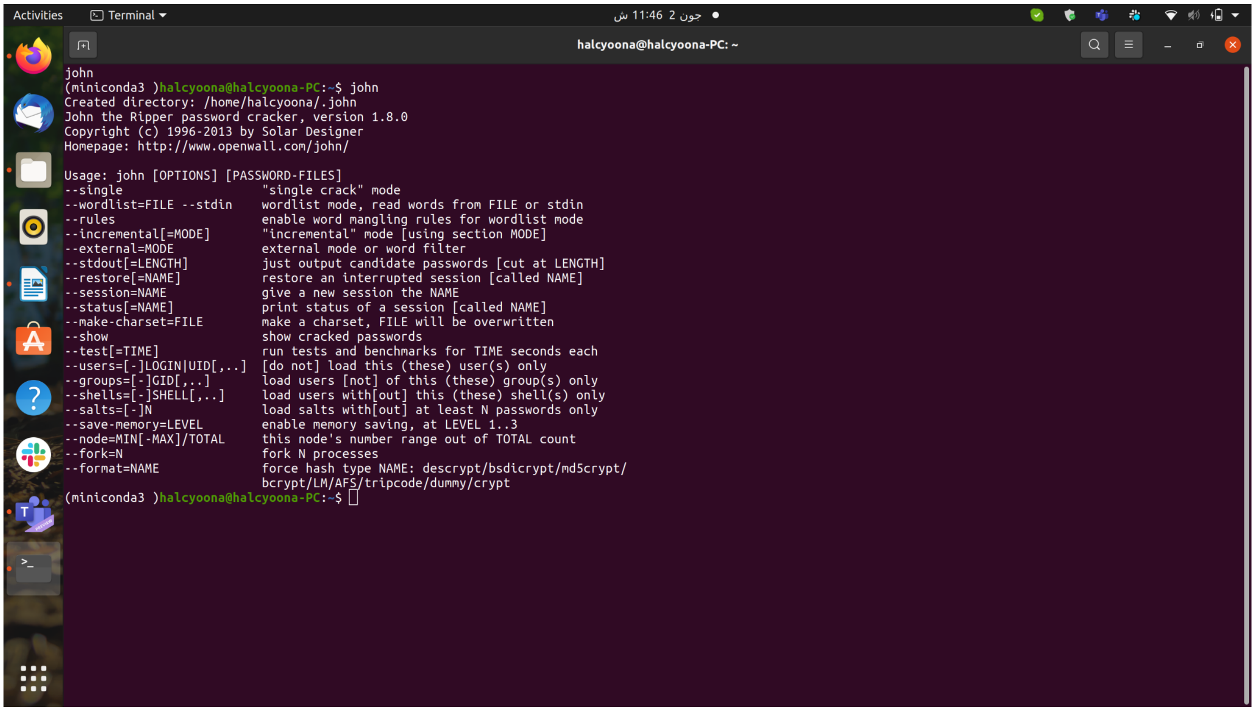
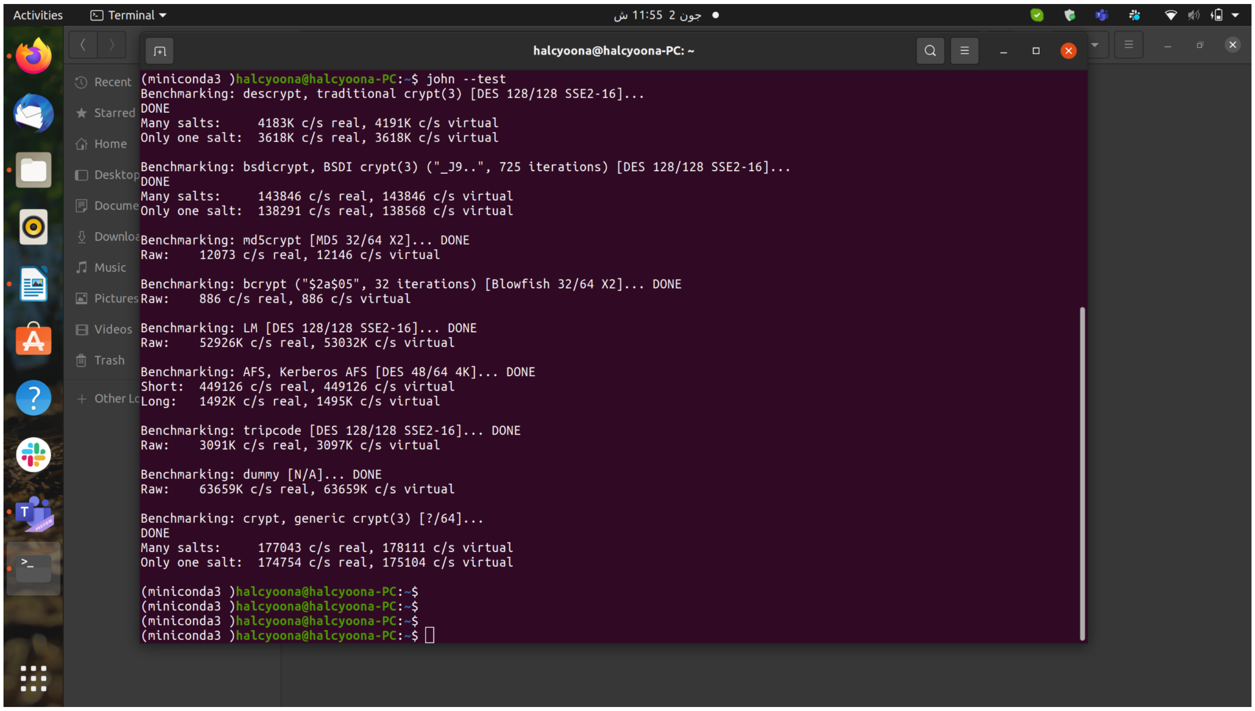
Assignment 01

