Abdullah-cybersec

by Student User

Submission date: 25-Mar-2021 05:34PM (UTC+0000)
Submission ID: 147965938
File name: Abdullah-cybersec_6951_1522723317.docx (801.95K)
Word count: 5211
Character count: 29920

Task 1A

An analysis of current cyber security risks to organisations

Cybersecurity includes technologies, processes and procedures designed to protect networks, computers, programs and data against attacks, damage or unauthorized access. In an IT context, security includes both cybersecurity and physical security. One of the most problematic elements of information security is the rapid and constant change in security risks. The traditional approach has been to focus most of the resources on the key components of the system and protect them from the key threats that required the need to leave behind some of the less important unprotected system components and some less dangerous unprotected ones.

Threats can turn potential vulnerabilities into attacks on computer systems, networks and more. They can endanger computer systems and individual computers. Therefore, security holes must be corrected so that attackers cannot penetrate the system and causes damage.

Threats include viruses, Trojans, backdoors and hacker attacks. Often, the term "mixed threat" is more precise, since more threats means more attacks. For example, an attacker could use a phishing attack to obtain information through a network and enter a network. (Zamora and Zamora, 2018)

Some recent cyber-attacks were:

Shadow Brokers

The mysterious hacking group known as the Shadow Brokers first surfaced in August 2016, claiming to have breached the spy tools of the elite NSA-linked operation known as the Equation Group. The Shadow Brokers offered a sample of alleged stolen NSA data and attempted to auction off a bigger trove, following up with leaks for Halloween and Black Friday in 2016.

This April, though, marked the group's most impactful release yet. It included a trove of particularly significant alleged NSA tools, including a Windows exploit known as EternalBlue, which hackers have since used to infect targets in two high-profile ransomware attacks.

The identity of the Shadow Brokers is still unknown, but the group's leaks have revived debates about the danger of using bugs in commercial products for intelligence-gathering. Agencies keep these flaws to themselves, instead of notifying the company that makes the software so the vendor can patch the vulnerabilities and protect its customers. If these tools get out, they potentially endanger billions of software users.(Newman and Keats, 2018)

WannaCry

A ransomware called wannacry was spread around the world on May 12 of 2017 targeting hundreds of thousands of people including large corporations.

Though powerful, the ransomware also had significant flaws, including a mechanism that security experts effectively used as a kill switch to render the malware inert and stem its spread. US officials later concluded with "moderate confidence" that the ransomware was a North Korean government project gone awry that had been intended to raise revenue while wreaking havoc. In total, WannaCry netted almost 52 bitcoins, or about $130,000—not much for such viral ransomware.

WannaCry's reach came in part thanks to one of the leaked Shadow Brokers Windows vulnerabilities, EternalBlue. Microsoft had released the MS17-010 patch for the bug in March, but many institutions hadn't applied it and were therefore vulnerable to WannaCry infection.(Newman and Keats, 2018)

Petya/NotPetya/Nyetya/Goldeneye

In April of 2017 months after wannaCry, another wave of ransomware infections that partially leveraged Shadow Brokers Windows exploits hit targets worldwide. This

malware, called Petya, NotPetya and a few other names, was more advanced than WannaCry in many ways, but still had some flaws, like an ineffective and inefficient payment system.

Though it infected networks in multiple countries—like the US pharmaceutical company Merck, Danish shipping company Maersk, and Russian oil giant Rosnoft—researchers suspect that the ransomware actually masked a targeted cyberattack against Ukraine. The ransomware hit Ukrainian infrastructure particularly hard, disrupting utilities like power companies, airports, public transit, and the central bank, just the latest in a series of cyber assaults against the country. (Newman and Keats, 2018)

Task 1B

An evaluation of the different controls that can be used to manage cyber security risks

E crops is cyber security firm which has several divisions into different areas such as real estate, banking and transportation, but the parent company's focus has always been cyber security. It is a very large scale organization and has thousands of branches both international and domestic. So a large scale organization like E corp need to protect their assets like their database and other various cyber features. Their networks and websites are crucial to ensure it is not susceptible to cyber-attacks. The Scheme highlights eight basic controls to put into place:

1. Boundary firewalls and internet gateways

Boundary firewalls, internet gateways or comparable network mechanisms should be in place to protect systems, applications, information and devices against unauthorised access and exposure to the internet. Without these, systems are at risk of being easily accessed, leaving information exposed and at risk of deletion. A boundary firewall acts as a defence by regulating inbound and outbound network traffic, blocking those common cyber threats that are created easily from widely and freely available tools on the internet.

