CARDIFF SCHOOL OF TECHNOLOGIES

4D Digidol | Data | Dylunio | Dyfodol

Academic Year: 2020/21

CIS7028 - Information Security

Term 1

Module Leader: Dr. Chaminda Hewage

Information Security Final Report

By

Rohit Saini

MSc Data Science (Internship)

St20183550

Contents

Task 1.1

Introduction

Whole world is suffering from a virus known as Corona Virus (COVID-19). We have to do something to stop this. Contact Tracing application is very helpful approach to decrease the spread of coronavirus. As we are going to install CCTV and launch Contact Tracing Application for tackling the corona virus spread, we should follow some Data protection rules and regulation and take some important steps to keep our data and process compliant.

General Data Protection Regulation

The General Data Protection Regulation is the regulation that provides greater control over the personal data of the citizens. The GDPR guarantee that the information is being security protected. It is the company or organization responsibility to put major in place in order to ensure that their customer data stay private. Documentation is the pillar to establish compliance.

Data Controller, Data Processor and Data Subject

Data controller is someone who determines the purpose of processing the personal data. Data processor is someone who processes the personal data on the behalf of data controller (Ico.org.uk, 2019b) and Data subject is a person whose data is processed by the controller or processor.

Personal Data (Where it comes from)

Generally personal data is any information related to already identified individual or that can identify an individual either directly or indirectly. For example: A person name, address, location can be considered as a personal data. As we are going to launch a Contact Tracing application then the data should be collected through this application only (Ico.org.uk, 2019l)

Principles

GDPR principles are the baseline for Contact Tracing Application. There are seven principles of Data Protection which matters the most in GDPR and are related to processing the personal data (Ico.org.uk, 2019l).

1. Transparency, Fairness and Lawfulness - The principle demands fairness, transparency and lawfulness in the usage and handling of personal data. The company will need to clarify with people about how they are using personal data and also need an appropriate lawful model to process the data.
2. Specified, Explicit and Legitimate Purposes – This principle demands limiting the processing of personal data to legitimate, explicit and specified purposes. The company will be unable to reuse or disclose personal data for the purposes that are not compatible with Contact Tracing.
3. Minimizing the storage and collection of Personal Data – This principle asks organization to collect and store data which is adequate and relevant for the planned purpose only. The company need to ensure that they only collect personal data that they actually need for contact tracing purposes.
4. Accuracy of Personal Data – This principle ensures the accuracy of personal data and enabling it to be erased and corrected. The company should ensure that the subject's

personal data they hold is accurate and can be corrected if any errors occurs. If the data will be inaccurate then the contact tracing app is useless for everyone.

5. Limiting the storage of Personal Data – As per the principle the company need to ensure that they retain personal data only for time being necessary to achieve the purposes for which the data was collected. In contact tracing purposes the data should be removed after the covid-19 patient will recovered from the virus.
6. Security, Integrity and Confidentiality – This principle ensures security, integrity and confidentiality of personal data. The company must take relevant steps to keep personal data secure through organizational and technical security measures. The company should implement techniques like Data loss prevention, Drive encryption, Data encryption to safeguard the personal data. Contact tracing data should be carefully and regularly encrypted and only authorized person would be allowed to access it.
7. Accountability – When processing people personal information, the company have to make sure that they do it in a way that is the least disturbing for individuals' privacy so that they can comply with data protection rules.

Lawfulness of Processing

The processing of data should be lawful only if that at least one of the following should applies- Consent, Contract, Legal Obligation, Vital Interest, Legitimate Interest and Public Task. (Ico.org.uk, 2019e) In contact tracing Legitimate Interest is applicable as the data is collected for making efforts to tackle covid-19. (ico.org.uk, 2020)

Rights of an Individual

There are total seven rights for an individual i.e. right to be informed, right to access, right to rectification, right to forgotten, right to restrict processing, right to data portability and right to automated decision making and profiling. (Ico.org.uk, 2019d)

For contact tracing purposes, only two of them are applicable i.e. (ico.org.uk, 2020).

1. Right to access- Every individual has the full right to know that exactly what data or information is held about them and how it is being used and processed.
2. Right to rectification- Every individual will be allowed to have personal data rectified if it is inaccurate or they have an option to complete it if it is incomplete.