Question # 1:

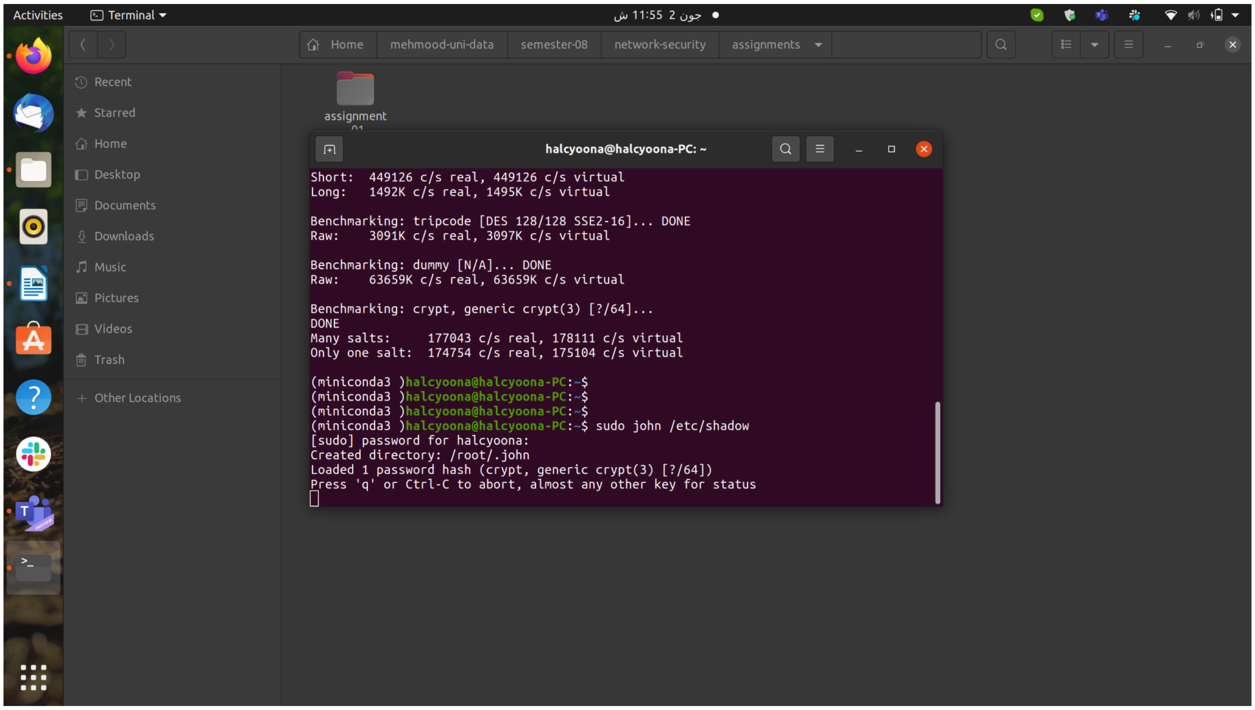
I have tried to crack my own laptop's password using john the ripper. Here are the screenshots.



