School of Computer Science and Engineering
November, 2020

Information Security Analysis and Audit
CSE3501

Privacy Policy

Team Members

Kshitiz Choudhary: 18BCE0606
Princy Jain:18BCE0563
Vaani Tripathi:18BCE0693

INDEX

1. PURPOSE

1.1 The Institution will comply with all relevant legislation, particularly the Data Protection Act 1998, and base its policies and practices on compliance with the eight Data Protection principles contained therein.

1.2 Ensuring compliance is a corporate responsibility of the Institution requiring the active involvement of, and appreciation by, all staff at all levels of the organisation.

1.3 The company will strive to ensure best practice with regard to data protection and data security processes and procedures.

1.4 The company will strive to improve practices and procedures using external guidance, monitoring of jurisprudence in the relevant areas, and adopting examples of best practice elsewhere.

1.5 The Institution will provide support and services to enable staff handling personal data to remain compliant with the legislation and the Institution's requirements in respect of data security.

2. SCOPE

2.1 This policy document defines common security requirements for all personnel and systems that create, maintain, store, access, process or transmit information.

2.2 This privacy policy describes how the personally identifiable information user may provide on the server and any of its related products and services is collected, protected and used.

2.3 It also describes the choices available to you regarding our use of your Personal Information and how you can access and update this information.

2.4 This Policy is a legally binding agreement between the user and us. By accessing and using the company services, you acknowledge that you have read, understood, and agree to be bound by the terms of this Agreement.

2.5 This Policy does not apply to the practices of companies that we do not own or control, or to individuals that we do not employ or manage.

3. POLICY STATEMENTS

3.1 Automatic collection of information

When a user accesses the site, the servers automatically record information that your browser sends. This data may include information such as your device's IP address, browser type and version, operating system type and version, language preferences or the webpage .Information collected automatically is used only to identify potential cases of abuse and establish statistical information regarding the usage and traffic of the Website and Services. This statistical information is not otherwise aggregated in such a way that would identify any particular user of the system.

3.2 Collection of personal information

Users can access and use the company's site and services without telling us who you are or revealing any information by which someone could identify you as a specific, identifiable individual. If, however, you wish to use some of the features, you may be asked to provide certain Personal Information. We receive and store any information you knowingly provide to us when you create an account, publish content, or fill any online forms on the Website. When required, this information may include the following:

- Personal details such as name, country of residence, etc.
- Contact information such as email address, address, etc.
- Account details such as user name, unique user ID, password, etc.
- Geolocation data such as latitude and longitude.

Some of the information the company can collect is directly from you via the Website and Services. However, it may also collect Personal Information about you from other sources such as public databases and our joint marketing partners. Users who are uncertain about what information is mandatory are welcome to contact us.

3.3 Use and processing of collected information

In order to make the site and Services available to you, or to meet a legal obligation, companies need to collect and use certain Personal Information. If users do not provide the information, the company may not be able to provide you with the requested products or services. Any of the information collected from you may be used for the following purposes:

- Create and manage user accounts
- Send administrative information
- Respond to inquiries and offer support
- Request user feedback
- Improve user experience
- Respond to legal requests and prevent harm
- Run and operate the Website and Services

Processing your Personal Information depends on how you interact with the Website and Services, where you are located in the world and if one of the following applies:

(i) you have given your consent for one or more specific purposes; this, however, does not apply, whenever the processing of Personal Information is subject to European data protection law;

(ii) provision of information is necessary for the performance of an agreement with you and/or for any pre-contractual obligations thereof;

(iii) processing is necessary for compliance with a legal obligation to which you are subject;

(iv) processing is related to a task that is carried out in the public interest or in the exercise of official authority vested in us;

(v) processing is necessary for the purposes of the legitimate interests pursued by us or by a third party.

3.4 Managing information

Users are able to delete certain Personal Information. The Personal Information user can delete may change as the Website and Services change. When user delete Personal Information, however, we may maintain a copy of the unrevised Personal Information in our records for the duration necessary to comply with our obligations to our affiliates and partners, and for the purposes described below. If a user would like to delete your Personal Information or permanently delete the account, you can do so by contacting us.