Task 1.2

Nowadays cyber-attacks, data stealing or data leaking are more common, it is really important to keep the data safe and secured. Personal Data of the data subject should be protected. We should be aware of data protection from developing the Contact tracing application to each time we process data. We have to implement some protective measures to protect our data. According to Article 32 of GDPR, the technical and the organizational measures such as pseudonymization and encryption of personal data should be implemented by the controller and the processors. (General Data Protection Regulation (GDPR), 2013)

As an organization it is important to implement appropriate technical measures to avoid data breach and ISO27001 provides an outstanding initial point to reduce the risk of the breach. (itgovernance, n.d.) ISO stands for International Standard Organization and 27001 is a specific standard for establishing an Information Security Management System (ISMS). Information security management system is a framework to make best practices for the day to day management of the security risks to the information that company processes, stores or transmits. (ISMS Online, 2017)

ISO 27001 and GDPR are not same but have a common perspective. ISO27001 suggests many data protection controls and techniques to GDPR. Common goal of both is to provide strong security and to avoid data breaches (Leal, 2018)

Let's see how ISO27001 would help in GDPR compliance and some stages and techniques can be (Dutton, 2017):

- **Risk Assessment**- For complying with GDPR, regular risk assessment must be conducted by the company to detect risk and weaknesses that can disturb the flow of data process and the data itself of the Contact tracing. Generally, there are 5 steps in risk assessment (Irwin, 2020).
    1. Creating a risk management framework- This step will help the company for making a proper flow that how they will be going to detect and handle the risk.
    2. Identifying the risk – In the second step, the company will be able to identify that what type of risk are affecting what type of data.
    3. Analyzing the risk- In the third step, the company will be able to analyze the threats that are affecting a particular data which can further help in finding the weaknesses of the Contact tracing application.
    4. Evaluating the Risk – the fourth step help the company to find how important is each risk and which risk should be handled first.
    5. The last step is treatment of the risk which can be done by removing it completely or by applying some security controls.

- **Data Encryption**- ISO27001 recommends Data Encryption as an important measure that should be applied to every data of Contact Tracing to decrease the security risks and data breach. With the help of risk assessment, the company would be able encrypt that data which are at a higher risk.
- **Testing and Assessment** – ISO27001 certified company will have to check whether their ISMS is constantly monitored, updated and reviewed regularly.

Data Breach

Stealing of data by an unauthorized party is known as Data breach. A data breach happens when someone successfully gets into our system and takes all the information from our system. This can be done by many methods.

Points to remember whenever a data breach occurs (Ico.org.uk, 2019f) –

- If a Data breach occurs then company has to notify the data breach to the supervisor within 72 hours.
- If the data breach causes a high risk to those affected individual, then they should also be informed as soon as possible.
- The company have to inform the ICO about the data breach as soon as possible.
- If the company fails to inform the ICO, then the company should be charged with a large fine.

Task 1.3

Some different techniques and technologies used for implementing data protection-

Data Audit – As a company you need to perform a data audit in order to get compliance with GDPR. There is some general question which a company should keep in mind "What type of data are the company collecting", "Is it a hard copy or the soft copy(digital copy)", " how the company will gather the data", "Where are company is storing the data", "In the company who will control the data" (www.nibusinessinfo.co.uk, n.d.). For contact tracing purposes, the company will collect the relevant information which can be "GPS location, Name and Address", the data will be in the soft copy and always store at the company backend servers, the company will collect the data directly from the individuals by providing them contact tracing application, the whole data will be controlled by the controller and the project teammates. As a central system the company main effort will be on highly occupied area in the case of covid-19 contact tracing.

Data Mapping - Data mapping is basically the flow of data in a particular organization. Nowadays many companies are using data mapping software to manage their data. These software helps the company to manage large amount of data and also helps in creating the maps. Many software comes with a inbuilt data security features which can be helpful for a company to secure their data. (GDPR Associates, 2019)

Data Protection Impact Assessment (DPIA) -

Some especially risking processing information such as the processing of large amounts of personal data for example health data, require a company to carry out a DPIA. When carrying out a DPIA the company should: (Ico.org.uk, 2019c)

1. Identify each operation performed on data
2. Access the specific data protection risk involved
3. Develop strategies to mitigate them

A DPIA will help the company to:

1. Model the processes they want to put in place
2. Understand how they could affect people
3. Ease any negative effects on the people whose information are processed
4. Stay compliant with data protection rules

DPIA is helpful for keeping the information secure. It is also about designing your processes from the start in a way that protect people privacy.