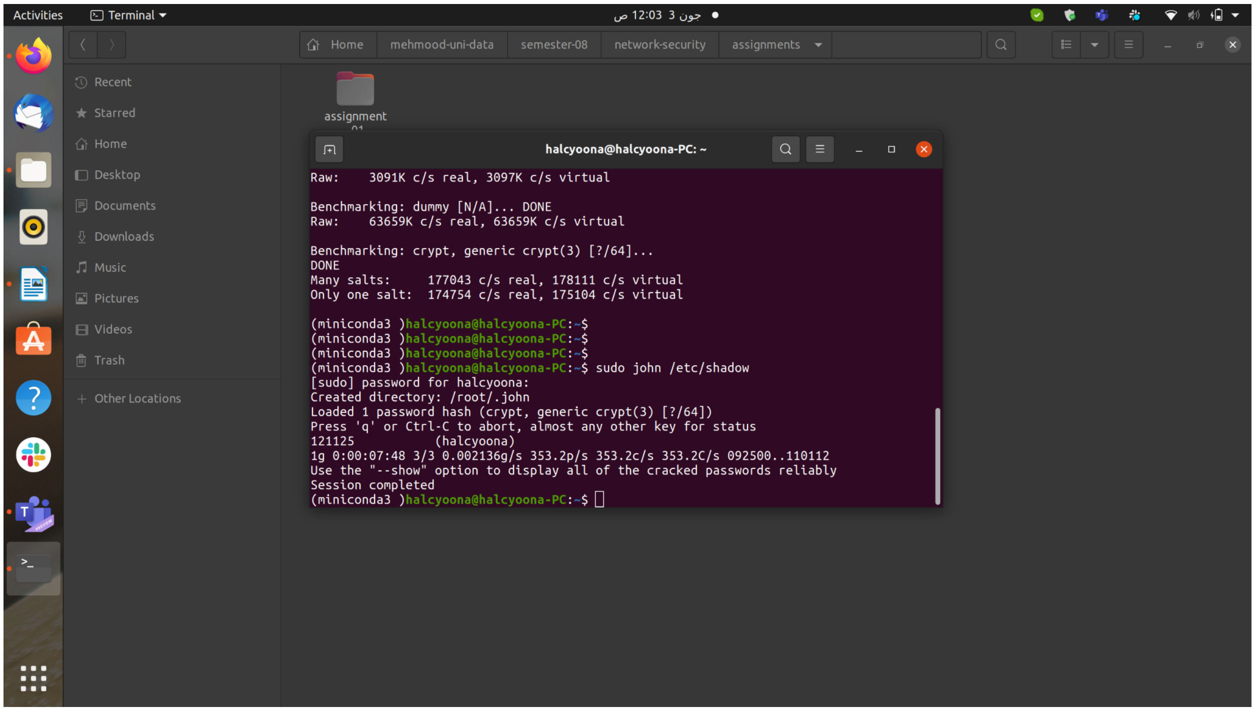
```
john
(miniconda3 )halcyoona@halcyoona-PC:~$ john
Created directory: /home/halcyoona/.john
John the Ripper password cracker, version 1.8.0
Copyright (c) 1996-2013 by Solar Designer
Homepage: http://www.openwall.com/john/

Usage: john [OPTIONS] [PASSWORD-FILES]
--single                   "single crack" mode
--wordlist=FILE --stdin    wordlist mode, read words from FILE or stdin
--rules                    enable word mangling rules for wordlist mode
--incremental[=MODE]       "incremental" mode [using section MODE]
--external=MODE            external mode or word filter
--stdout[=LENGTH]          just output candidate passwords [cut at LENGTH]
--restore[=NAME]           restore an interrupted session [called NAME]
--session=NAME             give a new session the NAME
--status[=NAME]            print status of a session [called NAME]
--make-charset=FILE        make a charset, FILE will be overwritten
--show                     show cracked passwords
--test[=TIME]              run tests and benchmarks for TIME seconds each
--users=[-]LOGIN|UID[,..]  [do not] load this (these) user(s) only
--groups=[-]GID[,..]       load users [not] of this (these) group(s) only
--shells=[-]SHELL[,..]     load users with[out] this (these) shell(s) only
--salts=[-]N               load salts with[out] at least N passwords only
--save-memory=LEVEL        enable memory saving, at LEVEL 1..3
--node=MIN[-MAX]/TOTAL     this node's number range out of TOTAL count
--fork=N                   fork N processes
--format=NAME              force hash type NAME: descrypt/bsdicrypt/md5crypt/
                           bcrypt/LM/AFS/tripcode/dummy/crypt
(miniconda3 )halcyoona@halcyoona-PC:~$ 
```