3.5 Disclosure of information

Depending on the requested Services or as necessary to complete any transaction or provide any service you have requested, we may share your information with your consent with our trusted third parties that work with us, any other affiliates and subsidiaries we rely upon to assist in the operation of the Website and Services available to you. We do not share Personal Information with unaffiliated third parties. These service providers are not authorized to use or disclose your information except as necessary to perform services on our behalf or comply with legal requirements. We may share your Personal Information for these purposes only with third parties whose privacy policies are consistent with ours or who agree to abide by our policies with respect to Personal Information. These third parties are given Personal Information they need only in order to perform their designated functions, and we do not authorize them to use or disclose Personal Information for their own marketing or other purposes.

We will disclose any Personal Information we collect, use or receive if required or permitted by law, such as to comply with a subpoena, or similar legal process, and when we believe in good faith that disclosure is necessary to protect our rights, protect your safety or the safety of others, investigate fraud, or respond to a government request.

3.6 Retention of information

We will retain and use your Personal Information for the period necessary to comply with our legal obligations, resolve disputes, and enforce our agreements unless a longer retention period is required or permitted by law. We may use any aggregated data derived from or incorporating your Personal Information after you update or delete it, but not in a manner that would identify you personally. Once the retention period expires, Personal Information shall be deleted.

Therefore, the right to access, the right to erasure, the right to rectification and the right to data portability cannot be enforced after the expiration of the retention period.

3.7 The rights of users

You may exercise certain rights regarding your information processed by us. In particular, you have the right to do the following: (i) you have the right to withdraw consent where you have previously given your consent to the processing of your information; (ii) you have the right to object to the processing of your information if the processing is carried out on a legal basis other than consent; (iii) you have the right to learn if information is being processed by us, obtain disclosure regarding certain aspects of the processing and obtain a copy of the information undergoing processing; (iv) you have the right to verify the accuracy of your information and ask for it to be updated or corrected; (v) you have the right, under certain circumstances, to restrict the processing of your information, in which case, we will not process your information for any purpose other than storing it; (vi) you have the right, under certain circumstances, to obtain the erasure of your Personal Information from us; (vii) you have the right to receive your information in a structured, commonly used and machine readable format and, if technically feasible, to have it transmitted to another controller without any hindrance. This provision is applicable provided that your information is processed by automated means and that the processing is based on your consent, on a contract which you are part of or on pre-contractual obligations thereof.

3.8 Email marketing

We offer electronic newsletters to which you may voluntarily subscribe at any time. We are committed to keeping your e-mail address confidential and will not disclose your email address to any third parties except as allowed in the information use and processing section. We will maintain the information sent via e-mail in accordance with applicable laws and regulations.

In compliance with the CAN-SPAM Act, all e-mails sent from us will clearly state who the email is from and provide clear information on how to contact the sender. You may choose to stop receiving our newsletter or marketing emails by following the unsubscribe instructions included

in these emails or by contacting us. However, you will continue to receive essential transactional emails.

3.9 Links to other resources

The Website and Services contain links to other resources that are not owned or controlled by us. Please be aware that we are not responsible for the privacy practices of such other resources or third parties. We encourage you to be aware when you leave the Website and Services and to read the privacy statements of each and every resource that may collect Personal Information.

3.10 Information security

We secure information you provide on computer servers in a controlled, secure environment, protected from unauthorized access, use, or disclosure. We maintain reasonable administrative, technical, and physical safeguards in an effort to protect against unauthorized access, use, modification, and disclosure of Personal Information in its control and custody. However, no data transmission over the Internet or wireless network can be guaranteed. Therefore, while we strive to protect your Personal Information, you acknowledge that

(i) there are security and privacy limitations of the Internet which are beyond our control;

(ii) the security, integrity, and privacy of any and all information and data exchanged between you and the Website and Services cannot be guaranteed;

(iii) any such information and data may be viewed or tampered with in transit by a third party, despite best efforts.

3.11 Data breach

In the event we become aware that the security of the site and Services has been compromised or users Personal Information has been disclosed to unrelated third parties as a result of external activity, including, but not limited to, security attacks or fraud, we reserve the right to take reasonably appropriate measures, including, but not limited to, investigation and reporting, as well as notification to and cooperation with law enforcement authorities. In the event of a data breach, we will make reasonable efforts to notify affected individuals if we believe that there is a

reasonable risk of harm to the user as a result of the breach or if notice is otherwise required by law. When we do, we will post a notice on the Website, send you an email.