The Scheme also recommends that:

- the password to the firewall should be strong and not the default option;
- an authorised individual should approve each rule that allows network traffic to pass through the firewall, which should be documented;
- routinely susceptible services and unapproved services should be locked at the boundary by default;
- the firewall should be kept up to date so that out of date rules are deleted; and
- it should not be possible to access the dashboard to manage the firewalls from the internet.

2. Secure configuration

Devices connected to a network must be configured to ensure that they can only provide the services required and are not given access to surplus networks or systems. This will help to reduce characteristic vulnerabilities of some devices. The default settings and applications on many devices can serve as a route for cyber attackers to gain easy access to the information on these network devices. The Scheme suggests that when installing network devices, some basic controls should be employed such as:

- user accounts that are not needed should be deleted;
- passwords should be changed from default at installation and must be strong;
- redundant software should be removed or disabled;
- software settings such as auto-run should be disabled to prevent software being active when accessing network folders and where removable storage is used; and
- a personal firewall should be enabled on computers and set to block unapproved connections by default - this may often be installed on a computer as part of an operating system.

Passwords

Passwords act as a first line of defence and should, therefore, be made as strong as possible. It is recommended to include:

- three or more words;
- symbols;
- upper and lower cases; and
- numbers.

It is also wise to avoid using common passwords; it is sometimes possible for cyber hackers to guess passwords from information displayed publically on social media accounts and other areas of public information and as a result it is recommended to avoid using:

- date of birth;
- name, family member's name or current partner's name;
- favourite holiday;
- significant dates;
- place of birth; and
- number sequences.

Compromised passwords can lead to vast amounts of information being easily accessed by cyber attackers. A concise policy on passwords setting out some top tips will help to communicate the importance of strong passwords to employees.

3. Access control

User accounts should allow for the minimum level of access required for applications, devices and networks. Users requiring special privileges to manage controls must be authorised individuals. To help control access, the Scheme suggests:

- inception of each user account must be approved in a formalised process;

- users with special privileges should be limited and details about those with special privileges should be documented and kept in a secure location;
- any administrative accounts should serve only that administrative purpose for which they are created;
- usernames and passwords should be unique and strong with passwords for access to devices, applications, email or the internet. Passwords should be changed regularly at least every 60 days; and
- when user accounts are no longer required or are inactive for a pre-defined period (e.g. three months), they should be removed or disabled, especially when special privileges are granted to user accounts.

4. Malware protection

Where computers are connected to the internet, malware protection software should be installed to protect against malicious software such as viruses, worms and spyware that serve to perform unauthorised functions on computers. Malware protection software can protect against malware which can be easily transmitted by a number of means including emails, websites or files on storage media. This may seem an obvious protection but it will help ensure greater protection from potential cyber-attacks. The protection software should be kept up to date and configured to automatically scan files once accessed and perform regular general scans. It should also be set up to block access to malicious websites.

The Scheme recommends that as well as the more established use of malware protection for desktop PCs, laptops and servers, devices such as tablets and smartphones are also likely to need malware protection.

5. Patch management

Devices like computers or other devices connected to a network are at risk of being exposed to weaknesses contained in software that such devices run. Once these flaws are exposed, which is often on a daily basis, they can quickly be exploited for misuse. Software producers will monitor flaws and release software updates known as patches. An organisation should formalise the patch management process so

that updates can be monitored effectively and installed efficiently, forming a strategy detailing the type of patches that should be applied to each software/system and at what time. Updates to software should be installed promptly; the Scheme suggests doing so as soon as updates are available or, at the latest, within 30 days of release. For security patches the recommended implementation time is immediately or within 14 days of release. In addition, any software used should be licenced and supported by the supplier or vendor of the software to ensure that the relevant security patches are provided. Software that is no longer supported should be removed from those network connected devices.
It is important to note that if an organisation has chosen not to implement a certain control as set out by the Scheme, due to reasonable business grounds that mean it is not practical or possible to install, alternative controls should be put in place and this should be detailed.
As well as providing guidelines on measures that organisations should take, the Scheme also offers a mechanism, through the Assurance Framework, for certification for organisations either of 'Cyber Essentials' or 'Cyber Essentials Plus'.

6. Encryption

In cryptography, encryption is the process of encoding a message or information in such a way that only authorized parties can access it and those who are not authorized cannot. Encryption does not itself prevent interference, but denies the intelligible content to a would-be interceptor. In an encryption scheme, the intended information or message, referred to as plaintext, is encrypted using an encryption algorithm – a cipher – generating ciphertext that can only be read if decrypted. For technical reasons, an encryption scheme usually uses a pseudo-random encryption key generated by an algorithm. It is in principle possible to decrypt the message without possessing the key, but, for a well-designed encryption scheme, considerable computational resources and skills are required. An authorized recipient can easily decrypt the message with the key provided by the originator to recipients but not to unauthorized users.