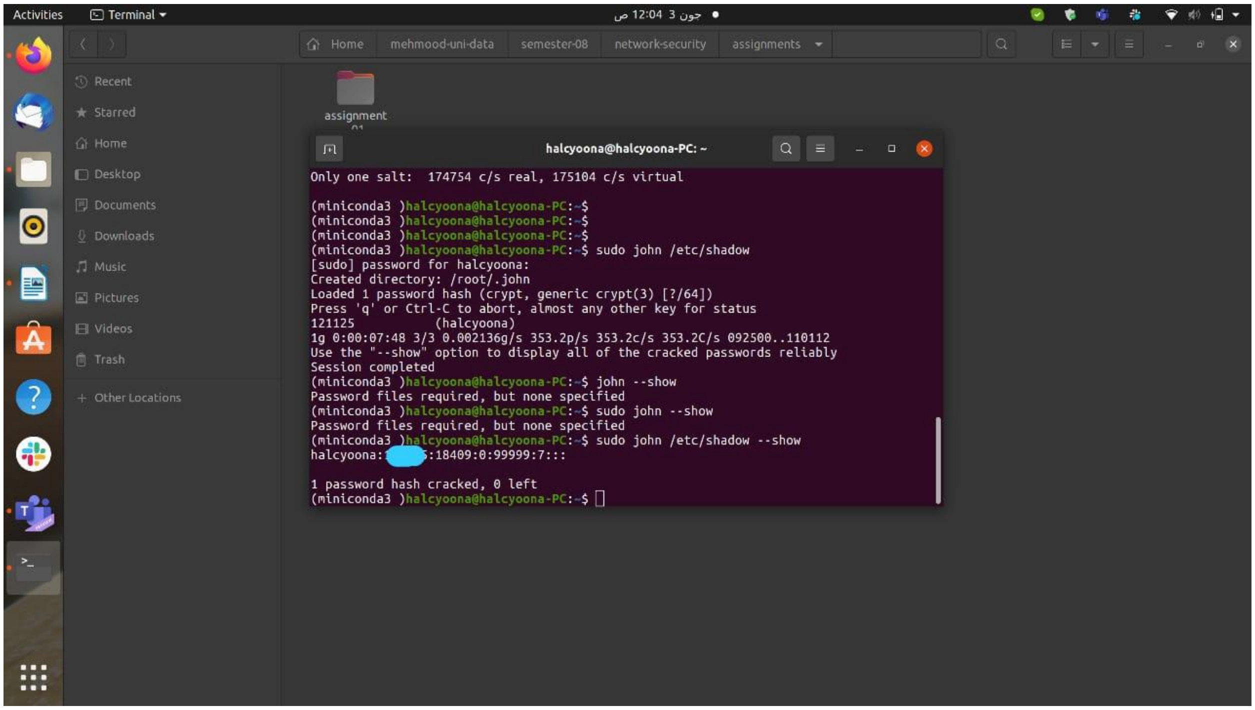
```
(miniconda3 )halcyoona@halcyoona-PC:~$ john --test
Benchmarking: descrypt, traditional crypt(3) [DES 128/128 SSE2-16]...
DONE
Many salts:     4183K c/s real, 4191K c/s virtual
Only one salt:  3618K c/s real, 3618K c/s virtual

Benchmarking: bsdicrypt, BSDI crypt(3) ("_J9..", 725 iterations) [DES 128/128 SSE2-16]...
DONE
Many salts:     143846 c/s real, 143846 c/s virtual
Only one salt:  138291 c/s real, 138568 c/s virtual

Benchmarking: md5crypt [MD5 32/64 X2]... DONE
Raw:    12073 c/s real, 12146 c/s virtual

Benchmarking: bcrypt ("$2a$05", 32 iterations) [Blowfish 32/64 X2]... DONE
Raw:    886 c/s real, 886 c/s virtual

Benchmarking: LM [DES 128/128 SSE2-16]... DONE
Raw:    52926K c/s real, 53032K c/s virtual

Benchmarking: AFS, Kerberos AFS [DES 48/64 4K]... DONE
Short:  449126 c/s real, 449126 c/s virtual
Long:   1492K c/s real, 1495K c/s virtual

Benchmarking: tripcode [DES 128/128 SSE2-16]... DONE
Raw:    3091K c/s real, 3097K c/s virtual

Benchmarking: dummy [N/A]... DONE
Raw:    63659K c/s real, 63659K c/s virtual

Benchmarking: crypt, generic crypt(3) [?/64]...
DONE
Many salts:     177043 c/s real, 178111 c/s virtual
Only one salt:  174754 c/s real, 175104 c/s virtual

(miniconda3 )halcyoona@halcyoona-PC:~$
(miniconda3 )halcyoona@halcyoona-PC:~$
(miniconda3 )halcyoona@halcyoona-PC:~$
(miniconda3 )halcyoona@halcyoona-PC:~$ 
```



```
Short:  449126 c/s real, 449126 c/s virtual
Long:   1492K c/s real, 1495K c/s virtual

Benchmarking: tripcode [DES 128/128 SSE2-16]... DONE
Raw:    3091K c/s real, 3097K c/s virtual

Benchmarking: dummy [N/A]... DONE
Raw:    63659K c/s real, 63659K c/s virtual

Benchmarking: crypt, generic crypt(3) [?/64]...
DONE
Many salts:     177043 c/s real, 178111 c/s virtual
Only one salt:  174754 c/s real, 175104 c/s virtual

(miniconda3 )halcyoona@halcyoona-PC:~$
(miniconda3 )halcyoona@halcyoona-PC:~$
(miniconda3 )halcyoona@halcyoona-PC:~$
(miniconda3 )halcyoona@halcyoona-PC:~$ sudo john /etc/shadow
[sudo] password for halcyoona:
Created directory: /root/.john
Loaded 1 password hash (crypt, generic crypt(3) [?/64])
Press 'q' or Ctrl-C to abort, almost any other key for status
```



```
Raw:    3091K c/s real, 3097K c/s virtual

Benchmarking: dummy [N/A]... DONE
Raw:    63659K c/s real, 63659K c/s virtual

Benchmarking: crypt, generic crypt(3) [?/64]...
DONE
Many salts:     177043 c/s real, 178111 c/s virtual
Only one salt:  174754 c/s real, 175104 c/s virtual

(miniconda3 )halcyoona@halcyoona-PC:~$
(miniconda3 )halcyoona@halcyoona-PC:~$
(miniconda3 )halcyoona@halcyoona-PC:~$
(miniconda3 )halcyoona@halcyoona-PC:~$ sudo john /etc/shadow
[sudo] password for halcyoona:
Created directory: /root/.john
Loaded 1 password hash (crypt, generic crypt(3) [?/64])
Press 'q' or Ctrl-C to abort, almost any other key for status
121125           (halcyoona)
1g 0:00:07:48 3/3 0.002136g/s 353.2p/s 353.2c/s 353.2C/s 092500..110112
Use the "--show" option to display all of the cracked passwords reliably
Session completed
(miniconda3 )halcyoona@halcyoona-PC:~$
```



```
Only one salt:  174754 c/s real, 175104 c/s virtual

(miniconda3 )halcyoona@halcyoona-PC:~$
(miniconda3 )halcyoona@halcyoona-PC:~$
(miniconda3 )halcyoona@halcyoona-PC:~$
(miniconda3 )halcyoona@halcyoona-PC:~$ sudo john /etc/shadow
[sudo] password for halcyoona:
Created directory: /root/.john
Loaded 1 password hash (crypt, generic crypt(3) [?/64])
Press 'q' or Ctrl-C to abort, almost any other key for status
121125           (halcyoona)
1g 0:00:07:48 3/3 0.002136g/s 353.2p/s 353.2c/s 353.2C/s 092500..110112
Use the "--show" option to display all of the cracked passwords reliably
Session completed
(miniconda3 )halcyoona@halcyoona-PC:~$ john --show
Password files required, but none specified
(miniconda3 )halcyoona@halcyoona-PC:~$ sudo john --show
Password files required, but none specified
(miniconda3 )halcyoona@halcyoona-PC:~$ sudo john /etc/shadow --show
halcyoona:[redacted]:18409:0:99999:7:::

1 password hash cracked, 0 left
(miniconda3 )halcyoona@halcyoona-PC:~$ 
```

