difference-between-passive-active-attacks-on-a-computer
- Distributed Denial of Service Attacks – The Internet Protocol Journal; Volume 7, Number 4 https://www.cisco.com/c/en/us/about/press/internet-protocol-journal/back-issues/table-contents-30/dos-attacks.html
- What is the difference between the dark web and the deep web? https://www.quora.com/What-is-the-difference-between-the-dark-web-and-the-deep-web
- Ethical Hacking Academy https://academy.ehacking.net/

- Hacker Tools Top Ten Our Recommended Pentesting Tools and Hacking Software for 2018 https://www.concise-courses.com/hacking-tools/top-ten/

4. Cyber security incident cases

Chapter abstract

Chapter goals: To present cyber incident cases and discuss presented incidents in appropriate timelines to show that proactive detection and prevention of incidents would have been possible if standards and controls had been implemented.

Learning outcomes: Knowledge of cyber incidents and important breaking points in time when incidents could be proactively resolved.

Chapter security incidents

Only cyber incidents with a great loss are reported in media. Almost every year, we face multiple cyber incidents which marked the cyber security arena. Graphics in this section show only a few causes of failures, and explain when it would be possible to spot attacks on time by using Minard's idea (Mason B., 2017) of graphical documentation of unfortunate events.

Central bank of Bangladesh

According to Reuters (2016), and (Krishna N. Das, and Jonathan Spicer, 2016), hackers tried to steal $951 million through multiple bank account orders using primarily the SWIFT messaging system in the first two weeks of February 2016. The attack was well prepared via installed malware on the inside network of the Central Bangladesh Bank, and sent via e-mail to one of the employees with access to the SWIFT system. In media reports, it has been revealed that cheap communication switches were used to connect different network parts. The attack began in late Thursday afternoon on February 4th, when attackers started transferring the $951 million Reuters (2016) and (Krishna N. Das, and Jonathan Spicer, 2016). The attackers accessed almost 1 billion dollars in the account of Central Bangladesh Bank located in New York. Federal Employees stopped the transfer of $850 million by asking the Central Bangladesh Bank for more information about the transaction. However, SWIFT messages never reached the recipient because attackers diverted all messages from New York Fed to the Central Bangladesh Bank, which was not aware of the attack. The rest of the money ($101 million) was not stopped, so it was transferred via Rizal Commercial Banking Corporation (RCBC) in Sri Lanka. However, $20 million which was supposed to go to the bank account in the Philippines was stopped by the Deutsche Bank because they noticed a spelling mistake.

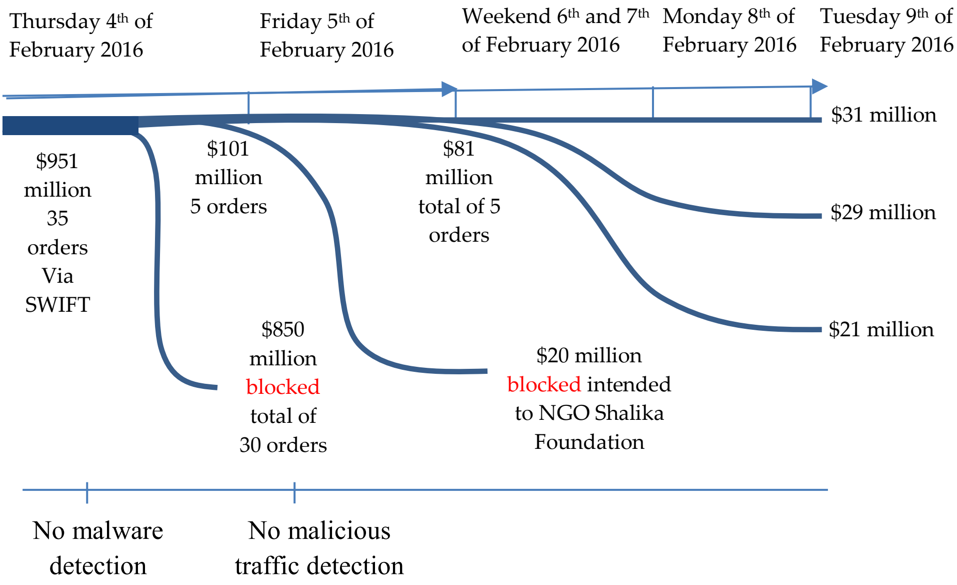

Thursday 4th of February 2016
Friday 5th of February 2016
Weekend 6th and 7th of February 2016
Monday 8th of February 2016
Tuesday 9th of February 2016
$31 million
$951 million 35 orders Via SWIFT
$101 million 5 orders
$81 million total of 5 orders
$29 million
$21 million
$850 million blocked total of 30 orders
$20 million blocked intended to NGO Shalika Foundation
No malware detection
No malicious traffic detection

Figure 44. Time Scale of Central Bangladesh Bank Heist 2016 (Reuters, 2016) and (Krishna N. Das, and Jonathan Spicer, 2016)

Attackers misspelled the name of the recipient of the NGO called "Shalika Foundation," and wrote "*Fundatioin*" instead of "*Foundation*."

The rest of the money ($81 million) was sent to bank accounts in Sri Lanka. On Friday morning of February 5, Central Bangladesh Bank noticed a problem with the SWIFT system, because it was not possible to send or receive messages via the SWIFT system. In addition to that, printing any kind of payment orders was not possible. However, personnel did not pay much attention to that because in the Central Bangladesh Bank it is a custom that after Friday midday, employees who pray do not have to come back to work after prayer.

On Saturday morning of February 6th, it was clear for the Central Bangladesh Bank SWIFT operation personnel that something was wrong, thus, they tried to contact New York Fed. However, it was not possible to reach it because it was a non-working day for New York Fed personnel.

On Monday of February 8th, the Central Bangladesh Bank realized that money was transferred to the Philippines, but it was not possible to contact the bank personnel there. The reason is because in Philippines, February 8th is a holiday and a non-working day. The stolen money was transferred to RCBC bank account and further sent mostly to casinos in Philippines (Krishna N. Das, and Jonathan Spicer, 2016).

No one was arrested or charged for this theft.

The Bangladesh police partially blamed SWIFT because there was no written document which explains what should be done to safeguard the local SWIFT infrastructure. The Bangladesh police admitted that information technology equipment of the Central Bank of Bangladesh was outdated. After the attack, SWIFT visited the Central Bank of Bangladesh and refused to take any responsibility for the incident, stating that the Central Bank of Bangladesh had to resolve recognised technical and organisational security issues on its own.

As a result of this incident, Bangladesh's central bank governor, Atiur Rahman, resigned (Reuters, 2016). in one of the largest cyber-heists in history and Bangladesh's Prime Minister, Sheikh Hasina, accepted his resignation one month after the incident on March 15, 2016.

Retail chain Target

As reported in the media (Vijayan, 2014), in the beginning of 2014, a large retail chain – Target was the victim of a large scale cyber breach, when data from up to 40 million credit and debit cards of Target's shoppers was stolen. In the cyber-attack analysis reports, it was revealed that the Target retailer failed to properly segregate systems which handled sensitive payment card data from the rest of the internal network.

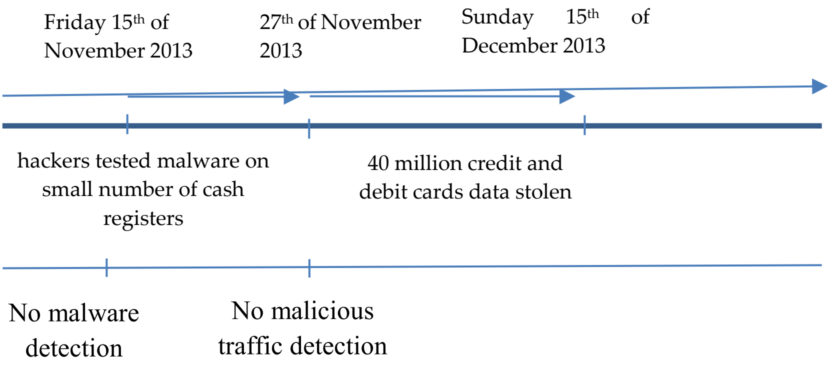

Friday 15th of November 2013
27th of November 2013
Sunday 15th of December 2013
hackers tested malware on small number of cash registers
40 million credit and debit cards data stolen
No malware detection
No malicious traffic detection

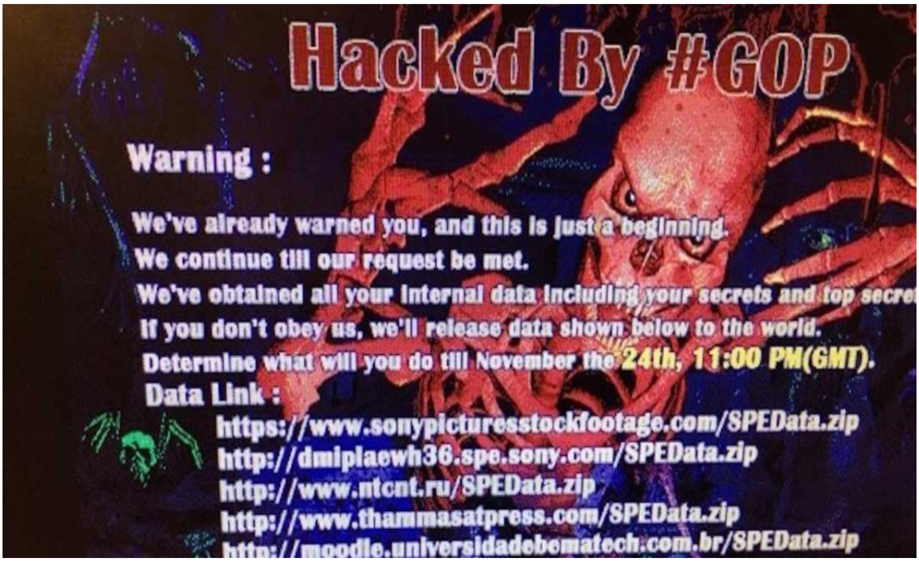
Figure 45. Time Scale of Target retail chain Cyber Attack, 2013

It was reported (Vijayan, 2014), that hackers made an intrusion through the supplier's network, and that of the air conditioning systems maintenance company. This company had access to Target's network with the goal of maintaining equipment and remotely monitoring energy consumption and temperature in Target's stores. Attackers gained access to Target's network on November 15, 2013, and began collecting data and uploading and installing malware on Target's network, or more specifically on the company's Point of Sale (POS) systems. Before the execution of this large-scale attack, which happened between November 27 and December 15, 2013, hackers tested the malware on a small number of cash registers. When they were certain that they will be able to steal a large amount of data, they carried out the attack on about 40 million debit and credit cards of Target's customers from the U.S., Brazil, and Russia.

Sony Entertainment Company

On November 24, 2014, a group of hackers called "Guardians of Peace" (GOP) (GOP, Paul 2014) released 100 TB of confidential information from the Sony Entertainment Company. A member of GOP claimed that they had the access a year before they released data. The Sony Entertainment Company received warnings from hackers on November 21st, demanding "monetary compensation." However, this e-mail was ignored and treated as spam.

Attackers were never brought to justice and early investigations suggested that hackers from North Korea were to blame because Sony was about to release the comedy film "The Interview," about an assassination attempt against Kim Jong-un. Later analysis suggested some other sources of attacks. Figure below shows that users of Sony Entertainment Company were informed about the attack on November 24, 2014. They could have seen a warning message on their screens or web-sites of the services which they used. The confidential information contained personal information of employees, social security numbers, personnel family information, passwords of Hollywood stars, employees' medical confidential reports, confidential information about new movies and music projects, released movies that were still not published, contracts already signed and contracts that were prepared.



Hacked By #GOP

Warning :

We've already warned you, and this is just a beginning.
We continue till our request be met.
We've obtained all your internal data including your secrets and top secre
If you don't obey us, we'll release data shown below to the world.
Determine what will you do till November the 24th, 11:00 PM(GMT).
Data Link :
https://www.sonypicturesstockfootage.com/SPEData.zip
http://dmiplaewh36.spe.sony.com/SPEData.zip
http://www.ntcnt.ru/SPEData.zip
http://www.thammasatpress.com/SPEData.zip
http://moodle.universidadebematech.com.br/SPEData.zip

Figure 46. "Guardians of Peace" (GOP), Paul 2014

Sony reported that direct financial loss was $15 million. That money was spent only for the analysis and collection of information on losses.

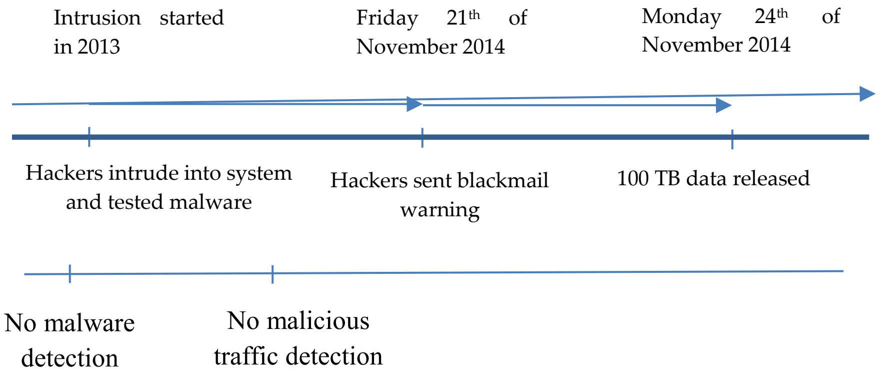

Intrusion started in 2013
Friday 21th of November 2014
Monday 24th of November 2014
Hackers intrude into system and tested malware
Hackers sent blackmail warning
100 TB data released
No malware detection
No malicious traffic detection

Figure 47. Time Scale of Sony Entertainment Company Cyber Attack, 2014

Reputation risk that includes data loss of partners, users, relationships, and other indirect losses, was immeasurable.

Hillary Clinton's presidential campaign

The US presidential campaign from 2016 still causes tremors in internal and external politics. One of the major topics was Senator Clinton's leaked e-mails. Senator Hilary Clinton ordered her engineers to set up an e-mail server at her home in New York, while she was the U.S. Secretary of State.

Clinton's private e-mail system development began in June 2008, when an Apple technician installed and configured an e-mail server in Clintons' New York Chappaqua home (FOX NEWS, 2016).