7. Antivirus

Antivirus software was made with the intention of finding and removing viruses and most kind of malware's which could harm the system. Antivirus these days can protect from mostly anything, like: malicious browser helper objects (BHOs), browser hijackers, ransomware, keyloggers, backdoors, rootkits, trojan horses, worms, malicious LSPs, dialers, fraudtools, adware and spyware. And some spefic can also protect from big computer threats, such as infected and malicious URLs, spam, scam and phishing attacks, online identity (privacy), online banking attacks, social engineering techniques, advanced persistent threat (APT) and botnet DDoS attacks.

8.Intrusion detection system

An intrusion detection system (IDS) is a device or software application that monitors a network or systems for malicious activity or policy violations. Any detected activity or violation is typically reported either to an administrator or collected centrally using a security information and event management (SIEM) system. A SIEM system combines outputs from multiple sources, and uses alarm filtering techniques to distinguish malicious activity from false alarms

9.Vulnerability scanning

Vulnerability scanning is an inspection of the potential points of exploit on a computer or network to identify security holes. A vulnerability scan detects and classifies system weaknesses in computers, networks and communications equipment and predicts the effectiveness of countermeasures.

Task 2A

A critical assessment of the vulnerabilities of the computer network security of your chosen organisation

Vulnerability is a cyber-security term that refers to a flaw in a system that can leave it open to attack. A vulnerability may also refer to any type of weakness in a computer system itself, in a set of procedures, or in anything that leaves information security exposed to a threat.

There are multiple factors contribute to these security problems and pose obstacles to the security solutions.
Among the most frequently mentioned sources of security vulnerability problems in computer networks are

- design flaws
- security management
- Internet technology vulnerability

Design flaws

The two major components of a computer system, hardware and software, quite often have design flaws. Hardware systems are less susceptible to design flaws than their software counterparts owing to less complexity, which makes them easier to test; limited number of possible inputs and expected outcomes, again making it easy to test and verify; and the long history of hardware engineering.

Despite all the factors backing up the hardware engineering, due to the complex design of the system, design flaws would still be occurred multiple times. The biggest issue derives from system security vulnerability and this is because of software design flaws. The software design flaws are caused by factors such as security issues. Although, the three main reasons are human factors, software complexity, and trustworthy software sources.

Poor security management

Poor security management is caused by having less control in the security department such as the security implementation, administration, and monitoring. It results in a failure when due to not having solid control over the security in the organization. When The security administrator is unaware about the security policies and who sets them along with who manages the system and incidents are then caused. Good security have various factors like risk management, information security policies and procedures, standards, guidelines, information classification, security monitoring, and security education. These are used to provide security over the company. *(Iso.org. 2017)*

Internet Technology Vulnerability

Internet technology has been vulnerable and they are present in both the hardware and software. The reports suggest problems such as of loopholes, weaknesses, and gaping holes

Vulnerability analysis, also known as vulnerability assessment, is a stage that helps in identifying and classifying security holes(vulnerabilities) in a network, computer or a communication infrastructure. Furthermore, vulnerability analysis can be used to predict the effectiveness of the countermeasures and evaluate the actual effectiveness when they are used in the system. *(Newman, L. and Keats, J.2018)*

Vulnerability Testing - checklist:

- Verify the strength of the password as it provides some degree of security.
- Verify the access controls with the Operating systems/technology adopted.
- Verifies how easily the system can be taken over by online attackers.
- Evaluates the safety level of the data of system.
- Checks if the system configuration or application configuration files are protected.

- Checks if the system allows user to execute malicious script.

Vulnerability Testing - Methods:

- Active and Passive testing
- Network and distributed testing
- Verifying File/system access

The Test tools I used for testing these methods were:
All of these tools were available in kali Linux