3.12 Changes and amendments

We reserve the right to modify this Policy or its terms relating to the Website and Services from time to time in our discretion and will notify you of any material changes to the way in which we treat Personal Information. When we do, we will revise the updated date at the bottom of this page. We may also provide notice to you in other ways at our discretion, such as through contact information you have provided. Any updated version of this Policy will be effective immediately upon the posting of the revised Policy unless otherwise specified. Your continued use of the Website and Services after the effective date of the revised Policy will constitute your consent to those changes. However, we will not, without your consent, use your Personal Information in a manner materially different from what was stated at the time Personal Information was collected.

3.13 Password Security

3.13.1 Requirements

1. All system-level passwords (Administrator, etc.) must be changed on a quarterly basis, at a minimum.
2. All user-level passwords (e.g., email, web, desktop computer, etc.) must be changed at least every six months.
3. All user-level and system-level passwords must conform to the standards described below.

3.13.2 Protective Measures

1. Do not share passwords with anyone, including administrative assistants or secretaries.
2. All passwords are to be treated as sensitive, confidential information.
3. Passwords should never be written down or stored on-line without encryption.
4. Do not reveal a password in email, chat, or other electronic communication.
5. Do not speak about a password in front of others.
6. Do not hint at the format of a password (e.g., “my family name”).

7. Do not reveal a password on questionnaires or security forms.
8. If someone demands a password, direct them to the IT department.
9. Always decline the use of the “Remember Password” feature of applications.

3.13.3 Passphrases

Access to the Networks via remote access is to be controlled using either a one time password authentication or a public/private key system with a strong passphrase.

1. A good passphrase is relatively long and contains a combination of upper and lowercase letters and numeric and punctuation characters. An example of a good passphrase: “Joe&Me1RBudz”.
2. All of the rules above that apply to passwords apply to passphrases.

4. RESPONSIBILITIES

4.1 Monitoring and Review

1. Privacy Officer (PO) : This Privacy Officer will oversee all ongoing activities related to the development, implementation, and maintenance of the company privacy policies in accordance with applicable federal and state laws.
2. Confidentiality / Security Team (CST): This team is made up of key personnel whose responsibility it is to identify areas of concern within the company and act as the first line of defense in enhancing the appropriate security posture. All members identified within this policy are assigned to their positions by the CEO. The term of each member assigned is at the discretion of the CEO, but generally it is expected that the term will be one year. Members for each year will be assigned at the first meeting of the Quality Council in a new calendar year. This committee will consist of the positions most responsible for the overall policy planning of the organization- the CEO, PO, CMO, ISO, and the CIO (where applicable).
3. CISO: He ensures that the correct resources are in place to adhere to the policies and procedures set forth by the steering committee.
4. Policy amendment and advisory committee: This committee has an important role in security governance; this group is responsible for setting the tactical and strategic direction for the organization as a whole.
5. Security Director: This role also acts as a liaison to other aspects of the business to articulate security requirements throughout the company. The security director manages the teams in developing corporate data security policies, standards, procedures, and guidelines.
6. Security Analyst: A security analyst builds the policies, analyses risk, and identifies new threats to the business. The analyst is also responsible for creating reports about the performance of the organization’s security systems.
7. Systems Administrator: A systems administrator is responsible for monitoring and maintaining the servers, printers, and workstations a company uses. In addition,

administrators add and/or remove user accounts as necessary, control access to shared resources, and maintain company-wide software.

4.2 Reporting

4.2.1 No additional reporting is required

4.2.2 Detection

Users should inform the appropriate company personnel when the user's software does not appear to be functioning correctly. The malfunction - whether accidental or deliberate - may pose an information security risk. Inform the appropriate personnel or ISO as soon as possible. Write down any unusual behavior of the computer (screen messages, unexpected disk access, unusual responses to commands) and the time when they were first noticed. Write down any changes in hardware, software, or software use that preceded the malfunction. The ISO should monitor the resolution of the malfunction or incident, and report to the CST the result of the action with recommendations on action steps to avert future similar occurrences.

4.2.3 Penalties

Any person found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

4.3 Records Management

Staff of XYZ must maintain all records relevant to administering this policy in the ERP (Enterprise Resource Planning) or on company recognised Company record keeping systems.