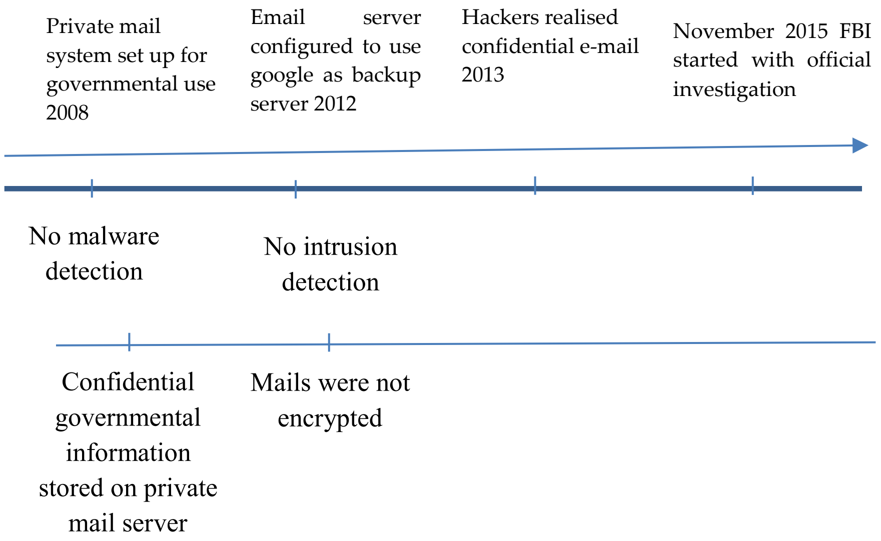

Private mail system set up for governmental use 2008
Email server configured to use google as backup server 2012
Hackers realised confidential e-mail 2013
November 2015 FBI started with official investigation
No malware detection
No intrusion detection
Confidential governmental information stored on private mail server
Mails were not encrypted

Figure 48. Time Scale of Private mail server usage for exchange of confidential governmental information

Two domains were created with a unique DNS names, namely *presidentclinton.com* & *wjcoffice.com*. Later that same year, Bryan

Pagliano, an IT specialist, was hired to set up an additional e-mail server. In 2009, Hilary Clinton was appointed as the Secretary of State. In March 2009, Bryan Pagliano and Justin Cooper transferred all e-mails from the Apple computer to a newly established e-mail server (Clinton Email Investigation Timeline, 2018). The old Apple computer that served as e-mail server was given to a household staff member as a personal computer (Clinton Email Investigation Timeline, 2018).

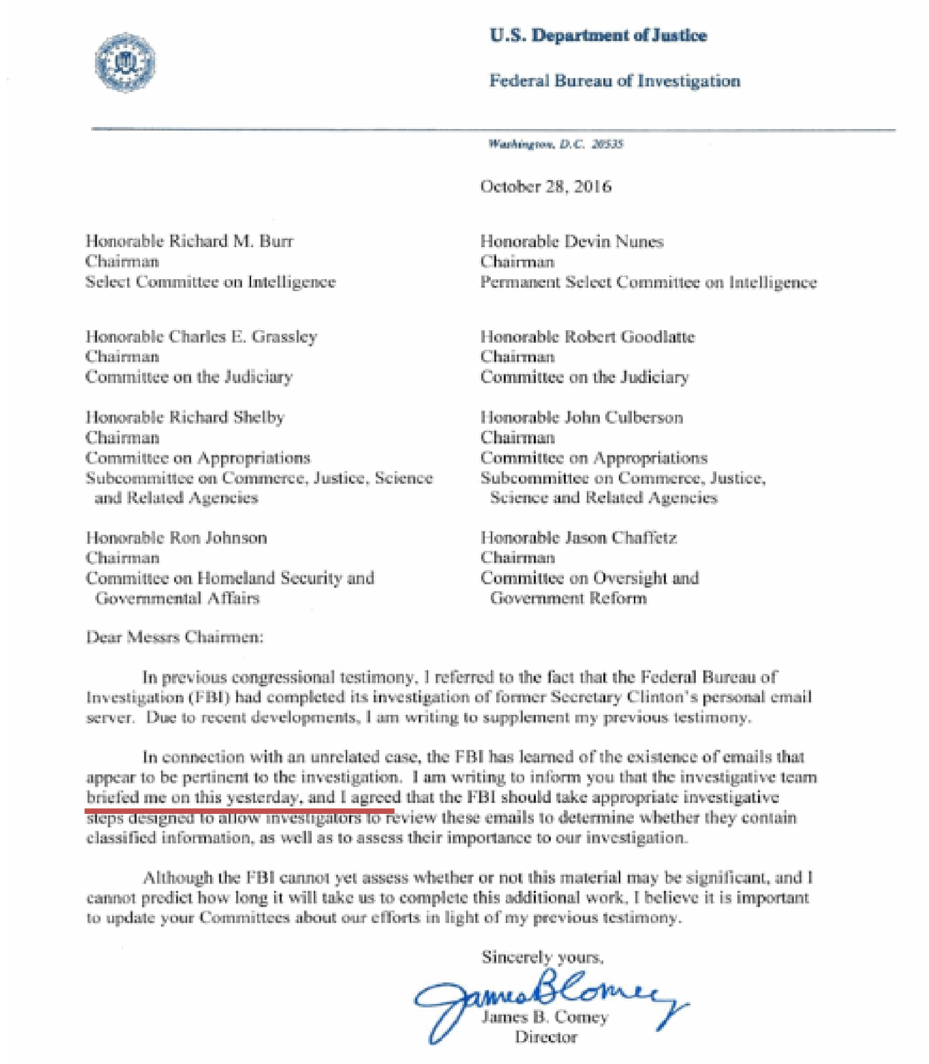
In November 2012, the private e-mail server was configured to use Google as the backup server, and a month later, investigators asked Hilary Clinton if she used a personal e-mail for classified e-mails (CNN, 2016), (Clinton Email Investigation Timeline, 2018).. From media reports it was obvious that e-mails were not encrypted, nor were they digitally signed. The reason was the lack of complying with available security standards and the best practices for official e-mail communication.

In March 2013, a hacker named "Guccifer" widely distributed e-mails sent to Clinton (The Smoking Gun, 2013). In November 2014, a special committee asked Clinton to release e-mails about terrorist attacks on the U.S. Consulate in Benghazi, so she released e-mails from her private and official .gov e-mail accounts (Kalvapalle R, 2016). On 10th of July 2015, the FBI formally began an investigation to determine whether a private e-mail server was used for storing or transmitting classified information by Hillary Clinton and her associates. In that way they wanted to check if she violated federal criminal statutes. On 26th of July 2015, Clinton denied that she used her private server to send classified e-mails while she was the Secretary of State (Scott E., 2015):

"I am confident that I never sent nor received any information that was classified at the time it was sent and received,"

On September 23, 2016, FBI released 200 pages (LoBianco T., 2016) from its investigation of Clinton's private e-mail server. On 28th of

October, the story about Clinton's private e-mail server culminated when FBI director James Comey announced (Silver N., 2017) his letter (Comey Letter, 2016), where he stated that e-mail server contains *"emails that appear to be pertinent to the investigation."*



U.S. Department of Justice

Federal Bureau of Investigation

Washington, D.C. 20535

October 28, 2016

Honorable Richard M. Burr
Chairman
Select Committee on Intelligence

Honorable Devin Nunes
Chairman
Permanent Select Committee on Intelligence

Honorable Charles E. Grassley
Chairman
Committee on the Judiciary

Honorable Robert Goodlatte
Chairman
Committee on the Judiciary

Honorable Richard Shelby
Chairman
Committee on Appropriations
Subcommittee on Commerce, Justice, Science
and Related Agencies

Honorable John Culberson
Chairman
Committee on Appropriations
Subcommittee on Commerce, Justice,
Science and Related Agencies

Honorable Ron Johnson
Chairman
Committee on Homeland Security and
Governmental Affairs

Honorable Jason Chaffetz
Chairman
Committee on Oversight and
Government Reform

Dear Messrs Chairmen:

In previous congressional testimony, I referred to the fact that the Federal Bureau of Investigation (FBI) had completed its investigation of former Secretary Clinton's personal email server. Due to recent developments, I am writing to supplement my previous testimony.

In connection with an unrelated case, the FBI has learned of the existence of emails that appear to be pertinent to the investigation. I am writing to inform you that the investigative team briefed me on this yesterday, and I agreed that the FBI should take appropriate investigative steps designed to allow investigators to review these emails to determine whether they contain classified information, as well as to assess their importance to our investigation.

Although the FBI cannot yet assess whether or not this material may be significant, and I cannot predict how long it will take us to complete this additional work, I believe it is important to update your Committees about our efforts in light of my previous testimony.

Sincerely yours,

James B Comey

James B. Comey
Director

Figure 49. Comey Letter (2016), (Silver N., 2017)

This letter had a significant impact on Senator Clinton's presidential election outcome since indicator polls (Silver N., 2017) of popularity declined and never recovered again. The US presidential election was held 12 days after Comey's letter, on Tuesday, November 8, 2016.

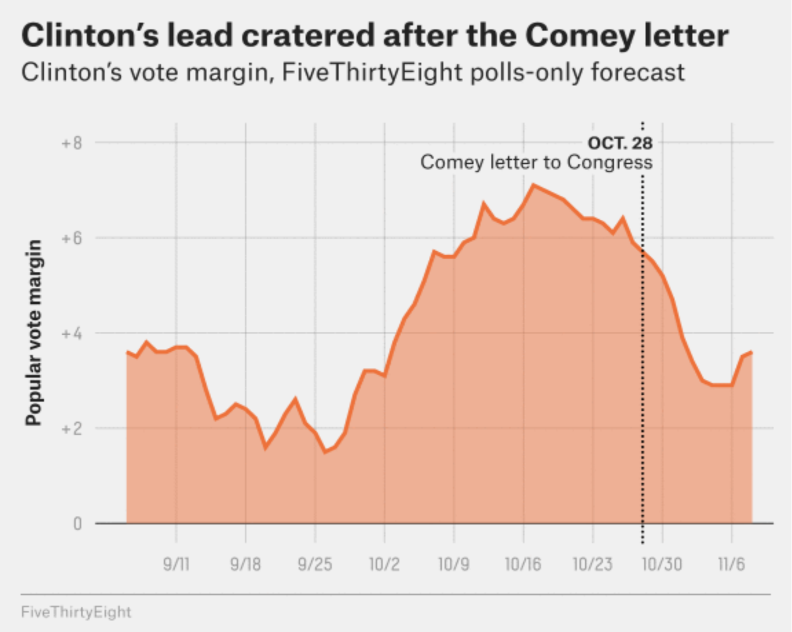


Figure 50. Polls show Clinton's popularity declined after FBI director letter was released (Silver N., 2017)

Webstresser

On April 2018, law enforcements from Britain, Croatia, Canada, Serbia and other countries (Cimpanu C., 2018) arrested administrators responsible for establishing the web service webstresser (webstresser.org and webstresser.co) in 2015.

This service whose monthly subscription costed 15 Euros provided its users the ability to launch DDoS attacks on selected Internet targets. Even inexperienced users could have used this service to launch devastating attacks (Eyerys, 2018).

It was assumed that attackers used botnets to amplify attacks on the targeted system. The service was looking for botnets which were later used to initiate the attack on specified targets.

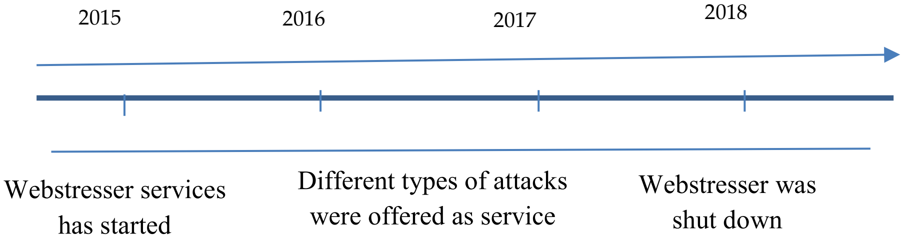
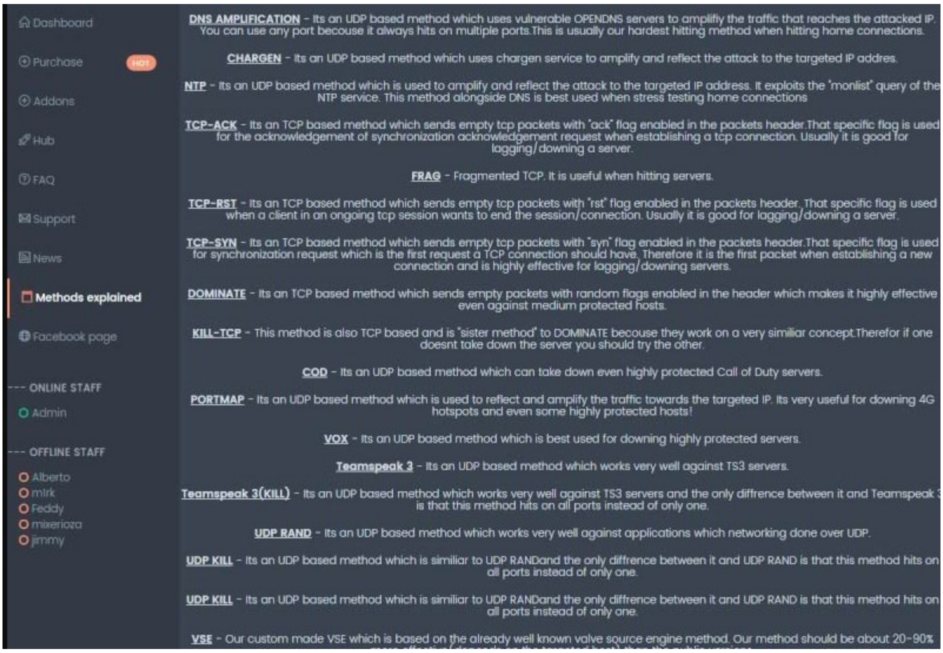

2015
2016
2017
2018
Webstresser services has started
Different types of attacks were offered as service
Webstresser was shut down

Figure 51. Webstresser existence time line

This is one of the newer types of hacking attacks where malicious attacks offered hacker's web service.



DNS AMPLIFICATION - Its an UDP based method which uses vulnerable OPENDNS servers to amplifiy the traffic that reaches the attacked IP. You can use any port becouse it always hits on multiple ports.This is usually our hardest hitting method when hitting home connections.

CHARGEN - Its an UDP based method which uses chargen service to amplify and reflect the attack to the targeted IP addres.

NTP - Its an UDP based method which is used to amplify and reflect the attack to the targeted IP address. It exploits the "monlist" query of the NTP service. This method alongside DNS is best used when stress testing home connections

TCP-ACK - Its an TCP based method which sends empty tcp packets with "ack" flag enabled in the packets header.That specific flag is used for the acknowledgement of synchronization acknowledgement request when establishing a tcp connection. Usually it is good for lagging/downing a server.

FRAG - Fragmented TCP. It is useful when hitting servers.

TCP-RST - Its an TCP based method which sends empty tcp packets with "rst" flag enabled in the packets header. That specific flag is used when a client in an ongoing tcp session wants to end the session/connection. Usually it is good for lagging/downing a server.

TCP-SYN - Its an TCP based method which sends empty tcp packets with "syn" flag enabled in the packets header.That specific flag is used for synchronization request which is the first request a TCP connection should have. Therefore it is the first packet when establishing a new connection and is highly effective for lagging/downing servers.

DOMINATE - Its an TCP based method which sends empty packets with random flags enabled in the header which makes it highly effective even against medium protected hosts.

KILL-TCP - This method is also TCP based and is "sister method" to DOMINATE becouse they work on a very similiar concept.Therefor if one doesnt take down the server you should try the other.