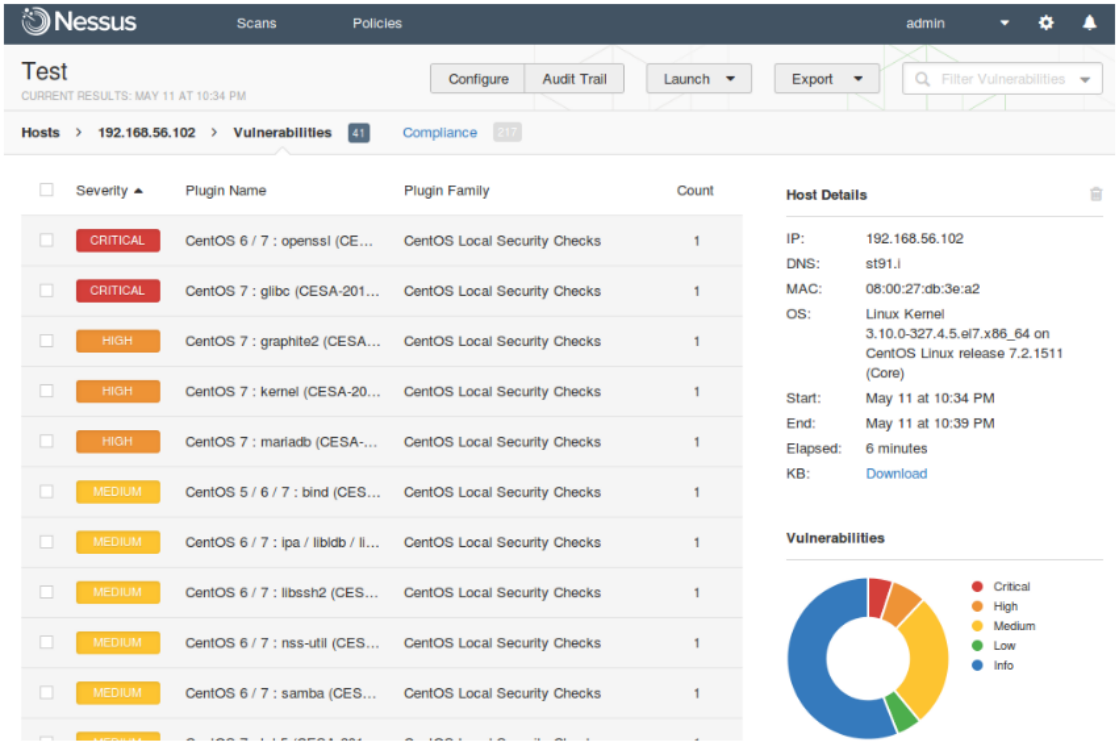
- Zenmap
- Nmap
- Hydra
- Whitewindows
- SET

Test results

Kali Linux- Kali Linux is a Debian-based Linux distribution aimed at advanced Penetration Testing and Security Auditing. Kali contains several hundred tools which are geared towards various information security tasks, such as Penetration Testing, Security research, Computer Forensics and Reverse Engineering. Kali Linux is developed, funded and maintained by Offensive Security, a leading information security training company. I have used many tools in kali linux to find any vulnerabilities that might be within the system and network. *(Newman, L. and Keats, J.2018)*

1

Zenmap-Zenmap is the official Nmap Security Scanner GUI. It is a multi-platform (Linux, Windows, Mac OS X, BSD, etc.) free and open source application which aims to make Nmap easy for beginners to use while providing advanced features for experienced Nmap users.

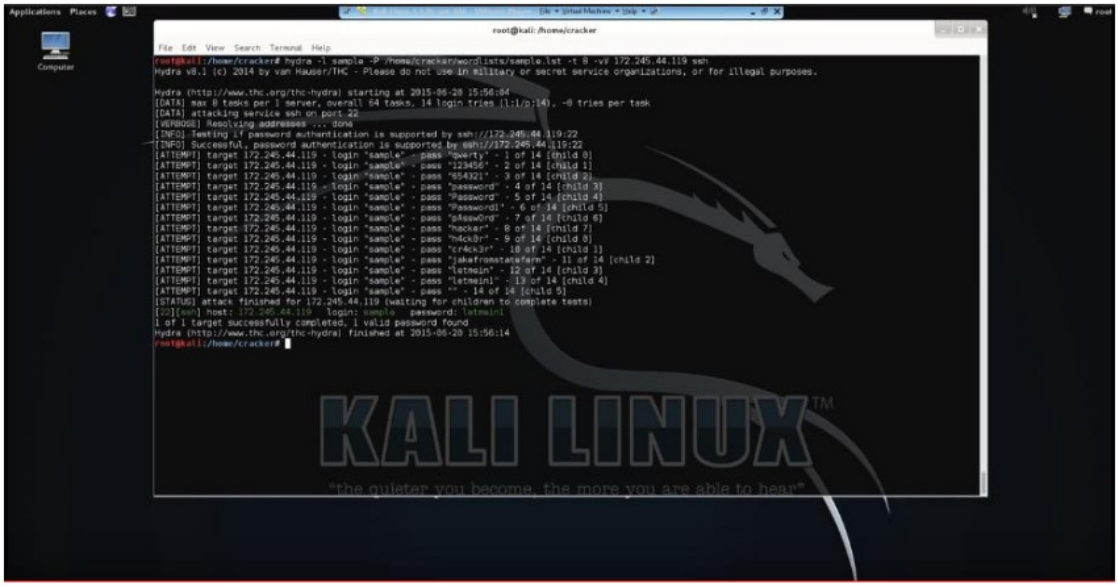


It showed that results are unreliable as they range from critical to a medium threat. I have used the Linux version.