You can see my password is cracked but I made it blur because of the security issues.

Question # 2:

NSA programs exposed:

1. The GCHQ scandal widened on 21 June when the Guardian reported that the UK spy agency was tapping fibre-optic cables that carry global communications and sharing vast amounts of data with the NSA, its US counterpart.The paper revealed it had obtained documents from Edward Snowden showing that the GCHQ operation, codenamed Tempora, had been running for 18 months.
2. After fleeing to Hong Kong, Edward Snowden told the South China Morning Post that the NSA had led more than 61,000 hacking operations worldwide, including many in Hong Kong and mainland China.He said targets in Hong Kong included the Chinese University, public officials and businesses."We hack network backbones - like huge internet routers, basically - that give us access to the communications of hundreds of thousands of computers without having to hack every single one," Mr Snowden was quoted as saying.
3. The scandal broke in early June 2013 when the Guardian newspaper reported that the US National Security Agency (NSA) was collecting the telephone records of tens of millions of Americans.The paper published the secret court order directing telecommunications company Verizon to hand over all its telephone

data to the NSA on an "ongoing daily basis".That report was followed by revelations in both the Washington Post and Guardian that the NSA tapped directly into the servers of nine internet firms, including Facebook, Google, Microsoft and Yahoo, to track online communication in a surveillance programme known as Prism.