COD - Its an UDP based method which can take down even highly protected Call of Duty servers.

PORTMAP - Its an UDP based method which is used to reflect and amplify the traffic towards the targeted IP. Its very useful for downing 4G hotspots and even some highly protected hosts!

VOX - Its an UDP based method which is best used for downing highly protected servers.

Teamspeak 3 - Its an UDP based method which works very well against TS3 servers.

Teamspeak 3(KILL) - Its an UDP based method which works very well against TS3 servers and the only diffrence between it and Teamspeak 3 is that this method hits on all ports instead of only one.

UDP RAND - Its an UDP based method which works very well against applications which networking done over UDP.

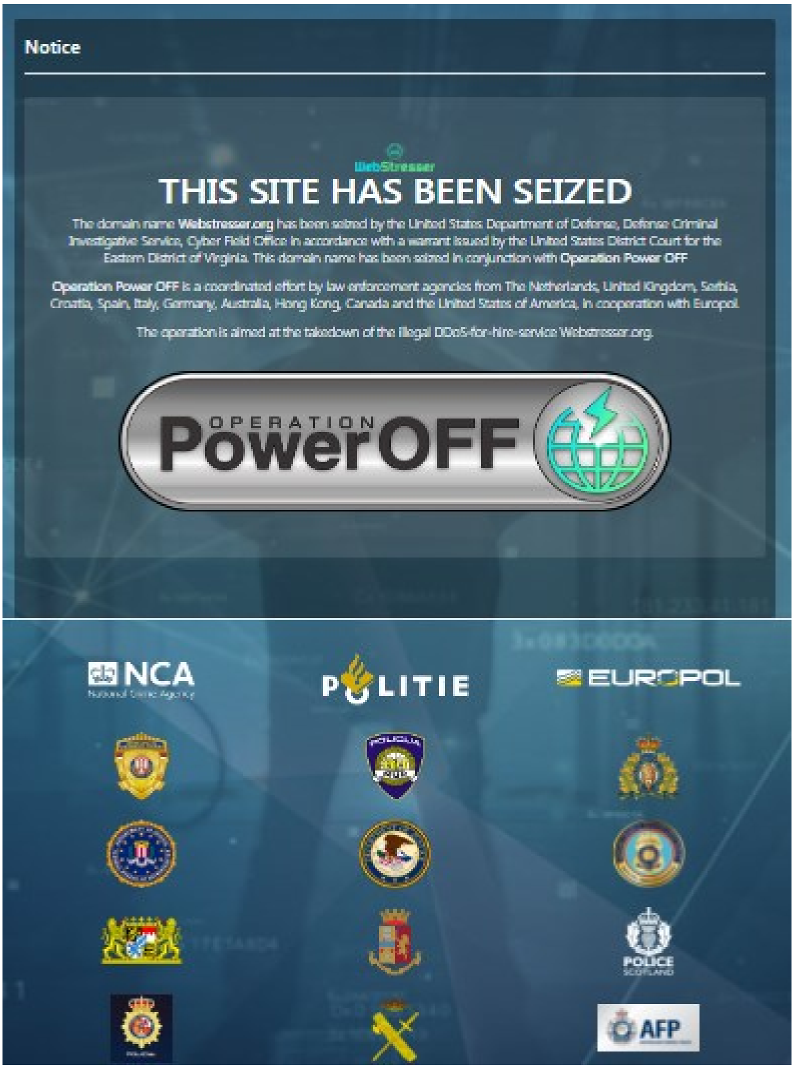
UDP KILL - Its an UDP based method which is similiar to UDP RANDand the only diffrence between it and UDP RAND is that this method hits on all ports instead of only one.

UDP KILL - Its an UDP based method which is similiar to UDP RANDand the only diffrence between it and UDP RAND is that this method hits on all ports instead of only one.

VSE - Our custom made VSE which is based on the already well known valve source engine method. Our method should be about 20-90%

Figure 52. (Eyerys, 2018)

According to Washington Post (Shaban H., 2018), this service had 136,000 registered users who performed 4 million attacks. As a result of the law enforcement action, webstresser hardware was seized in the United States, the Netherlands, and Germany. The mastermind of this hacker service was a 17-year-old Croatian citizen from a small town near the Croatian capital, Zagreb, with other hackers from Serbia, Canada, and Britain (Shaban H., 2018).



Notice

WebStresser

THIS SITE HAS BEEN SEIZED

The domain name **Webstresser.org** has been seized by the United States Department of Defense, Defense Criminal Investigative Service, Cyber Field Office in accordance with a warrant issued by the United States District Court for the Eastern District of Virginia. This domain name has been seized in conjunction with **Operation Power OFF**

Operation Power OFF is a coordinated effort by law enforcement agencies from The Netherlands, United Kingdom, Serbia, Croatia, Spain, Italy, Germany, Australia, Hong Kong, Canada and the United States of America, in cooperation with Europol.

The operation is aimed at the takedown of the illegal DDoS-for-hire-service Webstresser.org.

Figure 53. Locked *http://webstresser.org/* address accessed 01.07.2018

Law enforcements locked one of the webstresser's web pages.

Summary

All the mentioned threats and attacks in this chapter resulted in numerous known and unknown cyber and information security incident cases. Fewer well-known cases covered by media and presented in this book happened to the Central Bank of Bangladesh, the retail-chain Target, the Sony Entertainment Company, and during the 2016 US Presidential Campaign. Presented cases could have been avoided if appropriate cyber and information security controls had been implemented, monitored, and audited. In previous chapters are given explanations of security of cyber and information system components that play important role in shaping cyber security landscape. Core of the explained cases have roots in improper configuration and administration of information components. In some cases such as Webstresser case we can understand that criminals were not aware of consequences after they create technical solutions for automated attacks for any person who is willing to start attack. It is clear that general knowledge of cyber security is problem as well because attack organisers in many cases think that they will not be caught.

Knowledge acquired

In this chapter, it is possible to gain knowledge about well-known cyber incident cases reported by many resources and media, which further show why cyber security must be treated as one of the top priorities.

Review questions

1. What are key attack motivations in presented cases?
2. How could e-mail and data encryption help in preventing hacker attacks in presented cases?
3. For which of presented cases could antimalware protection prevent attack escalation?

Further readings

- India bank hack 'similar' to $81 million Bangladesh central bank heist https://www.reuters.com/article/us-city-union-bank-swift/india-bank-hack-similar-to-81-million-bangladesh-central-bank-heist-idUSKCN1G319K

- Before massive Bangladesh heist, New York Fed feared such cyber attacks https://www.reuters.com/article/us-bangladesh-heist-fed-insight-idUSKCN0XX28F

- Bangladesh to sue Manila bank over $81-million heist https://www.reuters.com/article/us-cyber-heist-bangladesh/bangladesh-to-sue-manila-bank-over-81-million-heist-idUSKBN1FR1QV

- Bangladesh Bank Attackers Hacked SWIFT Software https://www.bankinfosecurity.com/report-swift-hacked-by-bangladesh-bank-attackers-a-9061

- The Bangladesh Bank Heist: Lessons in Cyber Vulnerability http://theonebrief.com/the-bangladesh-bank-heist-lessons-in-cyber-vulnerability/

- Target cyber breach hits 40 million payment cards at holiday peak https://www.reuters.com/article/us-target-breach/target-cyber-breach-hits-40-million-payment-cards-at-holiday-peak-idUSBRE9BH1GX20131219

- Specialty retailer becomes target of cyber-attack https://www.chainstoreage.com/article/specialty-retailer-becomes-target-cyber-attack/

- Supply Chain Attacks on Retail – What Happens When Trusted Channels Can't be Trusted? https://www.rsaconference.com/blogs/supply-chain-

attacks-on-retail-what-happens-when-trusted-channels-cant-be-trusted

- The Untold Story of the Target Attack Step by Step https://aroundcyber.files.wordpress.com/2014/09/aorato-target-report.pdf

- Target Confirms Point-of-Sale Malware Was Used in Attack https://www.securityweek.com/target-confirms-point-sale-malware-was-used-attack

- Sony to pay staff $8m compensation over cyber-attack http://www.bbc.com/news/entertainment-arts-3493148

- The Attack on Sony https://www.cbsnews.com/news/north-korean-cyberattack-on-sony-60-minutes/

- Clinton campaign 'hacked' along with other Democratic groups http://www.bbc.com/news/election-us-2016-36927523

- How Russia-linked hackers stole the Democrats' emails and destabilised Hillary Clinton's campaign http://www.abc.net.au/news/2017-11-04/how-russians-hacked-democrats-and-clinton-campaign-emails/9118834

- Exclusive: Clinton campaign also hacked in attacks on Democrats https://www.reuters.com/article/us-usa-cyber-democrats-investigation-exc/exclusive-clinton-campaign-also-hacked-in-attacks-on-democrats-idUSKCN1092HK

- 2016 Presidential Campaign Hacking Fast Facts https://edition.cnn.com/2016/12/26/us/2016-presidential-campaign-hacking-fast-facts/index.html

- https://www.independent.co.uk/life-style/gadgets-and-tech/news/webstresser-internet-ddos-europol-nca-cybersecurity-a8321751.html

- WebStresser.org site linked to global cyberattacks is shut down https://www.irishtimes.com/news/world/europe/webstresser-org-site-linked-to-global-cyberattacks-is-shut-down-1.3478112

- DDoS-for-Hire Service Webstresser Dismantled https://krebsonsecurity.com/2018/04/ddos-for-hire-service-webstresser-dismantled/

- Video for Webstresser operation:

https://www.youtube.com/watch?v=-a9roduqf4I

5. Cyber security controls

Chapter abstract

Chapter goals: To present the Risk management process, define internal controls, and control objectives for which standards such as the ISO 27000 family 27000 (ISO 27001:2013, ISO 27005:2008, and other) and COBIT 5 framework can be implemented. Furthermore, the chapter explains and distinguishes between preventive, detective, corrective, general, and specific controls.

Learning outcomes: Gaining knowledge on risk management processes and the type of standards and frameworks which can be used for the establishment of internal controls to manage cyber security. Understanding different types of controls.

Information technology usage related to Cyber risk

In the present business environments, Information Technology (IT) is used to improve business operations and performances. Usage of IT in everyday operations is susceptible to unavoidable risks explained in the previous chapter.

Risk management

Every organisation has to manage risks associated with information technology usage. This process contains steps such as risk analysis, risk assessment, and risk treatment.

Risk analysis

Risk analysis helps in the identification of threats, vulnerabilities, likelihood, and the impact of unwanted events.

Risk assessment

In the risk assessment phase, information assets (people, information, services, hardware, software, network, site, organisation, and intangibles) have to be identified. Identified threats, vulnerabilities, likelihood, and impact have to be determined and calculated for the recognised information assets. The following phase is the risk treatment plan, and it has several strategies.

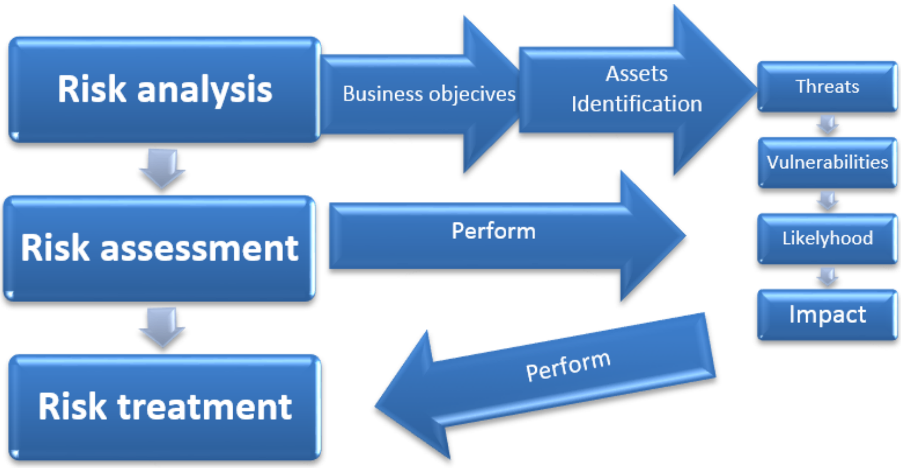


Figure 54. Risk management process

Risk treatment

Risk treatment can be done using the following strategies:

- Risk mitigation through implementation controls to reduce risk.

- Risk acceptance by accepting risk without taking any kind of control.
- Risk avoidance through avoiding the execution of an action which can cause risk.
- Risk transfer through transferring risk to somebody else, e.g. suppliers of web hosting service, taking insurance, etc.

Internal controls

Goals of internal controls have a dual nature – what should be achieved and what should be avoided. Internal controls are implemented through organisational policies, procedures, practices, and organisational systematization and structure with the goal of managing organisation's risks. Internal controls are applicable at all levels of any organisation. Management is responsible for strategic decisions in introducing internal controls into the organisation culture. There are three classes of internal controls: preventive, detective, and corrective.

Purpose of internal controls

The essential logic of audit is to investigate whether internal controls exist, how it is implemented, and whether it is monitored on regular basis. If internal controls do not exist, internal auditors suggest their implementation.

A typical risk in business is the neglecting of the need for internal controls when new technology is introduced, since all technology is implemented with the goal of having faster or cheaper operations. In essence, all technology has the risk of usage, and those who implement new technology usually overlook all associated risks. This is because they are preoccupied with core needs and benefits of implemented technology and do not consider all associated risk with the specific technology.

There are eight review areas Information Systems Audit and Control Association (ISACA), (CISA 2015, pp. 295) which can also be used in auditing:

1. Enterprise architecture and auditing
2. Hardware audit
3. Operating system audit
4. Database audit
5. Network infrastructure audit
6. Information system operation audit
7. Scheduling audit
8. Problem management reporting audit

Control objectives

Information system control objective has to be established with the goal to provide assurance that business objectives will be reached through selection of applicable controls which will be implemented and monitored.

Internal control requirements could be established to fulfil some or all aspects:

- Confidentiality
- Integrity
- Availability
- Effectiveness
- Economy

- Efficiency
- Non-repudiation
- Reliability
- Accountability

Internal controls should use a goal for criteria which can be an accepted standard and technique, best practice, or framework.

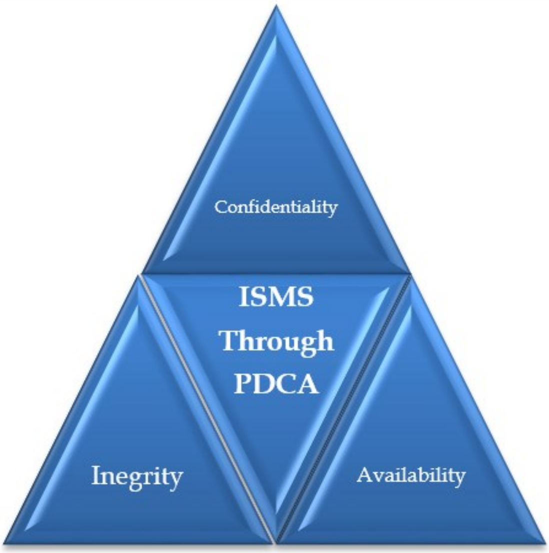


Figure 55. CIA Triad

ISO 27001

The above requirements are common for standards such as ISO 27001 (ISO 27001:2013) which acknowledges three aspects of information security, namely Confidentiality, Integrity, and Availability (CIA).