5. DEFINITION

The following definitions apply to this policy:

5.1 Data security breach: Any occurrence of any unauthorised or unlawful processing of personal data held by the company XYZ, or the accidental loss, destruction of or damage to any such personal data.

5.2 Data subject: A living individual who is the subject of personal data.

5.3 Data controller: A person or organisation which controls the purposes and manner in which data are processed. The XYZ is a data controller, and the point of contact is the CEO.

5.4 Data processor: Any person or persons that process information on behalf of a data controller.

5.5 Data: All information in digital format, or manual data within a 'relevant filing system'.

5.6 The Information Commissioner (ICO): The supervisory authority, reporting directly to Parliament, that enforces the policy, and other information related legislation. The ICO maintains a public register of data controllers. The process of adding an entry to the register is called notification. The user's notification covers the classes of data which are processed, and is updated from time to time.

5.7 Information life cycle: The time span that information processed by the company remains 'live' and relevant to the Institution (inclusive of its disposal or destruction) and for which the Institution has obligations under this, or any other policy.

5.8 Personal Information: Data which relate to a living and identifiable individual, including computerised data and some manual data .Personnel records are clearly part of

a "structured filing system" as they are arranged by surname or employee number. However, a member of staff may serve on a committee, and that person's name will appear in the minutes of that committee. The minutes are not structured by names, but by the dates of committee meetings.

5.9 Processing: An action of any sort taken in regards to personal data during the lifecycle of that personal data. This will include but is not limited to, obtaining, storing, adapting, transferring, transmitting, disposal and destruction.

5.10 Relevant filing system: Any set of information relating to individuals to the extent that, although the information is not processed by means of equipment operating automatically in response to instructions given for that purpose, the set is structured, either by reference to individuals or by reference to criteria relating to individuals, in such a way that specific information relating to a particular individual is readily accessible.

5.11 Sensitive personal data: The company recognises that certain types of personal data should be treated with particular regard. Such data include racial or ethnic origin; political opinions; religious beliefs; membership of a trade union; physical or mental health or condition; sexual life; and criminal offences.

6. RELATED LEGISLATION AND DOCUMENTS

Currently, India does not have comprehensive and dedicated data protection legislation. Some provisions of the Information Technology Act, 2000, as amended from time to time ("**IT Act**") and the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 ("**SPDI Rules**") framed under it deal with protection of personal information ("**PI**") and sensitive personal data and information ("**SPDI**").

There has been considerable traction with regard to data protection in recent times. The Government recently presented the Personal Data Protection Bill, 2019 ("**PDP Bill**") in Parliament and it is currently pending consideration before a Joint Parliamentary Committee. Although the PDP Bill has not been enacted, it is expected that it will soon see the light of day; we have therefore also touched upon its provisions as part of our responses to the questions below (on the assumption that it will be enacted in its present form), for the sake of completeness.

For example, in the UK, a list of relevant legislation would include:

- The Computer Misuse Act (1990)
- The Data Protection Act (1998)
- The Data Protection (Processing of Sensitive Personal Data) Order (2000)
- The Copyright, Designs and Patents Act (1988)
- The Computer Misuse Act (1990)
- The Human Rights Act (1998)

7. FEEDBACK

If a user would like to contact us to understand more about this Policy or wish to contact us concerning any matter relating to individual rights and their Personal Information, they may send an email to privacypolicy@XYZ.org.

Company staff and third party members may provide feedback about this document by emailing to privacypolicy@XYZ.org.

8. APPROVAL AND REVIEW DETAILS

Approval and Review	Details
Approval Authority	Chief Information Security Officer (CISO)
Advisory Committee to Approval Authority	[Relevant advisory committee, e.g. Learning and Teaching Committee]Policy amendment and advisory committee
Administrator	Security Director
Next Review Date	Nov 1st,2020

Approval and Amendment History	Details
Original Approval Authority and Date	[Relevant approval authority and first approved date DD/MM/YYYY] Security Analyst and Sep 14, 2020
Amendment Authority and Date	[Relevant approval authority DD/MM/YYYY]; [Policy Portal Administrator adds the latest amendment information.] Systems Administrator and Oct 15,2020
Approval Date	Oct 1, 2020