Attacks and programs shown:

1. The hacker team called Tailored Access operations hacks into computers and infects them with malware.It was for targeted operations when they can't find intelligence and need more detail.
2. XKeyscore: It is used to search for everything the user does on the internet.It can search everything which makes it impossible to keep anything secure on a device. Even when encrypted, even confidential files are not safe.
3. NSA undermines the encrypted data flowing, forcing companies to install backdoors, hacking into servers and computers, or promoting the use of weaker algorithms.It invades privacy in the name of cybersecurity, it is making the Internet less secure and exposing it to criminal hacking and unlawful surveillance. It will wear away the economic competitiveness of the larger companies.

Penetration techniques and attack strategy used

1. Valid access—As a contractor, Snowden was issued a valid Common Access Card (CAC). This smart card had preloaded cryptographic keys and digital certificates that authenticated his identity and provided basic trusted status and access to the information and systems he was authorized to access.

2. SSH Keys—As a systems administrator, Snowden used Secure Shell (SSH) keys to authenticate and manage systems as a part of his everyday job. Prior to working for the NSA, Snowden is known to have tested the limits of his administrator privileges to gain unauthorized access to classified information while at his CIA post in Geneva, Switzerland.

3. Limited computing resources—Like many external attackers, Snowden didn't have a bay of servers, top-end Macintosh computers, or even a Windows laptop hanging off the NSA network, which is referred to as NSAnet. It's been reported

> that Snowden had basic terminal or thin-client access to the NSAnet. He had much the same view an attacker might have after a successful initial intrusion or reconnaissance mission.

Question # 3:

Importance of Cyber Security:

Without a cybersecurity program, your organization cannot defend itself against data breach campaigns, making it an irresistible target for cybercriminals.

Both inherent risk and residual risk is increasing, driven by global connectivity and usage of cloud services, like Amazon Web Services, to store sensitive data and personal information. Widespread poor configuration of cloud services paired with increasingly sophisticated cyber criminals means the risk that your organization suffers from a successful cyber attack or data breach is on the rise.

Gone are the days of simple firewalls and antivirus software being your sole security measures. Business leaders can no longer leave information security to cybersecurity professionals.

Cyber threats can come from any level of your organization. You must educate your staff about simple social engineering scams like phishing and more sophisticated cybersecurity attacks like ransomware attacks (think WannaCry) or other malware designed to steal intellectual property or personal data.

GDPR and other laws mean that cybersecurity is no longer something businesses of any size can ignore. Security incidents regularly affect businesses of all sizes and often make the front page causing irreversible reputational damage to the companies involved.

If you are not yet worried about cybersecurity, you should be.

Importance of cyber warfare:

The advancement of technological innovation has armed attackers to expose cyber vulnerabilities inherent in networks and systems that handle sensitive information. Once believed to be exclusively designed and executed for military purposes, the realm of cyber warfare is fast expanding to include civilian industries. Menacingly, advanced information technology expertise and superior execution skills of cyber reconnaissance rogues are far outpacing policy developments and forging of combined international strategies, if any.

Interestingly, most countries try to project being passive victims, but a careful consideration reveals that an increasingly large number of countries are actively targeting opponents' commercial and security-specific information. While state-sponsored attacks are less frequent, counts of espionage and sabotage from individual groups are on the rise. However, the most sophisticated sabotage are carried out by states directly or via hackers supported by the state.

Security company Symantec has detailed how a sophisticated and multi-stage piece of malware, Regin, has been in use since 2008 as a mass surveillance tool. Believed to be a nation state espionage tool, Regin "has been used in spying operations against governments, infrastructure operators, businesses, researchers, and private individuals." Loaded with stealth features that are highly complex and work for several years, the malware targets ISPs, Exchange servers, and the commercial and military aviation, hospitality and energy sectors, among many others. "Even when its presence is detected, it is very difficult to ascertain what it is doing."