Privacy Enhancing Technologies

Privacy enhancing technologies are used to protect the personal data. There are many technologies and techniques which can be used as a privacy:

1. **Data Pseudonymization**- Pseudonymization means processing personal data in a way that reduces the personal information no longer attributable to specific individual without use of additional information like replacing somebody name with a code but keeping a separate list of which codes going to which names. Pseudonymized data is considered as a personal data (Data Privacy Manager, 2020)

2. **Data Minimization** – Data minimization means only data that are useful for the company purposes should be processed rather than taking a lot of data and then getting confused. Taking the unusual data can increase the time for everything like managing, processing and handling. (Ico.org.uk, 2019h)

Data loss prevention

Data loss prevention is a technique that used to safeguard that the personal data of an individual should not be lost, not be changed or misused by anyone. The company should put the appropriate actions like encryption to prevent the users for misbehaving with the personal data. (Groot, 2019)

Some ways that DLP can support GDPR (Andrada Coos, 2017):

1. DLP can help in finding out that where the personal data is kept. Most DLP can help the company to find out the sensitive data by scanning the whole system and also helps in generating the data reports much faster.
2. DLP can also help in reducing the data when it is no longer needed with the help of encryption and deletion of data.
3. DLP can help in maintaining security of the data. DLP tools can scan the data and control whether any data breaches have happened or not.

Task 2

As Coronavirus pandemic is trending all over the world. The cyber-attacks during this pandemic are increasing too. The attackers are utilizing this situation of panic to exploit the victims. There have been various cyber-attacks incidents during this crisis. One from the victim list is Canon.

Canon is a Japanese multinational firm formerly knowns as ‘The Kwanon’ which was founded in 1937 and specializing in lenses, camera, printers and semiconductor equipment. Canon products and equipment are used by maximum people all over the world. Big film industries like Hollywood and Bollywood used canon products for their filming. Recently during COVID-19 pandemic in August 2020, Canon was a victim of a ransomware attack by a group called “MAZE”. According to Bleeping Computer many services including USA website, canon emails, Microsoft teams and many internal applications were affected by this attack (Abrams, 2020). The hackers behind the attack moves to the canon infrastructure by finding a loophole in the infected network (Nair, 2020).