Implementation of the information security using the ISO 27001 standard (ISO 27001:2013) suggests that Information Security Management System (ISMS) has to be established and maintained through the Plan-Do-Check-Act (PDCA) process of improvement (ISO 27001:2013).

In the **Plan** phase, the project border agreement is established, thus, physical locations and systems are included or excluded form the scope. Afterwards, the overall information security policy is established and approved by the top management. The following stage entails the collection of information from information assets through process mapping and GAP analysis.

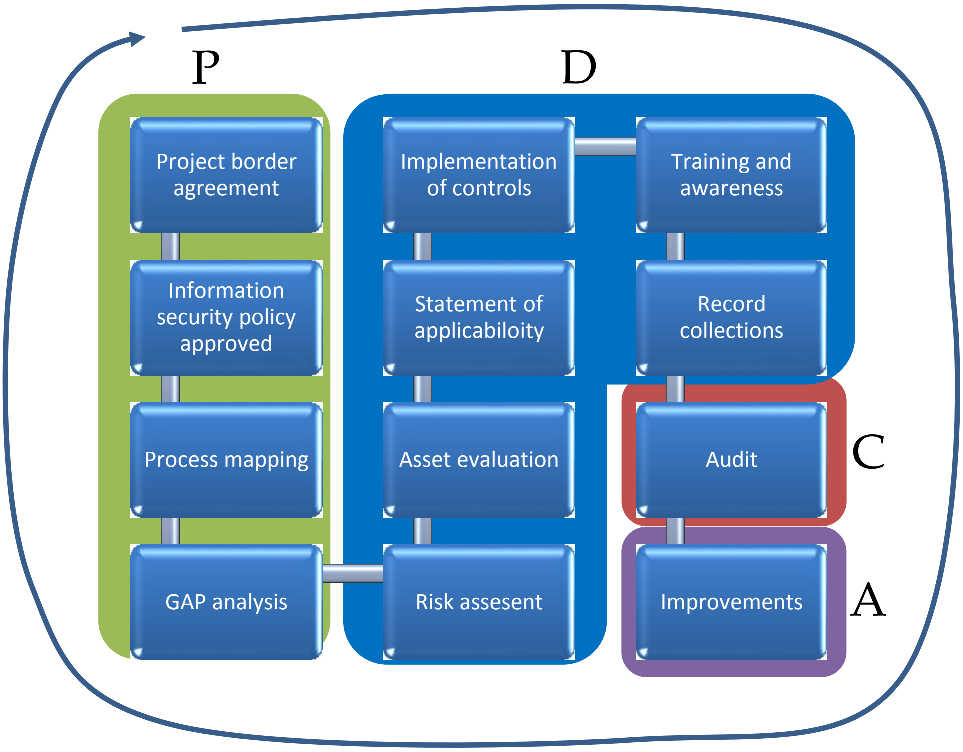


Figure 56. ISMS PDCA cycle

In the **Do** phase, risk assesent (ISO 27005:2008 standard for security risk management is developed suitable for ISO 27001:2013 implementation) is conducted through asset evaluation vulnerabilities, threats, likelyhood, and impact. After this stage, statement of applicability is created with a goal to approve plan for implementation of controls. Last come training and awareness and collection of records.

In the **Check** phase, information security audits are performed, folowing the previosly explained General scheme of the auditing process.

After detecting space for improvements in the check phase, the **Act** phase ensures that improvements are actually made. The purpose of the PDCA cycle is to constantly improve system performances through constant improvements. ISMS as a system can be certified by the external certification body which will additionally improve the system performance.

3E's

The 3E's approach KPMG (2018) of excellence is used for measuring performances of any organisation: Economy – reducing costs of inputs, Efficiency – the right effort allocation, Effectiveness –achieving determined goals.

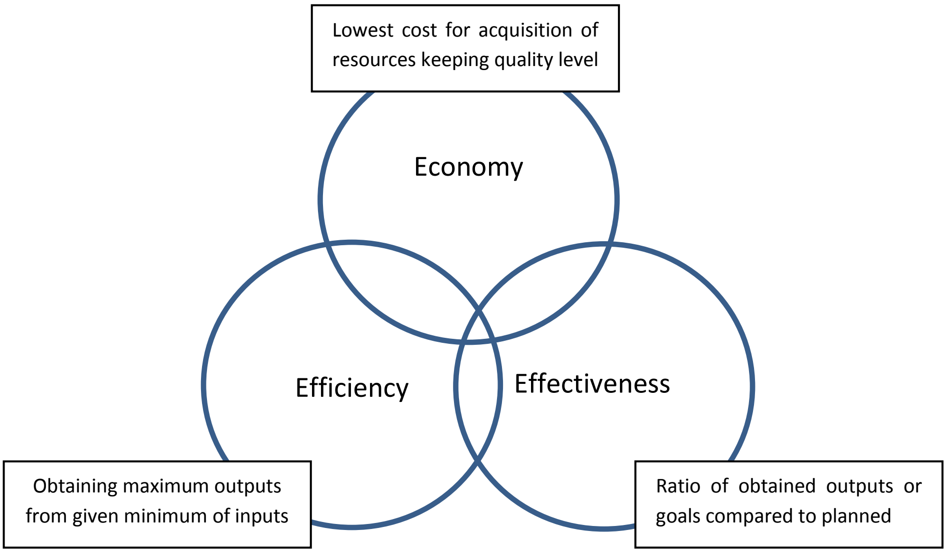

Lowest cost for acquisition of resources keeping quality level
Economy
Efficiency
Effectiveness
Obtaining maximum outputs from given minimum of inputs
Ratio of obtained outputs or goals compared to planned

Figure 57. Business performance measurement using 3E’s

(KPMG, 2018)

COBIT 5

ISACA developed Control Objective for IT (COBIT 5) framework with five major principles (ISACA, 2012):

1. Meeting stakeholders' needs – every organisation exists due to its stakeholders, thus business must use IT to meet stakeholders' needs.

2. Covering enterprise end-to-end – covering not only IT but all issues which encompass everyone and everything.

3. Applying single integrated framework – because there are many IT related frameworks, COBIT 5 aligns with all other frameworks and standards.

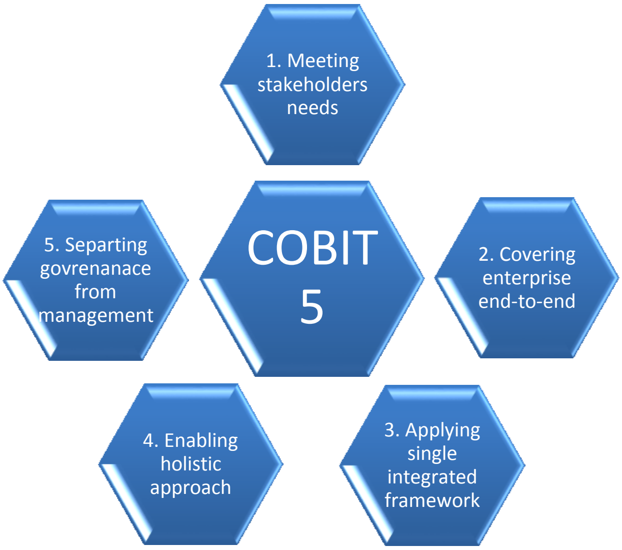

1. Meeting stakeholders needs
5. Separting govrenanace from management
COBIT 5
2. Covering enterprise end-to-end
4. Enabling holistic approach
3. Applying single integrated framework

Figure 58. ISACA's COBIT5 (ISACA, 2012):

4. Enabling holistic approach – COBIT 5 defines seven categories of enablers which support governance and management of enterprise (CISA 2015, pp.154.):

- "Principles, Policies, and Frameworks

- Processes
- Organisational Structures
- Culture, Ethics, and Behaviour
- Information
- Services, Infrastructure, and Applications
- People, Skills, and Competencies"

5. Separating governance from management – Governance and management, according to COBIT 5, have a recognisable distinction.

Preventive controls

Controls are established to avoid errors and interruptions, to segregate duties by implementing mechanisms such as four-eye, and to monitor for potential problems in their early stages.

Detective controls

Detective controls have to be established to detect malicious events, failures, and errors.

Corrective controls

Corrective controls are used to correct errors, interruptions, detected problems, and bottlenecks.

General controls

General controls are controls related to all parts of organisation, such as controls related to physical and logical security policies, accounting, proper use of assets, and tracking transactions, as well as administrative controls, and other related controls (CISA 2015, pp. 45.).

Specific controls

General controls can be used to create specific controls. From the perspective of information system controls with a goal of managing information and cyber security following areas can be used to create specific controls:

- Business continuity and disaster recovery planning;
- Access to information resources such as databases, configuration files, and communication devices;
- BYOD policy.

Specific controls examples

Following are few examples of areas which appear as particularly interesting for the implementation of specific controls.

Business continuity and Disaster recovery related controls

Business continuity and disaster recovery management addresses availability of information and information assets.

Physical security, utilities, and environment are needed so that equipment and employees are safe at work. Controls have to be established, so that security perimeters and backup communication links exist, and that backup power supply from secondary grid is available.

Disaster recovery planning is related to hardware, software, and infrastructure which support business operations (Everest D., et. al., 2008).

Business continuity planning is related to business operations and relies on infrastructure, software, and hardware (Everest D., et. al., 2008).

All mentioned aspects are needed to give resilience to business operations in a specific business surrounding. Before the digital age, business operations were possible without hardware and software. However, in today's business world, business is not possible without computers. As such, DRP has to support BCP (Everest D., et. al., 2008).

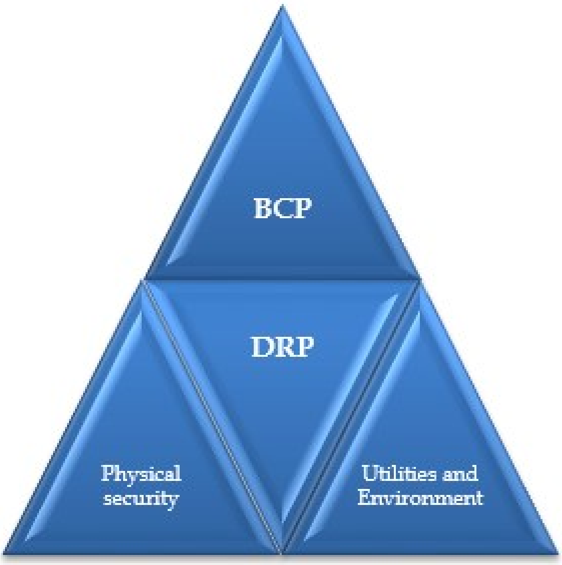


Figure 59. BCP DRP triangle

Risk assessment is a crucial part of BCP / DRP management process where Recovery Time Objective (RTO) and Recovery Point Objective (RPO) have to be determined (Everest D. et al, 2008). RTO represents how quickly operations have to be restored, while RPO shows the amount of unavailable operations and data, which could consequently cause problems.

Based on the risk, appetite management is willing to spend additional money for the implementation of strategies that specific technologies and facilities can support.

Every business process has to be supported by appropriate plans with conducted Business Impact Analysis (BIA).

BCP / DRP plans have to be tested at regular intervals, and recognised weaknesses in test process have to be resolved.

All the aforementioned areas are fields for the implementation of internal controls to monitor effectiveness of implementations.

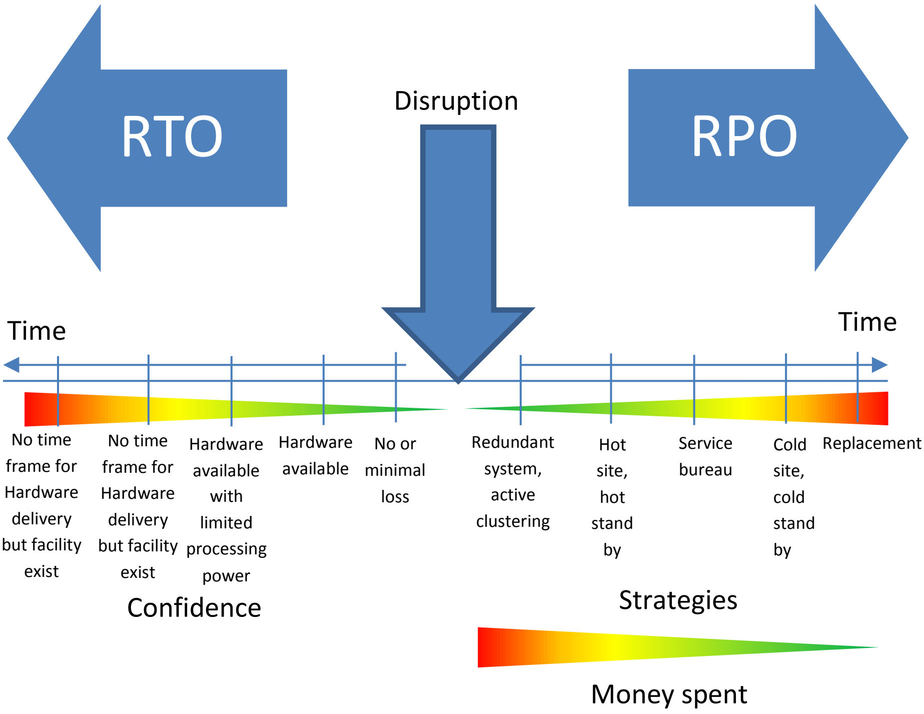

RTO
Disruption
RPO
Time
Time
No time frame for Hardware delivery but facility exist
No time frame for Hardware delivery but facility exist
Hardware available with limited processing power
Hardware available
No or minimal loss
Redundant system, active clustering
Hot site, hot stand by
Service bureau
Cold site, cold stand by
Replacement
Confidence
Strategies
Money spent

Figure 60. RTO / RPO relation

Bring Your Own Device (BYOD) controls

The Bring Your Own Device (BOYD) policy implements new types of security risks. The reason is because new personal devices are brought by people who use systems on production networks which are allowed by policies of many organizations. Tests for security weaknesses and risks have to be rigorous for this type of devices. This task is not easy because personal devices are not installed uniformly and usually have different software such as operating systems and application. These devices have to be taken care of by preventing infection with malware, and by making sure they are patched.

A BYOD device has to be configured so that when it is lost all data is deleted and information confidentiality remains intact.

If appropriate controls are not deployed, usage of these kinds of devices can increase security risks and produce negative consequences for the system in which they are brought.

Summary

Cyber and information security controls are needed as a management tool for setting up internal control mechanisms. This has to be done through appropriate risk management, such as risk analysis, risk assessment, and risk treatment. For this purpose, control objectives have to be defined. Control objectives can be classified as preventive controls, detective controls, corrective controls, general controls, or specific controls using available standards such as ISO 27001 (ISO 27001:2013), NIST, and COBIT 5.