9. APPENDIX

9.1 Background Work:

- **Case Study 1: Wiper**

A piece of malware referred to as "Wiper" was allegedly used in attacks against Iranian oil companies. In 2012, the International Telecommunication Union supplied Kaspersky Lab with hard drives allegedly damaged by Wiper for analysis. While a sample of the alleged malware could not be found, Kaspersky discovered traces of a separate piece of malware known as Flame.The Shamoon malware contained a disk wiping mechanism; it was employed in 2012 and 2016 malware attacks targeting Saudi energy companies, and utilized a commercial direct drive access driver known as Rawdisk. The original variant overwrote files with portions of an image of a burning U.S. flag. The 2016 variant was nearly identical, except using an image of the body of Alan Kurdi instead. A wiping component was used as part of the malware employed by the Lazarus Group—a cybercrime group with alleged ties to North Korea, during the 2013 South Korea cyberattack, and the 2014 Sony Pictures hack. The Sony hack also utilized RawDisk. In 2017, computers in several countries—most prominently Ukraine, were infected by a variant of the Petya ransomware, which had been modified to effectively act as a wiper. The malware infects the master boot record with a payload that encrypts the internal file table of the NTFS file system. Although it still demanded a ransom, it was found that the code had been significantly modified so that the payload could not actually revert its changes if the ransom were successfully paid.

- **Case Study 2: Deloitte Email hack**

In September 2017, The Guardian reported that Deloitte suffered a cyberattack that breached the confidentiality of its clients and 244,000 staff, allowing the attackers to access "usernames, passwords, IP addresses, architectural diagrams for businesses and health information". Reportedly, Deloitte had stored the affected data in Microsoft's Azure cloud hosting service, without two-step verification. The attackers were thought to possibly have had access from as

early as October 2016. Brian Krebs reported that the breach affected all of Deloitte's email and administrative user accounts. A later report by The Wall Street Journal repeated Deloitte's statement that only a few clients were affected. Deloitte said that neither its services nor its clients' businesses were disrupted. Deloitte reportedly first noticed suspicious activity in April 2017. Deloitte said that no sensitive information was compromised and that its investigators were eventually able to read every email obtained by the hackers.

- **Case Study 3: Moonlight Maze**

Moonlight Maze was a 1999 US government investigation into a massive data breach of classified information. By the end of 1999, the Moonlight Maze task force was composed of forty specialists from Law Enforcement, Military, and Government.The investigators claimed that if all the information stolen was printed out and stacked, it would be three times the height of the Washington monument (which is more than 550 ft tall). The Russian government was blamed for the attacks, although there was initially little hard evidence to back up the US' accusations besides a Russian IP address that was traced to the hack. Moonlight Maze represents one of the first widely known cyber-espionage campaigns in world history. It was even classified as an Advanced Persistent Threat (a very serious designation for stealthy computer network threat actors, typically a nation state or state-sponsored group) after two years of constant assault. Although Moonlight Maze was regarded as an isolated attack for many years, unrelated investigations revealed that the threat actor involved in the attack continued to be active and employed similar methods until as recently as 2016.

- **Case Study 4:Facebook–Cambridge Analytica Data Scandal**

This is regarding the data breach scandal involving Facebook.In March 2018, Facebook was caught in a major data breach scandal in which a political consulting firm – Cambridge Analytica – pulled out the personal data of more than 87 million Facebook users without their consent. The firm offered tools that could identify the personalities of American voters and influence their behavior.The data collected from user includes details on identities ,friend networks and likes basically to map personality traits and use it to target audiences with digital ads.Users were made

to install an app for a personality survey which scraped their personal information which was permitted by facebook then.This technique had been developed at Cambridge University's Psychometrics Center. Facebook said no passwords or "sensitive pieces of information" had been taken, though information about a user's location was available to Cambridge.Facebook stated that what Cambridge did was not a data breach, because it routinely allows researchers to have access to user data for academic purposes.

- **Case Study 5: LinkedIn Breach: Worse Than Advertised**

LinkedIn.com was hacked in June 2012, and a copy of data for 167,370,910 accounts has been obtained by LeakedSource In fact, the quantity of credentials suggests that attackers obtained virtually every LinkedIn username and hashed password. A hacker stole 6.5 million encrypted passwords from the site and posted them to a Russian crime forum. Now it appears that data theft was just the tip of the iceberg. Leaked Source says, noting that it purchased the credentials for 5 bitcoins on the dark web forum "The Real Deal" from a seller using the handle "Peace." It also claims that it's now cracked nearly all of the hashed passwords. LinkedIn has never confirmed how many user credentials were compromised, or if it even knows. In 2012, the company did confirm that passwords had been stolen, and noted that it had failed to salt those passwords, which makes them harder to crack. LinkedIn had also been using SHA1 to hash the passwords, which security experts have long warned is not fit for securing passwords. LinkedIn apologized immediately after the data breach , and asked its users to immediately change their passwords.As of 8 June 2012, the investigation was still in its early stages, and the company said it was unable to determine whether the hackers were also able to steal the email addresses associated with the compromised user accounts as well.