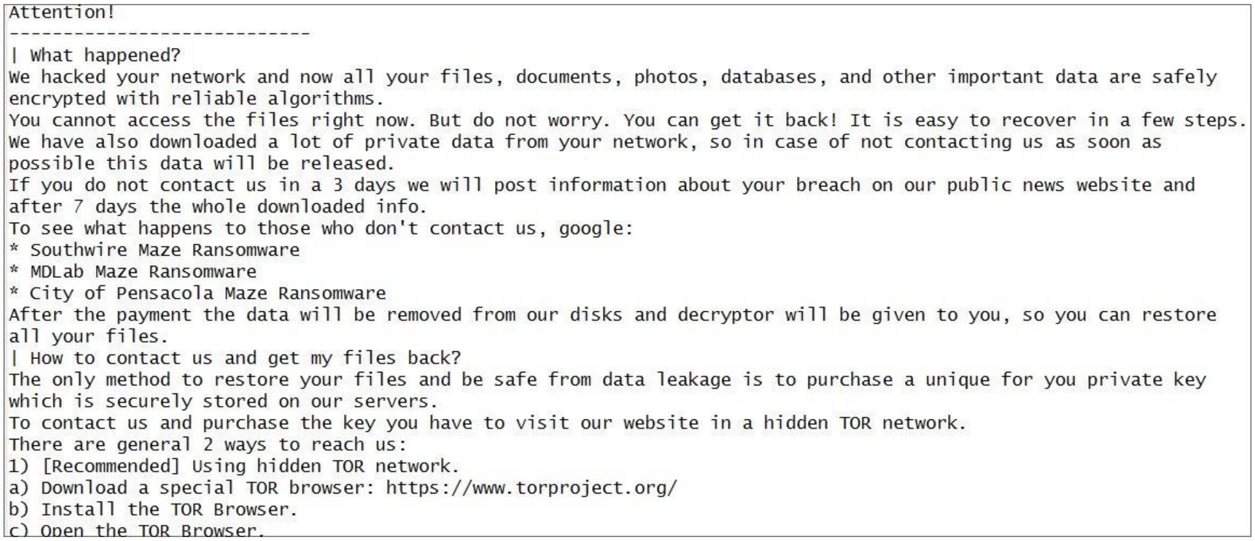
Let’s have a look on What is Ransomware? Ransomware is a type of malware which gets into a system, gets the access to the certain files or the system and lockdown all the files. Afterwards it seeks money from the user in order to get access to the locked files (kaspersky, 2020). When a malware is installed on the victim system then various things can be done by it like allows unauthorized access to the system, encrypt the whole hard drive, get access to social media account, installs a virus which may damage the whole system. Ransomware doesn’t have to stay hidden like other types of malware. According to McQuiggan, “Ransomware continues to be the favorite attack vector of cybercriminals” (Hope, 2020). Sending email attachments or links to the victims is one of the common methods which are used by attackers commonly known as “Phishing”. Attacker sends a spoof email to the victim containing a link in which malware is installed (Imperva, 2020). A type of ransomware is used in the Canon attack known as “Maze Ransomware” which is controlled by a group called “Maze”. What maze ransomware makes itself different from other ransomware is that Maze can infect a system and encrypts all data of the system so that it cannot be accessed (every ransomware does this) but Maze also steals and exfiltrates the data it finds to their own servers for blackmailing the victim if the ransom is not paid. This type of ransomware makes the attack a data breach as well (Bond, 2020).

In the case of Canon, there was a six day outage on the “image.Canon” website due to some technical issue with the backend servers. The “image.canon” website is used to store and upload images and videos by a mobile application. After some investigation by the canon team, they stated that some of the user’s images and videos saved to this site before 16th June is lost (Abrams, 2020c). While canon is dealing with the outage, the organization also suffered a cyber-attack known as Maze Ransomware attack which was carried out by a group called “Maze”. When contacting with the hacker group they say that the ransomware attack is done by them and they stole 10 terabytes data, databases etc. But they also specified that the image.canon outage was not caused by them (Jay, 2020). The organization has not yet released that how the hackers got into the canon system and exactly what types of techniques is used by them. Generally, Maze group has some techniques like they spread across a network, infects a particular system, steal the data, exfiltrates the whole data to their own servers and encrypts whole data of the victim system (Cluley, 2020). The biggest part of the ransomware job is to access the system. While many ransomwares use social engineering techniques to access the system, Maze use Exploit kits (Mark, 2020). Exploit kit is a tool that create, customize and distribute malware. Exploit kits silently exploit the vulnerabilities on the victim's system while browsing. A number of steps must be completed with the exploit kit to successfully gain the control of the victim system. A compromised website starts the exploit kit, if there will be any vulnerabilities then the compromised website will divert the traffic to the exploit. A vulnerable application is used by the exploit to run the malware in the victim system (Palo Alto Networks, 2020). The attack disabled more than dozens of Canon US website, Canon's Email, Microsoft teams and many other applications. The list of Canon domains that affected in this attack are: (Abrams, 2020).

- www.canonusa.com
- www.canonbroadcast.com
- b2cweb.usa.canon.com
- canondv.com
- canobeam.com
- canoneos.com
- bjc8200.com
- canonhdec.com
- bjc8500.com
- usa.canon.com
- imagerunner.com
- multisport.com
- canoncamerashop.com
- canoncctv.com
- canonhelp.com
- bjc-8500.com
- canonbroadcast.com
- imageland.net
- consumer.usa.canon.com
- bjc-8200.com
- bjc3000.com
- downloadlibrary.usa.canon.com
- www.cusa.canon.com
- www.canondv.com

After claiming by the Maze group that they stole 10tb data from the system, According to Abrams, Canon sends an internal message to their employee "*Canon U.S.A, Inc. and its subsidiaries understand the importance of maintaining the operational integrity and security of our systems. Access to some canon systems is currently unavailable as a result of a ransomware incident we recently discovered. This is unrelated to the recent issue which affected image.canon*" (Abrams, 2020).