Nmap-Nmap ("Network Mapper") is a free and open source (license) utility for network discovery and security auditing. Many systems and network administrators also find it useful for tasks such as network inventory, managing service upgrade schedules, and monitoring host or service uptime.

It showed they were Vulnerableas 4 ports were open which attacks can use a backdoor and can attain sensitive information.

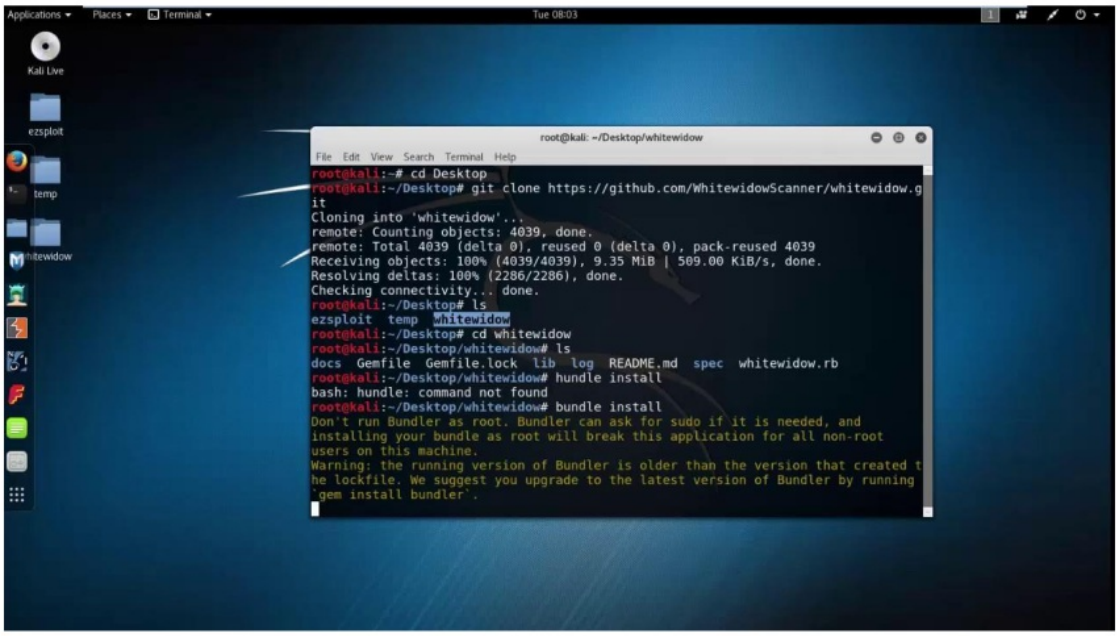
Hydra-THC Hydra – Brute force various protocols and services . When you need to brute force crack a remote authentication service, Hydra is often the tool of choice. It can perform rapid dictionary attacks against more than 50 protocols and services including telnet, ftp, http, https, smb, several databases, and much more.



The brute force attack was successful as it managed to capture the password of the indented target within company, exposing another flaw within the system.

Whitewindows-Whitewindows is an open source Python tool designed to audit for as well as automate injection attacks and exploit default configuration weaknesses in NoSQL databases and web applications using NoSQL in order to disclose or clone data

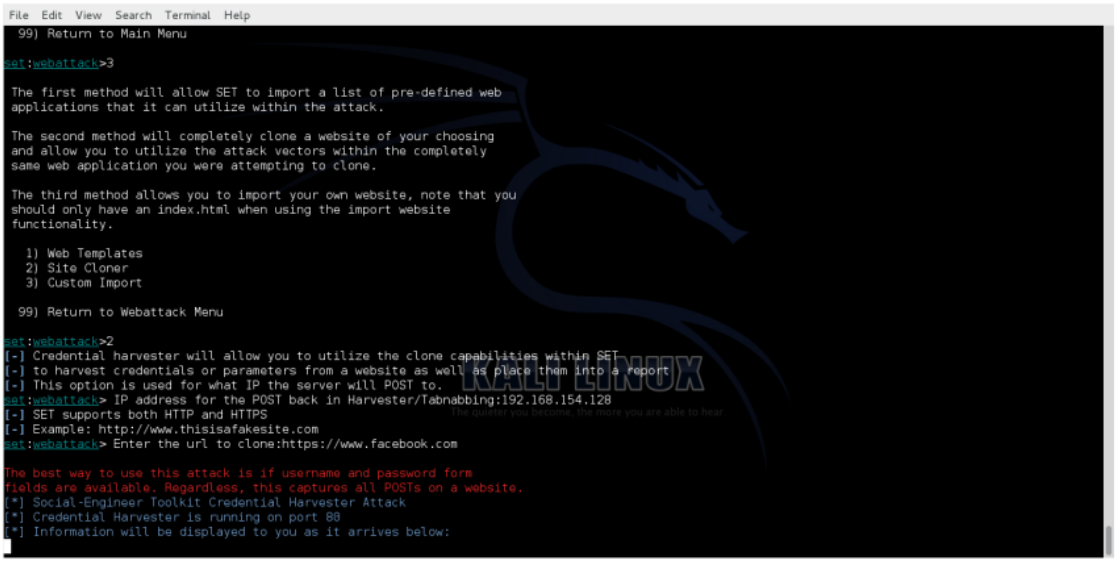
from the database.