Knowledge acquired

In this chapter, it is possible to gain knowledge about risk management process, different approaches for conducting risk assessment, and different risk management approaches.

Review questions

1. Explain the risk management process.

2. What are risk treatment options?

3. What are internal controls?

4. What are control objectives?

5. Explain PDCA cycle and for what purpose it is used.

6. Name possible preventive controls.

7. What can be a specific control?

8. Name possible specific controls.

9. What is BCP?

10. What is DRP?

11. Explain the meaning of RTO and RPO.

12. What is the risk analysis?

13. What are five major principles of the COBIT5 framework?

Further readings

- About Risk Management https://www.theirm.org/the-risk-profession/risk-management.aspx

- Risk Treatment https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/rm-process/risk-treatment

- 5 Types of Risk Treatment https://simplicable.com/new/risk-treatment

- INTERNAL CONTROLS http://www.accaglobal.com/gb/en/student/exam-support-

resources/fundamentals-exams-study-resources/f1/technical-articles/internal-controls.html

- ISO/IEC 27000 family - Information security management systems https://www.iso.org/isoiec-27001-information-security.html

- Economy, Efficiency, Effectiveness http://www.en.valuemex.com/node/23

- ARE YOU USING THE 3 E'S OF MANAGEMENT TO MEASURE YOUR PERFORMANCE? https://www.jhmriskmanagementservices.co.uk/blog/are-you-using-the-3-es-of-management-to-measure-your-performance/

- What is COBIT 5? https://www.youtube.com/watch?v=Y8kqh9q3Jwg

- Business Continuity and Disaster Recovery for InfoSec Managers https://www.sciencedirect.com/science/book/9781555583392

- BRING YOUR OWN DEVICE... HOW TO STAY IN CONTROL https://www.clearswift.com/sites/default/files/documents/pdf/bring-your-own-device-how-to-stay-in-control.pdf

6. Cyber security audit

Chapter abstract

Chapter goals: To present the three lines of defence model, organisation responsibilities in security governance, and cyber security audit. To present audit objectives, types of audits, and risk-based auditing. Chapter also aims to explain audit risk, and different types risk-based approaches such as qualitative and quantitative. Furthermore, it will introduce audit risk types and structure of audit reports which includes condition, criteria, cause, and effect of Internal Auditing. Based on ISACA guidelines, it is possible to perform cyber security audit for following areas: hardware, operating systems, databases, network infrastructure audit, information systems, scheduling audit, and problem management reporting.

Learning outcomes: Gaining knowledge of three lines of defence model and the role of internal audit in the organisation defence. Becoming acquainted with audit risk types and risk associated to audit process. Understanding areas and topics that can be object of auditing.

Organisation defence model

To perform audit of computer network infrastructure which supports organisation processing facilities, it is necessary that Internal Auditor (IA) has a good knowledge of the operation of equipment explained in previous chapters. An auditor has to ask questions verbally or in a documented way using questionnaire, and check the list to determine state of information security in the organisation so that she or he can provide audit assurance state of the information security. Organisations such as financial institutions (commercial services and regulatory organisations), military capacities, nuclear power plants which are considered as vital infrastructures can bring whole countries and regions into hard and challenging incident situations. That is why it is important to have well-defined lines of defences in digital surroundings at all levels. If the object of protection is communication lines, it is necessary to have more defence perimeters such as demilitarised zones, internal and external firewalls, network intrusion detection systems, host intrusion detection systems, and anti-malware software. In addition to engineers, multiple levels of defence precautions, specific organisational measures, and defence perimeters are needed. The well-known three lines of defence (TLoD) model implements a systematic approach to manage risk.

The Institute of Internal Auditors (IIA, 2013) recognised three lines of defence as following:

- First line of defence: Operational management
- Second line of defence: Risk management and compliance function
- Third line of defence: Internal audit

The three lines of defence model

There is a well-known saying which says: "divide and conquer". This saying is applicable to governing of cyber and information security. Explanation and modelling of the three levels of defence mechanisms acquired all over the globe and brought by IIA (2013) are given in the following paragraphs.

The first line of defence: Operational management

The first line of defence are managers, because they control and manage risks. Furthermore, managers implement internal controls and perform corrective actions. Operational management is placed in the first line of defence, because all operations that are supported for example by IT functions must be conducted at this level. Additionally, this defence includes controls against active and passive attacks, anti-malware protection, and definition and reinforcement of password policies.

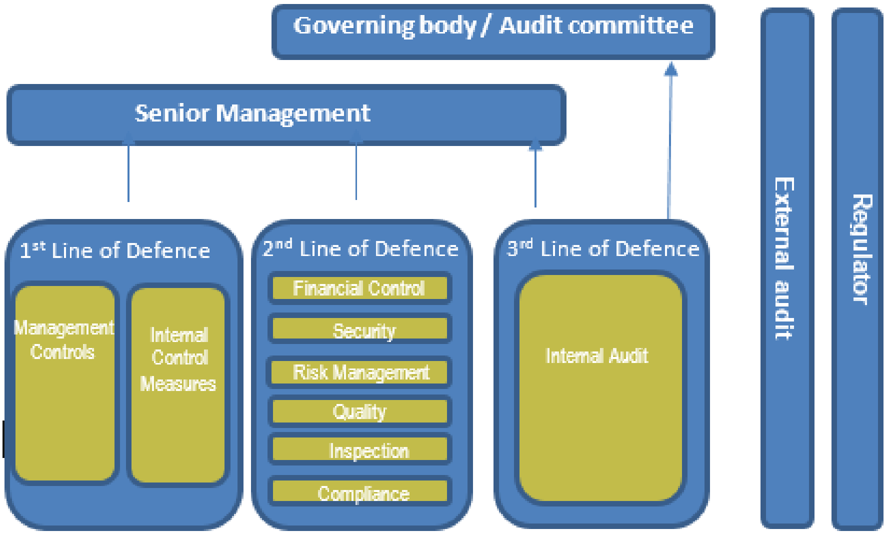


Figure 61. The three lines of defence model (IIA, 2013)

The second line of defence: Compliance and Risk Management

Goal of this defence level is to provide risk management framework by identifying risk areas and manage risk. This defence level is also responsible for monitoring effectiveness of internal controls, and adjusting internal operations with laws and regulatory requirements.

The third line of defence: Internal audit

In this model, internal audit is placed in the third defence line, and its function is to provide independent assurance using international standards. In its operations, internal audit function has to provide reports to audit committee and governing board about state of specific business area that was an object of audit.

Purpose of internal audit is to provide independent assurance regarding business operations and according to IIA (2013) to:

- Evaluate and report on degree of alignment;
- Evaluate and report on corporate risk management practices and results;
- Evaluate and report on efficiency;
- Evaluate and report on degree of effectiveness of measures in place and metrics in use;
- Evaluate and report on efficiency, effectiveness or resource management;

According to ISACA, auditors' task at management level is to evaluate and report on degree of alignment, while in strategic alignment, their task is to evaluate and report on corporate risk management practices and results. In the risk management process auditors need to evaluate and report on efficiency and to evaluate and report on degree of effectiveness of measures in place and metrics in use in organisation value delivery. Furthermore, their role in performance measurement is to evaluate and report on efficiency or resource management, and to evaluate and report on effectiveness of assurance processes performed by different areas of management compared to other organisational roles, as it is shown in Table 10.

Organisation responsibilities in security governance

Below is Brotby, (2006): in Information Security Governance: Guidance for Information Security Managers.

Management level	Strategic Alignment	Risk Management	Value delivery	Performance measurement	Resource Management	Process Assurance
Board Directors	Require demonstrable alignment	Establish risk tolerance Oversee a policy of risk management Ensure regulatory compliance.	Require reporting of security costs.	Require reporting of security effectiveness.	Oversee a policy of knowledge management and resource utilization.	Oversee a policy of assurance process integration.
Executive management	Institute processes to integrate security with business objectives	Ensure that roles and responsibilities include risk management in all activities. Monitor regulatory compliance	Require business case studies of security activities.	Require monitoring and metrics for security initiatives	Ensure processes for knowledge capture and efficiency metrics.	Provide oversight of all assurance functions and plans for integration
Steering committee	Review and assist security strategy and integration efforts Ensure that business owners support integration.	Identify emerging risks, promote business unit security practices and identify compliance issues.	Review and advise on the adequacy of security initiatives to serve business functions.	Review and advise whether security initiatives meet objectives.	Review processes for knowledge capture and dissemination.	Identify critical business and assurance providers. Direct assurance integration efforts
CISO/ information management	Develop the security strategy, oversee the security program and initiatives, and liaise with business process owners for ongoing alignment.	Ensure that risk and business impact assessments are conducted, Develop risk mitigation strategies. Enforce policy and regulatory compliance.	Monitor utilization and effectiveness of security resources	Develop and implement monitoring and metrics approaches, and direct and monitor security activities.	Develop methods for knowledge capture and dissemination, and develop metrics for effectiveness and efficiency.	Liaise with other assurance providers. Ensure that gaps and overlaps are identified and addressed.
Audit executives	Evaluate and report on degree of alignment.	Evaluate and report on corporate risk management practices and results	Evaluate and report on efficiency.	Evaluate and report on degree of effectiveness of measures in place and metrics in use.	Evaluate and report on efficiency or resources management.	Evaluate and report on effectiveness of assurance processes performed by different areas of management

Table 10. Relationship matrix in organisation structure of security governance Brotby, (2006):

Table 10. shows the way in which relationship in organisation structure of security governance could become clearer.

Cyber security audit

Cyber and information security audit is important for adding value to organisation, conducting audits, and reporting management on findings from conducted audits.

Performing an audit

Audit has to be performed through predefined steps with the goal of providing provide evidence of findings gathered during audit.

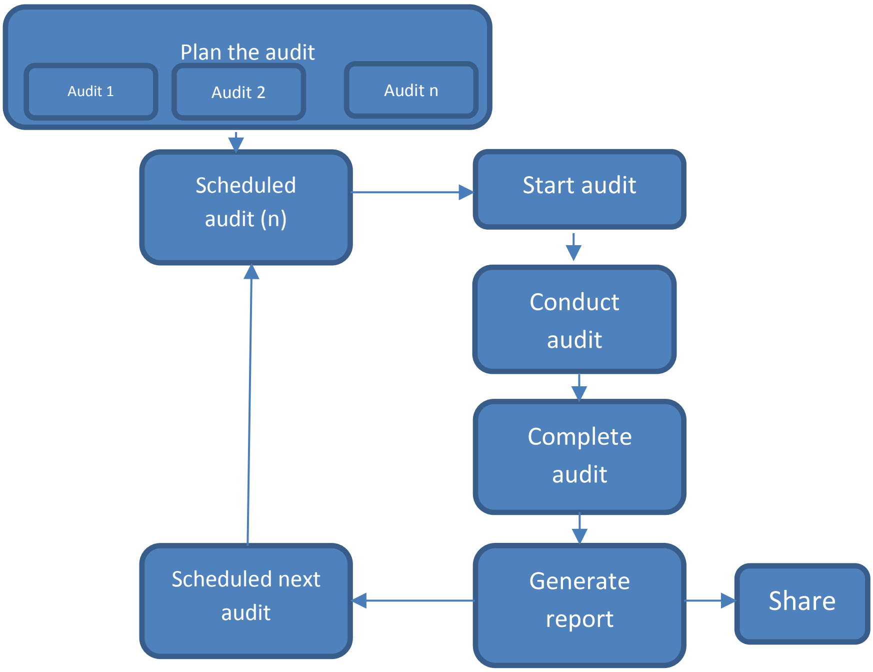


Figure 62. General scheme of audit process, (ISACA CISA 2015 pp. 42.)

Following steps are part of an audit process:

- Plan the audit engagement, by considering audit goals and risks associated with the object of audit.
- Build the audit plan with detailed goals of audit in a time line.

- Plan the execution according to an audit plan.
- Monitor project activity through reporting progress of an audit.

Audit objectives

Audit objectives are goals that are set up for each audit project and based on the selected audit type.

Types of audits

An information security auditor can perform different types of audits which are briefly explained below:

- Compliance audits are related to well-known standards such as ISO 27001, PCI DSS, HIPPA, and other related standards of specific industry and field of operation.
- Financial audits are performed to test correctness of financial reports.
- Operational audits are performed to assess specific controls of organisation processes, e.g. controls in implementation of BYOD policy.
- Administrative audits are performed to assess operational productivity effectiveness of an organisation.
- Information security audits can be used to assess the state of overall information security management system through an entire organisation. If Information Security Management System (ISMS) is implemented, limited or overall scope of the system can be an object of auditing. One of the examples is conducting limited audit scope to access rights, password policies, and segregation in networks where different checks and tests can be performed against infrastructure to provide assurance of implemented controls on network and

operating systems which represent a foundation of every infrastructure.

- Specialized audits can be conducted to assess third party services by using special standards and regulations related to specific industry.
- Integrated audits can include more types of audit, such as financial, operational, and information system and security audit.

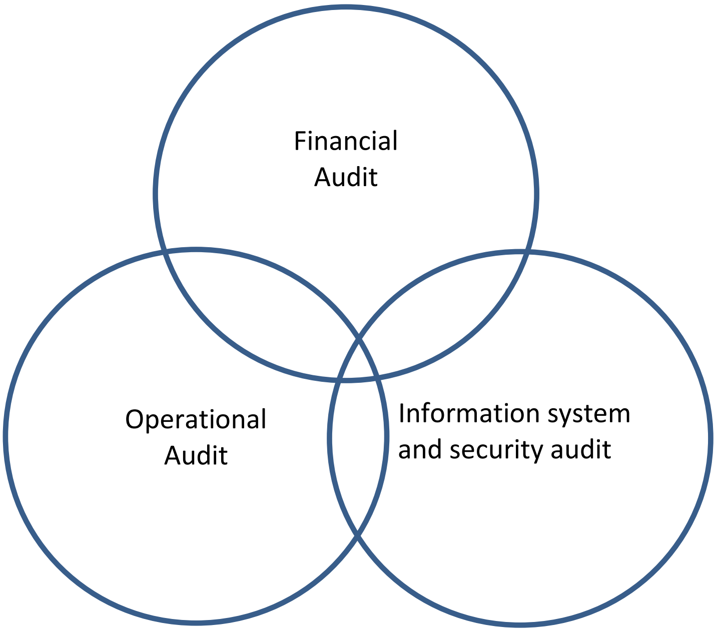


Figure 63. Integrated audit, (ISACA CISA 2015, pp. 62.)

- Forensic audits are performed after detecting fraud or a crime (CISA 2015, pp. 391.). Their main goal is to collect evidence in controlled environment and deliver it for review by authorities such as police and courts of law. Typical steps to conduct forensic investigations with a goal to prepare evidence admissible at courts are shown in Figure below.