- **Case Study 6:ASHLEY MADISON HACK**

In July 2015, a group calling itself "The Impact Team" stole the user data of Ashley Madison, a commercial website billed as enabling extramarital affairs. The Impact Team threatened to expose the identities of Ashley Madison's users if its parent company, Avid Life Media, did not shut down Ashley Madison and its sister site, "Established Men". A categorical breakdown of the email addresses disclosed in the first data dump is posted to Pastebin, revealing many

government, military, and corporate addresses that were used to sign up for Ashley Madison accounts. After a nearly day-long media frenzy met with much speculation over the validity of the leaked data, Brian Krebs discloses that numerous Ashley Madison account holders have confirmed that their information was published.None of the accounts on the website need email verification for the profile to be created, so people often create profiles with fake email addresses. Ashley Madison's company required the owner of the email account to pay money to delete the profile, preventing people who had accounts set up. against their consent from deleting them without paying. Hackers allege that Avid Life Media received $1.7 million a year from people paying to shut down user profiles created on the site. The company falsely asserted that paying them would "fully delete" the profiles, which the hack proved was untrue.

- **Case Study 7: City of Baltimore Discloses Data Loss From Ransomware Attack**

Hackers successfully infiltrated systems operated by the City of Baltimore last year in May. The attackers encrypted data files and demanded a ransom in exchange for the decryption keys. Mayor Bernard C. “Jack” Young refused to pay and IT leaders were instructed to rebuild the municipality’s computer systems. City of Baltimore officials placed a price tag of $18 million on the estimated cost of the ransomware attack. In August, city leaders voted to divert $6 million of parks and recreation funding to IT “cyber-attack remediation and hardening of the environment,” according to the city’s spending panel known as the Board of Estimates.

- **Case Study 8: Western Connecticut School District Hit With Second Ransomware Attack**

It is unfortunate when a ransomware attack occurs. And it is nearly unfathomable that a second attack would even be a consideration. However, Wolcott Public Schools in Connecticut finds its school district in this predicament. In June of last year, the school district was hit with a ransomware attack. The cyber hijackers requested $12,000 to release the encryption keys though the school board has not been paid for it. Reports in the Hartford Courant say that Wolcott Public Schools noticed suspicious activity in the district’s computer systems in early September of last year.

- **Case Study 9: City of Albany Shares Costs For Overtime, System Upgrades And Professional Services**

In March of last year, the city of Albany, New York had its computer systems shut down when a ransomware attack locked its data. Details have not been shared about the ransom amount requested to release the data. WNYT, an Albany news channel, requested the city disclose details of expenditures associated with the ransomware attack. City officials responded with a cost of $161,000 related to employee overtime for re-entering lost data, hardware and software system upgrades, credit monitoring services for city employees and professional cyber security services. The amounts differ from the $300,000 that Mayor Kathy Sheehan shared during an event.

9.2 References

1. https://www.wired.com/2015/08/happened-hackers-posted-stolen-ashley-madison-data/
2. https://www.bankinfosecurity.com/linkedin-breach-worse-than-advertised-a-9113
3. https://www.cshub.com/attacks/articles/top-cyber-security-breaches-an-overview-of-q2-2020-incidents
4. https://en.wikipedia.org/wiki/Ashley_Madison_data_breach
5. https://www.cshub.com/attacks/articles/
6. https://www.icmrindia.org/casestudies/catalogue/Business%20Ethics/Cambridge%20Analytica-Excerpts.htm#CAMBRIDGE%20ANALYTICA
7. https://en.m.wikipedia.org/wiki/Wiper_(malware)
8. https://en.m.wikipedia.org/wiki/Moonlight_Maze
9. https://en.wikipedia.org/wiki/Deloitte#E-mail_hack