It was successful as it copied the database and stored to my indented place, and the user did not realize his database has been compromised, giving me access to sensitive company data.

SET- Social Engineer Toolkit (SET) The Social-Engineer Toolkit (SET) is specifically designed to perform advanced attacks against the human element. ... The attacks built into the toolkit are designed to be targeted and focused attacks against a person

or organization used during a penetration test.



The social engineering tool did not work as the email became marked as a spam rather than going to its intended target, making the SET attack unsuccessful.

Task 2B

An evaluation of the impact of cyber security on your chosen organisation

My chosen organization is E corp which was initially a banking organization but grew subsidiaries in many different areas in farming, education and IT. The main focus is still the banks which are located worldwide. E crop is a very fast growing organization that makes industry changing technologies and innovations.

In 1986, Lester Moore was made CEO. Under him, the company became the world's largest employer in 1990, Bank of E became the world's largest consumer bank in 1992, and E Corp opened manufacturing plants in China, Japan, Singapore, and South Korea in 1993.

The wave of technology innovation is being rapidly adopted across E corps business venous and other institutions, creating unparalleled levels of access and connectivity across people, information, systems and assets worldwide – collectively a network delivered society. This unparalleled level of access has raised

the importance of cyber security as a specialized function in businesses for many reasons.

The importance of cybersecurity is far broader than simply addressing one issue such as securing data, securing mobile devices, or securing cloud computing environments. Nearly everything is interconnected and further complicated with hybrid enterprise environments that consist of a mix of cloud, non-cloud, internal and external IT service delivery models. These factors are creating security related stress to traditional IT professionals and organizations.

The Importance of Cybersecurity is Rising

The importance of cybersecurity, as a result, is rising to become an integral part of an overall security plan and IT security team. Cybersecurity is focused on the leakage (or loss) of sensitive data, intellectual property, and protecting digital assets – everything from networks to hardware and information that is processed, stored or transported by inter-networked information systems. *(Newman, L. and Keats, J.2018)*

1

Fsociety hacks

In May 2015, fsociety organize a coordinated attack on E Corp's digital records and the facilities housing the physical backups. E Corp keeps records of their data at the high security Steel Mountain facility, and following fsociety's initial DDoS attack in February, numerous other backup facilities. When the hack goes ahead, all of E Corps digital data is encrypted with a key that is virtually unbreakable. This includes their records on the amount of debt they are owed by people across the globe. The hack effectively wipes away this debt as E Corp has no records, whether physical or digital, of it. There is widespread panic globally as markets plummet.

The aftermath of this attack

In the aftermath of the attack, ecorp has changed its security policies with increase security in certain departments. They had to upscale security standards for all personnel entering any department with biometrics and a smart card.

Task 2 C

A critical evaluation of the cyber security strategies that are used within your chosen organisation, mapping these to industry standards

Policy brief & purpose

E-corp's company cyber security policy outlines our guidelines and provisions for preserving the security of our data and technology infrastructure.

The more we rely on technology to collect, store and manage information, the more vulnerable we become too severe security breaches. Human errors, hacker attacks and system malfunctions could cause great financial damage and may jeopardize our company's reputation.

For this reason, we have implemented a number of security measures. We have also prepared instructions that may help mitigate security risks. We have outlined both provisions in this policy. ***(****Ics-cert.us-cert.gov. 2017)*

1

Scope

This policy applies to all E-corp employees, contractors, volunteers and anyone who has permanent or temporary access to our systems and hardware.

Policy elements

Confidential data

Confidential data is secret and valuable. Common examples are:

- Unpublished financial information
- Data of customers/partners/vendors
- Patents, formulas or new technologies
- Customer lists (existing and prospective)
- All employees are obliged to protect this data. In this policy, we will give our employees instructions on how to avoid security breaches.