According to Bleeping Computer, Maze declined to share any information regarding proof of the stolen data, the total amount of devices that they encrypted and the ransom amount. Bleeping computer obtained a screenshot of the ransom note that Maze sends to Canon (Abrams, 2020).



```
Attention!
----------------------------
| What happened?
We hacked your network and now all your files, documents, photos, databases, and other important data are safely
encrypted with reliable algorithms.
You cannot access the files right now. But do not worry. You can get it back! It is easy to recover in a few steps.
We have also downloaded a lot of private data from your network, so in case of not contacting us as soon as
possible this data will be released.
If you do not contact us in a 3 days we will post information about your breach on our public news website and
after 7 days the whole downloaded info.
To see what happens to those who don't contact us, google:
* Southwire Maze Ransomware
* MDLab Maze Ransomware
* City of Pensacola Maze Ransomware
After the payment the data will be removed from our disks and decryptor will be given to you, so you can restore
all your files.
| How to contact us and get my files back?
The only method to restore your files and be safe from data leakage is to purchase a unique for you private key
which is securely stored on our servers.
To contact us and purchase the key you have to visit our website in a hidden TOR network.
There are general 2 ways to reach us:
1) [Recommended] Using hidden TOR network.
a) Download a special TOR browser: https://www.torproject.org/
b) Install the TOR Browser.
c) Open the TOR Browser.
```

Maze give seven days' time to the organization to pay the ransom in order to get the decryptor key and their data safe. In a short time, Canon is able to restore its systems and everyone think that they had paid the ransom. Unfortunately, everyone was wrong as after some days the Maze group started leaking the stolen data into its Darknet Website which is only done if the ransom is not paid. Maze published 2.2 GB of the stolen data, which is 5% of the total data. The published file is a zip file named as "SRATEGICPLANNINGpart62.zip". This file contains videos, marketing materials and some canon data related to website. File doesn't contain any personal data (Abrams, 2020d).

Canon ransomware attack is no different to cyber-attacks that took place before covid-19. In the last quarter of 2019, Allied Universal is the victim of Maze ransomware. Allied Universal is an American based firm which offers security systems and security staffing. The firm has almost 200,000 employees and has a net revenue of $7 billion. Maze got into organization system and stole data as they did in the case of Canon. Maze demands 300 bitcoins (approx. $2.3 million USD) to decrypt their network. Unfortunately, Allied Universal missed the deadline for paying the ransom then Maze published 700mb of stolen data (which is only 10% of the total data). Maze increase the ransom payment to $3.8 million USD and also stated that if the payment is not done on time, they will release the other 90% data. Allied Universal tried to negotiate with the Maze that they will not pay more than $50,000 USD (Abrams, 2019).

Nowadays majority of the things is depending on technology. No doubt that this modern technology has made our life easier but on the other hand our privacy and security is on the risk. Some of the important things we can do to protect yourself from cyber attacks can be: (Leaf, 2020)

- Always keep your system and software updated. Most cyber-attacks happen because your systems are not fully updated which can lead to weakness.

- Installing a firewall can be advantage. Putting your system behind a firewall is the best way to defend yourself from any type of attack.
- Always backup your important data. Backing up your data is the most important thing.
- Always have a strong and different password. Same password for everything can be very dangerous and helps the hacker to steal everything. Also change them regularly.
- Use latest virus- always use the latest virus like Quick Heal, Norton etc.
- Always check the URL of the website and make sure that you are accessing the right website.
- Always use trusted mail service like GMAIL, YAHOO
- Do not open link from the spam emails.
- Secure your Wi-Fi network and don’t connect your laptop or smartphone to an open or free Wi-Fi network.

To summarize, I would like to say that it's the time where almost everything is working remotely and businesses are facing major cyber-attacks. Smart and effective digital workforce is required to combat the cyber security threats that are occurring all around the globe. By taking appropriate measures we can protect the personal and sensitive information.