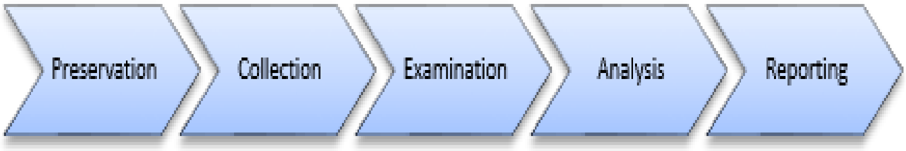


Figure 64. Digital forensic investigation (Ademu I. O., et al, 2011)

Risk-based auditing and audit risk

When selecting audit goals, it is necessary to understand what is feasible in the risk-based audit's conduct of risk assessment Chartered Institute of Internal Auditors (2014).

Risk assessment can be carried out through qualitative, semi-quantitative, or quantitative based risk assessment.

Qualitative risk-based approach

The simplest and most frequently used risk assessment approach is the qualitative risk-based approach. It uses description markings for likelihood and impacts. Furthermore, it utilizes checklists and ranking with three or four levels of risk: high, medium, and low (or very high, high, medium, low). It is based on a subjective opinion.

Semi-quantitative risk-based approach

Instead of using descriptive values such as high, medium, and low, these descriptions are also given numerical values. Thus, total weight for a specific area can be aggregated to calculate different factors and monitor outcomes.

Quantitative risk-based approach

This type of risk-based approach uses numerical values from different sources, such as the number of malware infections, number of unpatched operating systems, specific log events, number of attacks, and the time between patch release and patch implementation.

Audit risk types

Audit carries its own risks, some of which are briefly described below (CISA 2015, pp.48):

- Inherent risk existing in specific business environments, related to activities, processes, or technology used without any supervision, is considered audit risk.
- Control risk is associated with the risk that errors will not be detected on time due to no supervision or as a result of not conducting check-ups.
- Detection risk is associated with the risk that a specific error will not be recognised by an auditor.
- Overall audit risk associated with the risk that an error will not be detected by an auditor.

Evidence collection

There are different techniques to collect evidence (CISA 2015, pp. 39.):

- through structured interviews with relevant personnel
- using questionnaires,
- using checklists
- reviewing the organisation structure,
- reviewing policies,
- using relevant standards,
- reviewing documentations, system logs, and system settings,

- observing business and employee performances
- control walk-throughs
- statistical and non-statistical sampling
- attribute sampling
- stop-or-go sampling
- discovery sampling
- variable sampling

Condition, Criteria, Cause and Effect of Internal Auditing

In the audit process it advisable to use the Condition, Criteria, Cause and Effect approach (Watkins W., 2014) for the collection and documentation of evidence, as well as for the presentation of findings with audit recommendations.

Condition are pieces of evidence of that were found in the audit process.

Criteria can be best practice, known ways of doing something, how something should work, policy references, processes, and standards.

Cause is the reason that caused the recognised condition.

Effect is the impact or risk recognised set by a condition, when there are high probabilities of the condition being met, or the condition has been met already.

As already explained, there are eight review ISACA (CISA 2015, pp. 295) areas which can also serve as areas for cyber audit:

1. Enterprise architecture and auditing

2. Hardware audit
3. Operating system audit
4. Database audit
5. Network infrastructure audit
6. Information system operation audit
7. Scheduling audit
8. Problem management reporting audit

According to ISACA, environment audit is relevant for information systems and security audits, but is not relevant for cyber security because it is out of the given scope. Here mentioned are only a few issues related to environment audit in reference to information system assets.

For each ISACA area of interest there is a set of operational controls to be checked for which different standards were used, such as ISO 27001, NIST, COBIT5, and ISACA CISA (2015) guidelines. The list below, which provides the operational control sets, can be expanded with new risks recognised in the risk assessment process and risk analysis phase.

Enterprise architecture and auditing

One of the first steps in auditing information system is to review enterprise architecture, connections between branches, network design, and other infrastructure components.

Hardware audit

When performing hardware audit, it is necessary to check if all precautions are met to comply with available security controls (CISA, 2015 pp. 300):

- Protect hardware by considering different levels of security using security perimeters.
- Have a designated owner for each hardware component.
- Is the risk assessment for the critical infrastructure performed for confidentiality, integrity, and availability?
- Is maintenance performed at regular intervals specified by the vendors?
- Check if the BYOD policy is defined, and whether information security principles are satisfied.
- Separate power and communication cables, especially copper communication cables, due to possible electromagnetic interference.
- Communication cables have to be protected with conduits.

Operating system audit

When performing operating system audit it is necessary to check if all precautions are met in order to (CISA, 2015, pp. 297):

- Restrict and block unauthorised logical access controls.
- Prevent unauthorised physical or network access over IP consoles to the system console.
- Block capabilities which would enable an unauthorised person to interact with and interrupt the system.
- Maintain system patches and up-to-date system software.
- Change default passwords.

- Is there documentation where changes (addition, deletion) to access rights can be seen?
- Block unsupervised usage of Universal Serial Bus (USB) media.

When performing an operating system audit, is necessary to check if all of the following precautions are met to comply with available security controls connected to environment (CISA, 2015, pp. 297):

- Establish contracts with external parties for tasks that cannot be carried out with internal resources in process of marinating information system.
- Develop a mechanism to control access to critical infrastructure rooms using CCTV camera, biometric door locks, electronic door, or bolting door locks.
- Have UPS and electric generators to support constant power supply for computer and network infrastructure.

Database audit

When performing database audit, it is necessary to check if all of the following precautions are met in order to comply with available security controls (CISA, 2015, pp. 298.):

- All tables and views exist in entity relations as separate entities.
- All access rights and roles are justified for users and groups
- Password policy is established and a regular password change policy is implemented.
- Encryption is implemented as a result of the risk analysis.

- Copies of data on test environment are either masked or encrypted.

Network infrastructure audit

When performing network infrastructure audit, it is important to check if all of the following precautions are met in order to comply with available security controls (CISA, 2015, pp. 299.):

- Protect passive and active network components in safe rooms, e.g. server rooms.

- Have access control and video surveillance installed on access points and inside server rooms.

- Use MAC address filtering on switch ports.

- Check whether system is configured to do the following: change default passwords of active communication devices on all devices, force personalisation usernames (every user has a unique username), force password policy (remember last five passwords, change password every *n* days, request that passwords contain capital and small letters, numbers, and special characters), request the change of password if it is given to a third person, e.g. a maintainer, request an immediate change of password and/or blocking of user account if person who knew the password left the organisation.

- Use screen lock-out after specified time when there were no interactions in the established session or log-on to system resources (servers, routers).

- Log-on attempts to administrators / supervisor accounts has to be logged.

- Check if all log reports are reviewed at a regular basis.

- Make sure that only authorised access is allowed to computer resources, whether via network or stand-alone devices.

- Check if appropriate risk analysis is performed to determine if encryption is needed for data in transit or data stored on computer media.

- Report when network devices and all computer infrastructure are hardened, so that services and port which are not used are strictly prohibited.

- Implement segregation in networks for critical infrastructure with firewalls.

- Implement intrusion detection systems which are updated to recognise latest cyber and information security threats.

- Have controls to prevent abuse of PBX for tapping, eavesdropping (silent monitoring), traffic control, user tracking, and fraud.

- Document all IP addresses on interfaces.

Information system audit operation audit

When performing an operating system audit, it is necessary to check if all of the following precautions are met in order to comply with the available security controls (CISA, 2015, pp. 300):

- Check if information classification is established.

- Make sure that overall information cyber and information security of the organisation is delegated by a single position such as Chief Information Security Officer (CISO) or by other person on the manager position.

- Implement encryption mechanisms in order to protect personal data.

- Implement segregation of duties. Table 11. Shows the *Segregation of duties matrix* developed by ISACA (ISACA, 2015), where X indicates potential control weakness.

- Have incident management system running.

- Make sure that responsibilities for information security are delegated to all employees.

- Have backup and restore policies in place.

- Implement four-eye principle, so that transaction cannot be done by a single person.

- Have patch management in place.

- Record and monitor all logs at regular intervals to detect potential incident and problems.

- Have appropriate anti-malware policy and provide appropriate anti-virus solution.

- Have mechanisms and procedures to be able to reconstruct events in cyber and information security incident cases.

- Establish change management procedures, so that change activities are performed in line with approved change management procedures.

- Report the restore test to confirm that all data can be recovered and validated by data owner.

- Establish regular practice of performing in-house security tests and independent penetration testing.

- Establish Disaster Recovery Plans (DRP), and Business Continuity Plans (BCP).

- Report that DRP and BCP plans are tested on a regular basis.

- Have an overall cyber and information security awareness education programme.

- Have adequate controls of logical access.

	Control group	Systems analyst	Application programmer	Help Desk and Support Manager	End User	Data Entry	Computer Operator	Database	Network	Systems	Security administrator	System programmer	Quality Assurance
Control group		X	X	X		X	X	X	X	X		X	
Systems analyst	X			X	X		X				X		X
Application programmer	X			X	X	X	X	X	X	X	X	X	X
Help Desk and Support Manager	X	X	X		X	X		X	X	X		X	
End User		X	X	X			X	X	X			X	X
Data Entry	X		X	X			X	X	X	X	X	X	
Computer Operator	X	X	X		X	X		X	X	X	X	X	
Database Administrator	X		X	X	X		X		X	X		X	
Network administrator	X		X	X	X		X	X					
System administrator	X		X	X			X	X				X	
Security administrator		X	X				X					X	
Systems programmer	X		X	X	X		X	X		X	X		X
Quality Assurance		X	X		X							X	

Table 11. Segregation of duties matrix (CISA 2015, pp. 116.)

Scheduling audit

When performing audit of job and personnel scheduling, it is necessary to check if all of the following precautions are met to comply with available security controls (CISA, 2015, pp. 301.):

- Business activities are scheduled.
- All jobs are performed according to the schedule.
- Persons who make changes must be authorized to make changes.
- Existing personnel supports scheduled business activities.
- There is a priority list of critical applications and infrastructure components that has to be recovered with regard to Recovery Time Objective (RTO) and Recovery Point Objective (RPO).

Problem management reporting audit

When performing an operating system audit, it is necessary to check if all of the following precautions are met to comply with available security controls (CISA, 2015, pp. 302.):

- Functionality of a system allows problems to be reported.
- There are responsible persons who monitor problems in the system.
- Mechanisms for resolving submitted reported problems exist.
- There are defined procedures for escalating recognised incidents.

Timeline for cyber security audit

Because order of audits can help in a better organisation of findings and the audit effectiveness, there needs to be a planned time scale for cyber security audit (Figure below).

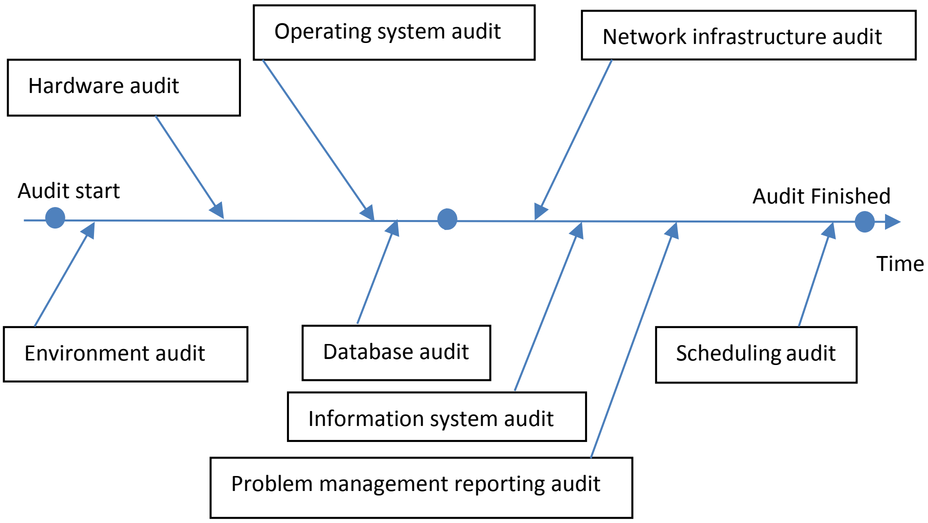


Figure 65. Cyber security timeline audit

Every audit has limited resources, such as time, and auditors' skills.

ISACA CISA (2015) guidelines and BCP / DRP triangle (Rouse M., 2018), which has a specific order in establishing business operations (DRP has to come first before BCP to support business operations) are used for the timeline in Figure above.

First of all, environment and utility issues, followed by infrastructure with hardware, operating systems, networking, and data base audit need to be checked. Afterwards, information system has to be audited for scheduling, problem and incident management, and reporting.

Because of known limitations and possible unknown interruptions and limitations in the audit planning phase, auditors have to determine time windows for each phase. If possible, they should predict the flow of events in the expected timeline.

Duration of audit depends on complexity of organisation that can be couple weeks or couple months.

The cyber security audit timeline can be seen as a workflow which uses a set of audit practices and methods to collect information required to complete the audit process. Each step in the workflow might require looping, branching, and repetition of previous steps.

The Condition, Criteria, Cause, and Effect approach has to be used to make a clear distinction between current or possible conditions and effect/risk using criteria to detect the cause of condition.

Summary

Due to risk of cyber security incidents, it is necessary to perform appropriate management tasks to protect information assets. One important part of safeguarding information assets is to conduct regular audits. Because all current or future business models already are or will be supported by electronic ways of communication and processing, cyber security is a crucial part that has to be supported. As the third line of defence, audit is important for the cyber security assurance. Audit needs to be planed according to available standards, and audit objectives need to be well defined. Before and during auditing, type of audit has to be selected. To minimise human intervention in the process of choosing the object of auditing, it is necessary to conduct risk-based auditing. In practise, there are three types of risk assessment (Qualitative risk-based approach, Semi-quantitative risk-based approach, Quantitative risk-based approach), which are related to organisation maturity and to the risk-based management. Audit process has audit risks which have to be acknowledged during performing audits.

When auditing, it is wise to use already defined controls to minimize risk of not detecting weaknesses. Additionally, it is important to have a common point of reference which can be used by auditors and management or operational representatives of organisation's unit which is the object of auditing. Without a common ground reference and risk assessment based audit, one might think that internal auditors reached particular findings and requested internal controls, without understanding that they are international standard requirements. Common ground or reference point in auditing process is called criteria. Criteria are used to compare auditing process with current process condition in order to detect cause and define possible effects and risks.

Knowledge acquired

In this chapter it is possible to gain knowledge about cyber audit processes.

Review questions

1. What are the three lines of defence model?
2. Explain the third line of defence: Internal audit.
3. Name steps of cyber security audit.
4. What are the types of audits?
5. What is an integrated audit?
6. Explain risk-based auditing and audit risk.
7. Explain risk-based approach?
8. What are audit risk types?
9. How can Condition, Criteria, Cause, and Effect of Internal Auditing help in writing audit reports?

Further readings

- THE THREE LINES OF DEFENSE IN EFFECTIVE RISK MANAGEMENT AND CONTROL https://na.theiia.org/standards-guidance/Public%20Documents/PP%20The%20Three%20Lines%20of%20Defense%20in%20Effective%20Risk%20Management%20and%20Control.pdf

- Governance of risk: Three lines of defence https://www.iia.org.uk/resources/audit-committees/governance-of-risk-three-lines-of-defence/

- What is an Integrated Audit? https://rmas.fad.harvard.edu/faq/what-integrated-audit

- INTEGRATED AUDITING https://www.iia.nl/SiteFiles/IIA_leden/Praktijkgidsen/PG%20Integrated%20Auditing[1].pdf

7. Conclusions

Chapter abstract

Chapter goals: To summarise book goals and review gained knowledge.