Protect personal and company devices

When E-corp employees use their digital devices to access company emails or accounts, they introduce security risk to our data. We advise our employees to keep both their personal and company-issued computer, tablet and cell phone secure. They can do this if they:

- Keep all devices password protected.
- Choose and upgrade a complete antivirus software.
- Ensure they do not leave their devices exposed or unattended.
- Install security updates of browsers and systems monthly or as soon as updates are available.
- Log into company accounts and systems through secure and private networks only.

We also advise our employees to avoid accessing internal systems and accounts from other people's devices or lending their own devices to others.

When new hires receive company-issued equipment they will receive instructions for:

[Disk encryption setup]
[Password management tool setup]
[Installation of antivirus/ anti-malware software]
They should follow instructions to protect their devices and refer to our [Security Specialists/ Network Engineers] if they have any questions.

Keep emails safe

Emails often host scams and malicious software (e.g. worms.) To avoid virus infection or data theft, we instruct E-corp employees to:

- Avoid opening attachments and clicking on links when the content is not adequately explained (e.g. "watch this video, it's amazing.")

- Be suspicious of clickbait titles (e.g. offering prizes, advice.)
- Check email and names of people they received a message from to ensure they are legitimate.
- Look for inconsistencies or give-aways (e.g. grammar mistakes, capital letters, excessive number of exclamation marks.)

If an employee isn't sure that an email they received is safe, they can refer to our [IT Specialist.]

Manage passwords properly

Password leaks are dangerous since they can compromise our entire infrastructure. Not only should passwords be secure so they won't be easily hacked, but they should also remain secret. For this reason, we advise our employees to:

Choose passwords with at least eight characters (including capital and lower-case letters, numbers and symbols) and avoid information that can be easily guessed (e.g. birthdays.)

Remember passwords instead of writing them down. If employees need to write their passwords, they are obliged to keep the paper or digital document confidential and destroy it when their work is done.

Exchange credentials only when absolutely necessary. When exchanging them in-person isn't possible, employees should prefer the phone instead of email, and only if they personally recognize the person they are talking to.

Change their passwords every two months.

Remembering a large number of passwords can be daunting. We will purchase the services of a password management tool which generates and stores passwords. Employees are obliged to create a secure password for the tool itself, following the abovementioned advice. *(Ptac.ed.gov. 2017)*

1

Transfer data securely

Transferring data introduces security risk. E-corp employees must:

- Avoid transferring sensitive data (e.g. customer information, employee records) to other devices or accounts unless absolutely necessary. When mass transfer of such data is needed, we request employees to ask our [Security Specialists] for help.
- Share confidential data over the company network/ system and not over public Wi-Fi or private connection.
- Ensure that the recipients of the data are properly authorized people or organizations and have adequate security policies.
- Report scams, privacy breaches and hacking attempts

Our [IT Specialists/ Network Engineers] need to know about scams, breaches and malware so they can better protect our infrastructure. For this reason, we advise our employees to report perceived attacks, suspicious emails or phishing attempts as soon as possible to our specialists. Our [IT Specialists/ Network Engineers] must investigate promptly, resolve the issue and send a companywide alert when necessary. (*Itgovernance.co.uk. 2017)*

E-corp Security Specialists are responsible for advising employees on how to detect scam emails. We encourage our employees to reach out to them with any questions or concerns.

Additional measures

To reduce the likelihood of security breaches, we also instruct our employees to:

- Turn off their screens and lock their devices when leaving their desks.
- Report stolen or damaged equipment as soon as possible to [HR/ IT Department].
- Change all account passwords at once when a device is stolen.
- Report a perceived threat or possible security weakness in company systems.
- Refrain from downloading suspicious, unauthorized or illegal software on their company equipment.
- Avoid accessing suspicious websites.

We also expect our employees to comply with our social media and internet usage policy.

E-corp [Security Specialists/ Network Administrators] should:

- Install firewalls, anti malware software and access authentication systems.
- Arrange for security training to all employees.
- Inform employees regularly about new scam emails or viruses and ways to combat them.
- Investigate security breaches thoroughly.
- Follow this policies provisions as other employees do.

E-corp company will have all physical and digital shields to protect information.

Remote employees

Remote employees must follow this policy's instructions too. Since they will be accessing our company's accounts and systems from a distance, they are obliged to follow all data encryption, protection standards and settings, and ensure their private network is secure.

We encourage them to seek advice from our [Security Specialists/ IT Administrators.]