Reference List

1. Ico.org.uk. (2019b). *Controllers and processors*. [online] Available at: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/key-definitions/controllers-and-processors/ [Accessed 22 Oct. 2020].

2. Ico.org.uk. (2019l). *What is personal data?* [online] Available at: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/key-definitions/what-is-personal-data/ [Accessed 22 Oct. 2020].

3. Ico.org.uk. (2019l). *The principles*. [online] Available at: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/ [Accessed 222 Oct. 2020].

4. Ico.org.uk. (2019e). *Lawful basis for processing*. [online] Available at: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/ [Accessed 22 Oct. 2020].

5. ico.org.uk. (2020). *Collecting customer and visitor details for contact tracing*. [online] Available at: https://ico.org.uk/global/data-protection-and-coronavirus-information-hub/coronavirus-recovery-data-protection-advice-for-organisations/collecting-customer-and-visitor-details-for-contact-tracing/.

6. Ico.org.uk. (2019d). *Individual rights*. [online] Available at: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/ [Accessed 22 Oct. 2020].

7. General Data Protection Regulation (GDPR). (2013). *Art. 32 GDPR – Security of processing | General Data Protection Regulation (GDPR)*. [online] Available at: https://gdpr-info.eu/art-32-gdpr/ [Accessed 23 Oct. 2020].

8. itgovernance. (n.d.). *ISO 27001 and the GDPR*. [online] Available at: https://www.itgovernance.eu/en-ie/gdpr-and-iso-27001-ie?utm_campaign=youtube&utm_source=social&utm_medium=youtube [Accessed 23 Oct. 2020].

9. ISMS Online (2017). *ISMS Online*. [online] ISMS.online. Available at: https://www.isms.online/iso-27001/ [Accessed 23 Oct. 2020].

10. Leal, M.M. (2018). *GDPR and ISO 27001 Mapping: Is ISO 27001 Enough for GDPR Compliance?* [online] https://blog.netwrix.com/. Available at: https://blog.netwrix.com/2018/04/26/gdpr-and-iso-27001-mapping-is-iso-27001-enough-for-gdpr-compliance/ [Accessed 24 Oct. 2020].

11. Dutton, J. (2017). *How ISO 27001 can help to achieve GDPR compliance*. [online] IT Governance UK Blog. Available at: https://www.itgovernance.co.uk/blog/how-iso-27001-can-help-to-achieve-gdpr-compliance [Accessed 24 Oct. 2020].

12. Irwin, L. (2020). *5 steps to an effective ISO 27001 risk assessment*. [online] IT Governance Blog En. Available at: https://www.itgovernance.eu/blog/en/5-steps-to-an-effective-iso-27001-risk-assessment-2 [Accessed 24 Oct. 2020].

13. Ico.org.uk. (2019f). *Personal data breaches*. [online] Available at: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/personal-data-breaches/ [Accessed 24 Oct. 2020].

14. www.nibusinessinfo.co.uk. (n.d.). *GDPR data audit checklist | nibusinessinfo.co.uk*. [online] Available at: https://www.nibusinessinfo.co.uk/content/gdpr-data-audit-checklist [Accessed 25 Oct. 2020].

15. GDPR Associates. (2019). *Data Mapping and GDPR: How Are They Related?* [online] Available at: https://www.gdpr.associates/data-mapping-and-gdpr-how-are-they-related-2/ [Accessed 25 Oct. 2020].

16. Ico.org.uk. (2019c). *Data protection impact assessments*. [online] Available at: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-impact-assessments/ [Accessed 26 Oct. 2020].

17. Data Privacy Manager. (2020). *Pseudonymization according to the GDPR [definitions and examples]*. [online] Available at: https://dataprivacymanager.net/pseudonymization-according-to-the-gdpr/ [Accessed 26 Oct. 2020].

18. Groot, J.D. (2019). *What is Data Loss Prevention (DLP)? A Definition of Data Loss Prevention*. [online] Digital Guardian. Available at: https://digitalguardian.com/blog/what-data-loss-prevention-dlp-definition-data-loss-prevention [Accessed 26 Oct. 2020].