Learning outcomes: Gain understanding of cyber security and audit landscape.

Cyber security overview

Cyber security should be the core of every business which relies on digital technologies. This strong dependence is reflected through success of companies which use latest technologies and incorporate them in their everyday business operations and models which represent only one side of business associated with the usage of information systems in the cyber space.

Another side of digital technology is related to cyber incident cases presented in this book – Central Bank of Bangladesh, retail-chain Target, Sony Entertainment Company, Hilary Clinton's presidential campaign, and Webstresser's malicious service.

One way to prevent incidents is to treat cyber security with respect which it deserves. That could be done by implementing applicable industry standards such as IOS 27001, NIST, CobIT, and performing audit by using ISACA guidelines such as CISA (2015).

IIA's three lines of defence model should be used in the internal organisation structure for auditing. The first line of defence model is operational management, second is supported by compliance and risk management, and third line of defence is task of internal audit using IIA, and other applicable standards and guidelines.

Cyber security audit overview

Cyber security audit has to be performed within defined audit objectives and types. Audit has to be based on a risk-based analysis where different types of risk analysis can be used: qualitative, semi-quantitative, and quantitative risk-based analysis. Output of the risk analysis has to be used for implementation of internal controls by using relevant international standards. These controls are used by auditors and compared to standard criteria and practices. In this process, auditors collect the evidence which is information used to support auditor's opinion.

Cyber security audit can be performed using ISACA CISA (2015) guidelines which propose eight areas for auditing: hardware audit, operating system audit, database audit, network infrastructure audit, information system audit, scheduling audit, problem management reporting audit, and environment audit.

Standards from the ISO 27000 (ISO 27001:2013, ISO 27005:2008, and other) family of standards can be used for the implementation of internal controls. They can also be used for documentation for creating checklists and audit implementation of internal controls.

To successfully perform auditing, an auditor should have sound technical knowledge and experience with technological issues which are partially presented in this book.

List of Figures

List of Tables

Acronyms

ACK	Acknowledgement
BCM	Business Continuity Management
BCP	Business Continuity Plan
BS	British standard
BSI	British Standardisation Institute
CERT	Centre for Emergency Report Team
COBIT	Control Objectives for Information and Related Technologies
CISA	Certified Information Security Auditor
CISM	Information Security Manager
CISP	Certified Information Security Professional
CISO	Chief Information Security Officer
CISWG	Corporate Information Security Workgroup
CSO	Chief Security Officer
DMZ	Demilitarised zone
DoS	Denial of Service
DDoS	Distributed Denial of Service

FTP	File Transfer Protocol
HTTP	Hyper Text Transfer Protocol
IA	Internal Auditor
ICMP	Internet Control Message Protocol
IDS	Intrusion Detection System
IP	Internet Protocol
IPPM	IP Performance Management Group
IPS	Intrusion Prevention System
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronic Engineers
IPX	Internetwork Packet Exchange
ISACA	Information Systems Audit and Control Association
ISM	Information Security Manager
ISMS	Information Security Management System
ISO	International Standardisation Organisation
ISSEA	International Systems Security Engineering Association
IT	Information Technology
ITIL	Information Technology Infrastructure Library
KPI	Key Performance Indicator
LAN	Local Area Network

MIB	Management Information Base
NIST	National Institute of Standards & Technology
NMS	Network Management Station
OID	Object identifier
OSI	Open System for Interconnection
PDCA	Plan Do Check Act
QoS	Quality of Service
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
SQL	Simple query language
SPX	Sequenced Packet Exchange
SYN	Synchronize
TCP	Transmission Control Protocol
TNM	Telecommunications Management Network
UDP	User Datagram Protocol
UPS	Uninterruptable Power Supplies
USB	Universal Serial Bus
VPN	Virtual Private Network
WAN	Wide Area Network
XML	Extensible Markup Language

References

Andress J. and Winterfeld S. (Author)Cyber Warfare: Techniques, Tactics and Tools for Security Practitioners, Syngress; 2nd edition (October 1, 2013)

Anttila J., Jusila K., Kajava J., Kmaja I., Integrating ISO / IEC 27001 and other managerial discipline standards with processes of management in organisations, 2012 Seventh International Conference on Availability, Reliability, and Security, pp 425 – 436. IEEE Conference Publications.

Aversano, Lerina; Bodhuin, Thierry; Canfora, Gerardo; Tortorella, Maria, A framework for measuring business processes based on GQM, Proceedings of the 37th Annual Hawaii International Conference on System Sciences, 2004. IEEE Conference Publications.

Aris MashZone (2013) Available from: http://www.mashzone.com/en/mashzone [Accessed on 17.07.2013]

Arkalgud Ramaprasad, "On the Definition of Feedback", Behavioral Science, Volume 28, Issue 1. 1983. Available at: http://onlinelibrary.wiley.com/doi/10.1002/bs.3830280103/pdf [Accessed on 08.02.2018]

Bejtlich R., (2004) The Tao of Network Security Monitoring, Pearson Education Inc. Second printing 2004

Boehemer W., Cost-benefit trade-off analysis of an ISMS based on ISO 27001, 2009 International Conference on Availability, Reliability, and Security, pp 392 – 399, IEEE Conference Publications.

Brotby W. K., Bayuk J., Coleman C.,Leonardo V.,Henning R. R., Katz Stephen R., Malik W., Parulekar Y., Schwartz E., Tester D., Vael M., (2006) Information Security Governance: Guidance for Boards of Directors and Executive Management 2nd Edition, IT Governance Institute, Available from: http://www.isaca.org/Knowledge-Center/Research/Documents/Information-Security-Govenance-for-Board-of-Directors-and-Executive-Management_res_Eng_0510.pdf [Accessed on 25.07.2018]

Brotby W. Krag (2009), Information Security Management Metrics, A definitive Guide to Effective Security Monitoring and Measurement, CRC Press.

Brunner J., 1975, The Shockwave Rider, Harper & Row, 1975

Businesstopia, Avaialble at: https://www.businesstopia.net/communication/shannon-and-weaver-model-communication [Accessed on 19.10.2018]

Cain & Abel (2018), Available from: http://www.oxid.it/cain.html [Accessed on 25.04.2018]

Calder Alan and Watkins Steve, (2007) Information Security Risk Management, IT Governance Publishing 2007

Calder Alan and Watkins Steve, (2006) International IT Governance, An executive Guide to ISO 17799 / 27001, Kogan Page 2006

Calder Alan (2006), implementing Information Security based on ISO 27001 / ISO 17799 – A Management Guide, Van Haren Publishing 2006

CEH 2018, Available at: https://www.eccouncil.org. [Accessed on 25.04.2018]

CERT vulnerability statistics (2008), Available from: http://www.cert.org/stats/vulnerability_remediation.html [Accessed on 25.04.2008]

Charles Joseph Minard, Napoleon's Retreat from Moscow (The Russian Campaign 1812-1813), 1869, Available at: http://www.masswerk.at/minard/, [Accessed on 27.06.2013]

Chartered Institute of Internal Auditors (2014), Risk based internal auditing, Available from: https://global.theiia.org/standards-guidance/topics/documents/201501guidetorbia.pdf [Accessed on 25.07.2018]

Chevallier, V. (1871) Notice necrologique ´ sur M. Minard, inspecteur gen´ eral ´ des ponts et chaussees, ´ en retraite. Annales de Ponts et Chaussees ´, 2(Ser. 5, No. 15):1–22, 1871.

Chew Elizabeth, Clay Alicia, Hash Joan, Bratol Nadya, Brown Anthony, Guide for Developing Performance metrics for Information Security, NIST Special Publication 800-80, 2006

Cimpanu C., 2018, Europol Shuts Down World's Largest DDoS-for-Hire ServiceEuropol Shuts Down World's Largest DDoS-for-Hire Service, Available from: https://www.bleepingcomputer.com/news/security/europol-shuts-down-worlds-largest-ddos-for-hire-service/ [Accessed on: 07.05.2018]

CISA (2015) Review manual 26th Edition, ISACA, 2015, ISBN 978-1-60420-367-7

Cisco (2018), VPN Services, Available from: https://www.cisco.com/c/en/us/products/security/vpn-endpoint-security-clients/what-is-vpn.html, [Accessed on: 07.05.2018]

Cisco Remote Monitoring 2018, Available from: http://docwiki.cisco.com/wiki/Remote_Monitoring [Accessed on: 07.05.2018]

Clinton Email Investigation Timeline, 2018, Available from: http://www.thompsontimeline.com/tag/justin-cooper/ [Accessed on 24.07.2018]

Comey Letter, 2016 Oct. 28 FBI letter to congressional leaders on Clinton email investigation, Available from: https://www.washingtonpost.com/apps/g/page/politics/oct-28-fbi-letter-to-congressional-leaders-on-clinton-email-investigation/2113/ [Accessed on 01.06.2018]

CNN 2016, Available from: https://edition.cnn.com/2016/10/28/politics/hillary-clinton-email-timeline/index.html [Accessed on 31.05.2018]

Cowing J., Ransomware Are You Prepared?, 2018, Available from: http://m.isaca.org/chapters2/san-Francisco/events/Documents/Ransomware%20ISACA%202018-6-28%20V0.1.pdf [Accessed on 24.10.2018]

Deep and Dark Web (2018), Available from: https://www.thedarkwebsites.com/ [Accessed on 07.05.2018]

Donkey (2018) https://www.emule-project.net/home/perl/general.cgi?l=1 [Accessed on 17.07.2018]

Dualcomm, Available from: https://www.dualcomm.com/product-page/dual-gbe-copper-and-fiber-network-tap [Accessed on 07.06.2018]

Eisenberg T., Gries D., Hartmanis J., Holcomb D., Stuart L. M., Thomas Sant oro The Cornell Commission:On Morris and the Worm,]une 1989 Volume 32 Number 6

English Oxford Dictionaries, 2018 Available from: https://en.oxforddictionaries.com/definition/fraud [Accessed on 24.07.2018]

Ethernet, 2018, Available from: https://www.electronics-notes.com/articles/connectivity/ethernet-ieee-802-3/cables-types-pinout-cat-5-5e-6.php [Accessed on 12.07.2018]

Ethernet IEEE 802.3 Standards, 2018 Available from: https://www.electronics-notes.com/articles/connectivity/ethernet-ieee-802-3/standards.php [Accessed on 12.07.2018]

eTOM, 2018, Available from: https://www.tmforum.org/business-process-framework/ [Accessed on 12.10.2018]

Everest D., Garber R. E., Keating M., Peterson B., 2008, Business Continuity Management, Global Technology Audit Guide (GTAG) https://chapters.theiia.org/montreal/ChapterDocuments/GTAG%2010%20-%20Business%20Continuity%20Management.pdf

Eyerys, Authorities Shut Down One of the World's Largest DDoS-For-Hire Service, Available from: https://www.eyerys.com/articles/timeline/authorities-shut-down-one-worlds-largest-ddos-hire-service?page=4#event-a-href-articles-timeline-one-fifth-all-enterprise-applications-were-born-cloudone-fifth-of-all-enterprise-applications-were-born-in-the-cloud-a, [Accessed on 25.04.2018]

Featherly K., ARPANET UNITED STATES DEFENSE PROGRAM, Available from: https://www.britannica.com/topic/ARPANET, [Accessed on 25.04.2018]

FOX NEWS, 2016, Available from: http://www.foxnews.com/politics/2016/09/02/timeline-clinton-email-server-setup.html

Gibson W., Neuromancer, Ace; 1st edition (July 1, 1984)

Gourley Bob (2014) The Cyber Threat: Know the threat to beat the threat, Sep 3, Amazon Digital Services LLC

Gregory H.Peter (2016) CISA Certified Information Systems Auditor All-in-One Exam Guide, Third Edition, McGraw-Hill Education; 3 edition (October 26, 2016)

Hajdarevic K., Allen P., A New Method for the Identification of Proactive Information Security Management System Metrics, MIPRO 35 Proceedings of the 35th International Convention, Publication Year: 2013, IEEE Conference Publications.

Hajdarevic K., Kozaric K., Hadzigrahic J., Architecture and Infrastructure for Governing Information Security in Central Banks, Journal of Central Banking Theory and Practice, Volume 1, Number 2, pp. 5-17, October 2012.

Hajdarevic K., Pattinson C., Kozaric K., Hadzic A., Information Security Measurement Infrastructure for KPI Visualization, MIPRO 35 Proceedings of the 35th International Convention, Publication Year: 2012, Page(s): 1543 – 1548, IEEE Conference Publications.

Henckler Aron, Waterfall Charts using Excel, Available at: http://chandoo.org/wp/2009/08/10/excel-waterfall-charts/
[Accessed on 24.11.2012]

History of the Web, World Wide Web Foundation, Available at: https://webfoundation.org/about/vision/history-of-the-web/
[Accessed on 12.06.2018]

IIA Position Paper: THE THREE LINES OF DEFENSE IN EFFECTIVE RISK MANAGEMENT AND CONTROL, JANUARY 2013, Available at: https://na.theiia.org/standards-guidance/Public%20Documents/PP%20The%20Three%20Lines%2

0of%20Defense%20in%20Effective%20Risk%20Management%20and%20Control.pdf [Accessed on 23.02.2018]

InetDaemon, Available at: https://www.inetdaemon.com/tutorials/basic_concepts/communication/frames_packets_n_pdus.shtml [Accessed on 23.09.2018]

Ademu I. O., Imafidon C. O., Preston D. S., A New Approach of Digital Forensic Model for Digital Forensic Investigation, (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 2, No.12, 2011

Iasiello E., Cyber Attack: A Dull Tool to Shape Foreign Policy, Available at: https://ccdcoe.org/cycon/2013/proceedings/d3r1s3_Iasiello.pdf [Accessed on 23.09.2018]

Internet Protocol Version 6 (IPv6) / IP Next Generation (IPng), Available at: http://tcpipguide.com/free/t_InternetProtocolVersion6IPv6IPNextGenerationIPng.htm [Accessed on 23.02.2018]

IPPM, 2018, Available at: https://datatracker.ietf.org/wg/ippm/documents/ [Accessed on 12.07.2018]

ISACA (2008) in Information Security Governance: Guidance for Information Security Managers

ISACA (2012) COBIT 5, Available at: https://www.isaca.org/COBIT/Documents/COBIT5-Introduction.ppt [Accessed on 20.07.2018]

ISO 27001:2013 Information technology – Security techniques – information Cecurity Managamanet System – Requirements, Second edition 2013-10-01, ISO IEC

ISO 27005 ISO 27005:2008 Information technology – Security techniques – information security management, first edition 2008-06-15, ISO IEC

ISO 7498:1984, Information processing systems – Open Systems Interconnection – Basic Reference Model, Available at: https://www.iso.org/standard/14252.html [Accessed on 20.07.2018]