Disciplinary Action

We expect all our employees to always follow this policy and those who cause security breaches may face disciplinary action:

- First-time, unintentional, small-scale security breach: We may issue a verbal warning and train the employee on security.
- Intentional, repeated or large scale breaches (which cause severe financial or other damage): We will invoke more severe disciplinary action up to and including termination.

We will examine each incident on a case-by-case basis.

Additionally, employees who are observed to disregard our security instructions will face progressive discipline, even if their behaviour hasn't resulted in a security breach.

Take security seriously

Everyone, from our customers and partners to E-corp employees and contractors, should feel that their data is safe. The only way to gain their trust is to proactively protect our systems and databases. We can all contribute to this by being vigilant and keeping cyber security top of mind. *(WhatIs.com. 2017)*

The standards we use are

ISO/IEC 27003:2017	Information technology -- Security techniques -- Information security management systems -- Guidance
ISO/IEC 27552	Information technology -- Security techniques -- Enhancement to ISO/IEC 27001 for privacy management -- Requirements
ISO/IEC 27001:2013	Information technology -- Security techniques -- Information security management systems -- Requirements
ISO/IEC 27010:2015	Information technology -- Security techniques -- Information security management for inter-sector

and inter-organizational communications

These are the strategies we using within our company to ensure that the highest standards are always met.

Task 3C

Produce a training plan for improving network security including user awareness and prevention mechanisms.

Training should be a key part of the organization as it prevents further threats. An individual should be always ready to act in case an attack comes, and should be prepared to deal with it in the most efficient way**.** (*Honeywellprocess.com. 2017)*

The cyber security awareness training that this plans covers are:

- **Threats**
- **Policies**
- **Prevention**
- **Awareness**

Threats

There are many threats in cyber space from corrupting malwares to more tactical like social engineering. An individual should be very alert when entering the cyber space and should not go into restricted or "fishy" areas. The individual should not download anything without the confirmation of the supervisor as any link or webpage might include a virus or so on.

Policies

The Policies are a set of guidelines which should be followed as they will prevent any unforeseen action by a clueless or unknowing individual. These policies will help in areas of password protection, socializing on the internet and so on.

Prevention

Prevention should be the main objective as prevention would stop a threat from arsing. Prevention will save a lot of time and money as a threat can be avoided or terminated before it becomes too powerful to stop or spread to other department's or systems.

Awareness

Awareness is important as it allows individual to understand what are actual threats are and how to deal with them properly. Employees should receive information about who to contact if they discover a security threat and be taught that data as a valuable corporate asset.

Reference:

Honeywellprocess.com. (2017). Cite a Website - Cite This For Me. [online] Available at: https://www.honeywellprocess.com/library/marketing/whitepapers/Assessments-for-Cyber-Security-Risk-Mitigation.pdf [Accessed 14 Nov. 2017].

WhatIs.com. (2017). What is cybersecurity? - Definition from WhatIs.com. [online] Available at: http://whatis.techtarget.com/definition/cybersecurity [Accessed 24 Oct. 2017].

Itgovernance.co.uk. (2017). Cyber security risk assessment – IT Governance*. [online] Available at: https://www.itgovernance.co.uk/cyber-security-risk-assessments-10-steps-to-cyber-security [Accessed 14 Nov. 2017].*

Ics-cert.us-cert.gov. (2017). Cite a Website - Cite This For Me. [online] Available at: https://ics-cert.uscert.gov/sites/default/files/documents/10_Basic_Cybersecurity_Measures-WaterISAC_June2015_S508C.pdf [Accessed 14 Nov. 2017].

Iso.org. (2017). Management System Standards list. [online] Available at: https://www.iso.org/management-system-standards-list.html [Accessed 6 Dec. 2017].

Ptac.ed.gov. (2017). Cite a Website - Cite This For Me. [online] Available at: http://ptac.ed.gov/sites/default/files/Data%20Security%20and%20Management%20Training.pdf [Accessed 6 Dec. 2017].

Zamora, W. and Zamora, W. (2017). How to create a successful cybersecurity policy - Malwarebytes Labs. [online] Malwarebytes Labs. Available at: https://blog.malwarebytes.com/101/2016/03/how-to-create-a-successful-cybersecurity-policy/ [Accessed 6 Dec. 2017].

Newman, L. and Keats, J. (2018). The Biggest Cybersecurity Disasters of 2017 So Far*. [online] WIRED. Available at: https://www.wired.com/story/2017-biggest-hacks-so-far/ [Accessed 20 Jan. 2018].*

Abdullah.Kashif

Cyber Security

Unit 5.1

Abdullah-cybersec

ORIGINALITY REPORT

99%	77%	11%	99%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	Submitted to Western International College (WINC London) Student Paper	99%

Exclude quotes	On	Exclude matches	Off
Exclude bibliography	On		