19. Andrada Coos (2017). *Top 5 Ways DLP can help with GDPR compliance*. [online] Endpoint Protector Blog. Available at: https://www.endpointprotector.com/blog/top-5-ways-dlp-can-help-with-gdpr-compliance/#:~:text=The%20GDPR%20states%20that%20processors [Accessed 26 Oct. 2020].

20. Abrams, L. (2020). *Canon confirms ransomware attack in internal memo*. [online] BleepingComputer. Available at: https://www.bleepingcomputer.com/news/security/canon-confirms-ransomware-attack-in-internal-memo/#employee. [Accessed 25 Oct. 2020].

21. Nair, P. (2020). *Canon USA Websites Offline Following Cyber Incident*. [online] www.databreachtoday.com. Available at: https://www.databreachtoday.com/canon-usa-websites-offline-following-cyber-incident-a-14777?highlight=true. [Accessed 25 Oct. 2020].

22. Kaspersky (2020). *Resource Centre | www.kaspersky.co.uk*. [online] Available at: https://www.kaspersky.co.uk/resource-center/definitions/what-is-ransomware. [Accessed 25 Oct. 2020].

23. Hope, A. (2020). *Canon Suffers a Maze Ransomware Attack Leaking Terabytes of Data*. [online] CPO Magazine. Available at: https://www.cpomagazine.com/cyber-security/canon-suffers-a-maze-ransomware-attack-leaking-terabytes-of-data/. [Accessed 25 Oct. 2020].

24. Imperva. (2020). *What is phishing | Attack techniques & scam examples | Imperva*. [online] Available at: https://www.imperva.com/learn/application-security/phishing-attack-scam/#:~:text=Phishing%20is%20a%20type%20of [Accessed 25 Oct. 2020].

25. Bond, R. (2020). *Why MAZE Ransomware Attacks are So Devastating*. [online] SecureOps. Available at: https://secureops.com/why-maze-ransomware-attacks-are-so-devastating/ [Accessed 25 Oct. 2020].

26. Abrams, L. (2020c). *Suspicious Canon outage leads to image.canon data loss*. [online] BleepingComputer. Available at: https://www.bleepingcomputer.com/news/technology/suspicious-canon-outage-leads-to-imagecanon-data-loss/. [Accessed 25 Oct. 2020].

27. Jay, J. (2020). *Canon suffers Maze ransomware attack, loses 10TB data to hackers*. [online] teiss. Available at: https://www.teiss.co.uk/canon-ransomware-attack/ [Accessed 25 Oct. 2020].

28. Cluley, G. (2020). *Maze Ransomware – What You Need to Know*. [online] The State of Security. Available at: https://www.tripwire.com/state-of-security/featured/maze-ransomware-what-you-need-to-know/ [Accessed 25 Oct. 2020].

29. Mark (2020). *How does the Maze Ransomware work? Blog*. [online] Galaxkey. Available at: https://www.galaxkey.com/blog/how-does-the-maze-ransomware-work/#:~:text=While%20most%20other%20forms%20of [Accessed 26 Oct. 2020].

30. Palo Alto Networks. (2020). *What is an Exploit Kit?* [online] Available at: https://www.paloaltonetworks.com/cyberpedia/what-is-an-exploit-kit [Accessed 25 Oct. 2020].

31. Abrams, L. (2020d). *Canon USA's stolen files leaked by Maze ransomware gang*. [online] BleepingComputer. Available at: https://www.bleepingcomputer.com/news/security/canon-usas-stolen-files-leaked-by-maze-ransomware-gang/ [Accessed 26 Oct. 2020].

32. Abrams, L. (2019). *Allied Universal Breached by Maze Ransomware, Stolen Data Leaked*. [online] BleepingComputer. Available at: https://www.bleepingcomputer.com/news/security/allied-universal-breached-by-maze-ransomware-stolen-data-leaked/ [Accessed 26 Oct. 2020].

33. Leaf. (2020). *10 Ways to Prevent Cyber Attacks*. [online] Available at: https://leaf-it.com/10-ways-prevent-cyber-attacks/ [Accessed 26 Oct. 2020].