LoBianco T., 2016, FBI releases notes from Clinton email investigation, September 24, 2016https://edition.cnn.com/2016/09/23/politics/fbi-investigation-hillary-clinton-emails/index.html

Jaquith Andrew, Security Metrics, Replacing Fear, Uncertainty, and Doubt. Addison-Wesley, 2009 [Accessed on 23.07.2018]

John the Ripper (2018) Available at: http://www.openwall.com/john/ [Accessed on 08.05.2008]

Kalvapalle R, 2016 Available at: https://globalnews.ca/news/3035703/hillary-clinton-email-scandal-timeline/ [Accessed on 08.05.2008]

Kismet (2018), Available from: https://www.kismetwireless.net/ [Accessed on 08.05.2008]

KPMG, Value For Money, Available from: https://home.kpmg.com/sg/en/home/services/advisory/risk-consulting/internal-audit-services/value-for-money.html, [Accessed on 08.10.2018]

Krishna N. Das, Ruma Paul, Exclusive: Bangladesh probes 2013 hack for links to central bank heist, Available at: https://www.reuters.com/article/us-cyber-heist-bangladesh/exclusive-bangladesh-probes-2013-hack-for-links-to-central-bank-heist-idUSKCN0YG2UT [Accessed on 08.05.2018]

Krishna N. Das, and Jonathan Spicer, 2016, How millions from the Bangladesh Bank heist disappeared, Available at: https://www.reuters.com/article/us-cyber-heist-philippines/how-millions-from-the-bangladesh-bank-heist-disappeared-idUSKCN1011AT [Accessed on 08.05.2018]

LaFraniere S., Californian Who Unwittingly Aided Russian Election Interference Gets 6 Months in Prison, Avaialble at: https://www.nytimes.com/2018/10/10/us/politics/richard-pinedo-sentencing-mueller.html?rref=collection%2Fnewseventcollection%2Frussian-election-hacking&action=click&contentCollection=politics&region=stream&module=stream_unit&version=latest&contentPlacement=9&pgtype=collection [Accessed on Oct. 10, 2018]

Lee T. B. 2013, Everything you need to know about the NSA and Tor in one FAQ, Available at: https://www.washingtonpost.com/news/the-switch/wp/2013/10/04/everything-you-need-to-know-about-the-nsa-and-tor-in-one-faq/?noredirect=on&utm_term=.815bf3f47636, October 4, 2013, [Accessed on 08.07.2018]

Lord N., 2018, A History of Ransomware Attacks: The Biggest and Worst Ransomware Attacks of All Time, April 6, 2018, Available at: https://digitalguardian.com/blog/history-ransomware-attacks-biggest-and-worst-ransomware-attacks-all-time [Accessed on 24.07.2018]

Mason B. (2017), The Underappreciated Man Behind the "Best Graphic Ever Produced," Available at: https://news.nationalgeographic.com/2017/03/charles-minard-cartography-infographics-history/ [Accessed on 12.06.2018]

Maswerk, (2013), Available at: http://www.masswerk.at/minard/ [Accessed on 10.06.2018]

Mar S., Johannessen R., Coates S., Wegrzynowicz K., Andreesen T., Global Technology Audit Guide (GTAG®) Information Technology Risk and Controls, IPPF – Practice Guide, March 2012 Available: at: https://chapters.theiia.org/montreal/ChapterDocuments/GTAG%201%20-%20Information%20technology%20controls_2nd%20ed.pdf [Accessed on 16.06.2018]

Mitchell B. 2018, Gnutella P2P Free File Sharing and Download Network, Updated February 06, 2018 https://www.lifewire.com/definition-of-gnutella-818024 [Accessed on: 22. 07. 2018]

Mission Assurance, 05.04.2000 Available at: http://www.hq.nasa.gov/office/codeq/pra.pdf [Accessed on 23.07.2013]

Mueller P. and Yadegari B., The Stuxnet Worm, Available from: https://www2.cs.arizona.edu/~collberg/Teaching/466-566/2012/Resources/presentations/2012/topic9-final/report.pdf [Accessed on: 12. 06. 2018]

Napster, (2018) Available at: https://www.reddit.com/r/nostalgia/comments/1v98nm/downloading_songs_on_napster_with_a_56k_modem/ [Accessed on 23.05.2018]

Nimonik (2018) Available at: https://nimonik.com/help/associate-a-company-or-public-template-to-a-facility/ [Accessed on 23.05.2018]

Norman J, 2018, Norbert Wiener Issues "Cybernetics," the First Widely Distributed Book on Electronic Computing http://www.historyofinformation.com/expanded.php?id=850 [Accessed on 12.06.2018]

Nmap/Zenmap (2018), Available: at: https://nmap.org/zenmap/ [Accessed on 12.07.2018]

Nuangjamnong C., Maj S. P., Veal D., The OSI Network Management Model- Capacity and Performance Management, Proceedings of 4th IEEE International Conference on Management of Innovation and Technology . ICMIT 2008. (pp. 1266-1270). Bangkok, Thailand. IEEE

Overview of TMN Recommendations, Telecommunications management network M.3000–M.3599 (02/2000), ITU 2001. Available at: https://www.itu.int/rec/T-REC-M.3000-200002-I/en [Accessed on 23.05.2018]

Probst W. C., Hunker J., Bishop M., Gollmann D. Insider Threats in Cyber Security (Advances in Information Security), Springer; 2010 edition (August 10, 2010)

Passive and active attacks, SECURITY CONCEPTS FOR CORPORATE NETWORKS, Available from: http://www.tc11.uni-frankfurt.de/CONF/SEC94/roppl.html [Accessed on 08.05.2008]

Paul, December 28, 2014 20:39 New Clues in Sony Hack Point To Insiders, Away from DPRK, Available from: https://securityledger.com/2014/12/new-clues-in-sony-hack-point-to-insiders-away-from-dprk/, [Accessed on: Friday, March 9, 2018]

Pelkey J., (2007) Transmission Control Protocol (TCP) 1973-1976, Available from: http://www.historyofcomputercommunications.info/Book/6/6.4-TransmissionControlProtocol(TCP)73-76.html, [Accessed on: 18.06.2018]

Pelkey J., (2007) Chapter 9 Standards: 1979-1984, ISO/OSI (Open Systems Interconnection): 1979 - 1980, Available from: http://www.historyofcomputercommunications.info/Book/9/9.5_I

SO-OSI-OpenSystemsInterconnection-79-80.html, [Accessed on: 12.06. 2018]

Reuters (2016), UPDATE 3-Bangladesh central bank governor resigns over cyber heist, Available from: https://www.reuters.com/article/usa-fed-bangladesh-resignation/update-3-bangladesh-central-bank-governor-resigns-over-cyber-heist-idUSL3N16N3MB, [Accessed on: 12.06. 2018]

Rouse M., Available from: https://searchdisasterrecovery.techtarget.com/definition/business-continuity [Accessed on: 12.06. 2018]

Ruma P., (2018), Bangladesh to sue Manila bank over $81-million heist, Available from: https://www.reuters.com/article/us-cyber-heist-bangladesh/bangladesh-to-sue-manila-bank-over-81-million-heist-idUSKBN1FR1QV, [Accessed on: 12.06. 2018]

Sahin T., x Omidyar 1988, ;Bauman T.M., 1988, Telecommunications management network (TMN) architecture and interworking designs, May 1988, Page(s): 685 - 696, IEEE Journal on Selected Areas in Communications (Volume: 6, Issue: 4, May 1988)

SamSpade, Available at: http://www.majorgeeks.com/files/details/sam_spade.html [Accessed on 23.05.2018]

Sandwith L. 2006 Does Internal Audit have an effective game plan to address fraud? Available at: https://www.iia.org.uk/media/1688757/1-internal-audit-game-plan-l-sandwith-.pdf [Accessed on 23.10.2018]

Scott E., 2015, Hillary Clinton on emails: “The facts are pretty clear,” Available at:

https://edition.cnn.com/2015/07/25/politics/clinton-confident-never-sent-classified-emails/index.html, [Accessed on 23.05.2018]

Shaban Hamza, Global police just shut down world's largest marketplace that allegedly disrupted millions of sites, Available from: https://www.washingtonpost.com/news/the-switch/wp/2018/04/25/global-police-just-shut-down-worlds-largest-marketplace-that-allegedly-disrupted-millions-of-sites/?noredirect=on&utm_term=.924b110f7630 [Accessed on: Monday, April 9, 2018]

Shannon, C.E., & Weaver, W. (1949). The mathematical theory of communication. Urbana: University of Illinois Press.

Silver N., The Comey Letter Probably Cost Clinton The Election, Available from: https://fivethirtyeight.com/features/the-comey-letter-probably-cost-clinton-the-election/ [Accessed on: April 5, 2018]

Spremić, M, Sigurnost i revizija informacijskih sustava u okruženju digitalne ekonomije, Mario Spremić, 2017, ISBN: 978-953-346-037-6

Stuxnet, Symantec, July 13, 2010, Available from: https://www.symantec.com/security-center/writeup/2010-071400-3123-99 [Accessed on: 18. 07. 2018]

Stamatelatos Michael, Probabilistic Risk Assessment: What Is It and Why Is It Worth Performing It, NASA Office of Safety and

Stoneburner Gary, Goguen Alice, and Feringa, Risk Management Guide for Information Technology Systems, NIST, 2002 Available at: http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf [Accessed on 24.11.2012]

Syed Aakhtar and Syed Aafsar, Business Continuity Planning Methodology, Sentryx, 2004

TCP/IP Internet Protocol, 1981, Available from: https://www.livinginternet.com/i/ii_tcpip.htm, [Accessed on: 18. 06. 2018]

Techopedia (2018), Information Systems Security (INFOSEC), 2018, Techopedia, Available from: https://www.techopedia.com/definition/24840/information-systems-security-infosec, [Accessed on: 12. 06. 2018]

The Smoking Gun, 2013, Available at: http://www.thesmokinggun.com/buster/sidney-blumenthal/hacker-distributes-memos-784091 [Accessed on 23.05.2018]

Thomson I., 2016, Meet the malware that screwed a Bangladeshi bank out of $81m, Available at: https://www.theregister.co.uk/2016/04/25/bangladeshi_malware_screwed_swift/ [Accessed on 02.05.2018]

Toigo Jon William, Disaster Recovery Planning Preparing for the Unthinkable, Prentice Hall PTR 2003.

TOR (2018) Available at: https://www.torproject.org/about/overview, [Accessed on 23.05.2018]

Vasudaven Vinod, Anoop Mangla, Application Security in the ISO 27001 Environment, IT Governance LTD 2008

Vacca R. J., (2013) Cyber Security and IT Infrastructure Protection 1st Edition, Syngress; 1 edition (August 22, 2013)

Vigila M., Buchmann J., Cabarcasb D., Weinerta C., Wiesmaierc A., Integrity, authenticity, non-repudiation, and proof of existence for long-term archiving: A survey, Computers & Security Volume 50, May 2015, Pages 16-32, Elsevier

Vijayan Jaikumar, (2014), Available at: https://www.computerworld.com/article/2487425/cybercrime-hacking/target-breach-happened-because-of-a-basic-network-segmentation-error.html [Accessed on 23.04.2018]

Von Neumann, J., Burks, Arthur W., Theory of self-reproducing automata, Urbana, University of Illinois Press, 1966

Watkins W. (2014), Condition, Criteria, Cause and Effect of Internal Auditing, Available at: https://www.iiafiji.org/resources/bbc5020b-a5ab-4388-b633-83813515c797.pdf [Accessed on 24.04.2018]

Wireshark (2018) Available at: https://www.wireshark.org/, [Accessed on 01.07.2018]

Wikipedia (2018) Timeline of computer viruses and worms, Available at: https://en.wikipedia.org/wiki/Timeline_of_computer_viruses_and_worms [Accessed on 01.07.2018]

Wong Caroline, Security Metrics: A Beginner's Guide, McGraw Hill, 2012

(x.200. 1995), Data Networks and Open System Communications, Open Systems Interconnection - Model and Notation, International Telecommunication Union

Yixi, Guo; Hui, Guan, Research on Method of Metrics for Information Ferry in Secret Intranet, International Conference on Intelligent Computation Technology and Automation (ICICTA), 2011

ZAP 2018, Available at: https://www.owasp.org/index.php/File:ZAP-ScreenShotHistoryFilter.png [Accessed on 23.05.2018]

Zurcher A., (2016). “Hillary Clinton emails - what's it all about?,” Available at: https://www.bbc.com/news/world-us-canada-31806907 [Accessed on 12.06.2018]

Overview of Digital Forensics, Available at: https://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/overview-of-digital-forensics.aspx, [Accessed on 12.06.2018]

Index

About author

Kemal Hajdarevic PhD received B.Sc. from Faculty of Electrical Engineering, University of Sarajevo, Bosnia and Herzegovina, M.Sc. and PhD from Leeds Metropolitan University / Leeds Beckett University, Leeds, UK. He is currently working at the Central Bank of Bosnia and Herzegovina as a Senior Internal Auditor for information Security and IT projects, and he has a teaching position at the Faculty of Electrical Engineering, University of Sarajevo, and International Burch University, Sarajevo, Bosnia and Herzegovina. He teaches Computer Communication and Networks, Network Management, IT Governance, Computer Modelling and Simulations, Ethical Hacking, and Digital Forensics. He is a licensed radio amateur with call sign E71HK.

Colin Pattinson: *"As business organisations of all types and sizes place greater dependence on their information technology to provide their core operational requirements, it is sadly inevitable that there is a growth in the number of malicious individuals attempting to exploit that dependency, whether by unauthorised access to resources, theft of data or by making the systems unusable for their required purpose. Defence against attacks like these, and the many other ways in which systems or information can be compromised, is invaluable, but needs careful planning combined with the tools, knowledge and techniques to carry out those plans.*

This book explains how those plans should be developed and provides the means by which they can be carried out. It begins from the fundamental basis that knowledge about how any system is configured and how it is behaving are fundamental to the ability to control and manage. The second significant requirement for defence is to know what an opponent is capable of. Identifying which of the potential threats might be realised then leads to an audit of the system to determine the real threats and any gaps in defences. This book covers each of those stages in a logical and thorough manner. After an explanation of the range and types of network and communications technologies likely to be encountered, the book then discusses the potential threats, supported by informative actual cases to show that these are not simply abstract concepts, but that real organisations have suffered real losses though security breaches. The book then provides the reader with the necessary tools and techniques to assess and manage the risks, ending with a comprehensive discussion of the design and conduct of a full cyber security audit, addressing all levels of a typical business IT system. Structured tutorial / revision questions support each chapter, allowing the reader to reinforce their learning at each stage, before moving on to the next chapter. Alternative pathways through the book are identified to allow readers to develop their particular specialist interest.

This book meets a demand which is certain to increase in importance in the years to come.

Mario Spremic: *"As there are not so many quality publications in this area, especially the books like this one with holistic (technology, management, regulation, etc.) approach to cyber security and information system auditing, I do recommend this book for students, researchers and practitioners to gain fundamental knowledge and understanding and broaden their horizons."*

ISBN 9789958834646
9 789958 834646