Data Recovery and Advanced Digital Forensic Analysis

Module: STW318SE

BYOD Policy And Investigation Methodology

Submitted to: Mr. Ganesh Bhushal CUID: 10176391

Submitted by: Niraj Sangraula SID: 190228

Submission deadline: 20th Feb, 2022

Acknowledgement

This semester has been a blast as I learned about many digital forensic tools and their practical usage in day-to-day life from this module (STW318SE), from Mr. Ganesh Bhushal. Not only him, but I'm also grateful to my college Softwarica College for providing this subject, **Advanced digital forensics**. I got to know about various things that have enhanced my knowledge and understanding of forensics, international laws and so on through this final assignment of the subject.

Abstract

As the present BYOD policies weren't holding up well for the school, I have drafted a solid foundation of new BYOD policies, which covers all areas in this document by discussing with all the parties, i.e., staff, school administration, parents and students. Not only that, but in this document, you will also find GDPR Policies that play an essential role in the life cycle of an individual's privacy, organization data, misuse of one's data and so on. Similarly, this document has also discussed devices' seizure and examination process by following ACPO and SWGDE principles. You will also find the procedures to follow before the seizure and examination phase here in the document and about extraction guidelines after seizing evidence.

Table of Contents

Table of Figures

Introduction

I was hired as a digital forensic investigator for this school to make a solid BYOD policy as the current BYOD policies of this school weren't holding up and instead getting breached. Take all the views of staff, administration, parents and students into consideration. Most importantly, following GDPR policies, a new set of BYOD policies were formed, which should stop the downgrading reputation of the school. Similarly, ACPO and SWGDE guidelines were also followed as a legal reference for seizure and examination of devices used by the parents, students and, most notably, staff. These guidelines should help the information technology manager of this school to determine whether the school staffs are guilty or not. Individual privacy and data aren't compromised as GDPR guidelines are written efficiently.

Purpose

The purpose for drafting this document is to ensure that the GDPR guidelines to be followed properly when handling student, parents and mainly staffs data by the school. Furthermore, by introducing GDPR in this document I want to aware the school about the current data privacy. Similarly, by introducing SWGDE and ACPO I want to notify the school investigators what standard and guideline to follow when seizing and examining found evidence keeping privacy in check. The school can punish the staffs if they are found to be violating school rules according to legal and BYOD (bring your own device) compliances which are written in below sections.

SWGDE

Scientific Working Group on Digital Evidence or simply SWGDE provides guidelines, principles and standard for digital forensics evidence collection and handling, equipment preparation, evidence examination and so on. SWGDE standard and guidelines is followed all over the world by forensic community as it provides consistency and quality in evidence handling since 1998. Although it is US based organization it's standard is followed all over the world as it has been approved by International Organization on Computer Evidence (IOCE). So, it used by most forensics' investigators all around the world for evidence handling and for other purposes. In our case too this standard was needed for seizure and examination guidelines. SWGDE standard is

also used in this document for evidence collection and evidence handling processes. (Focus, 2020)

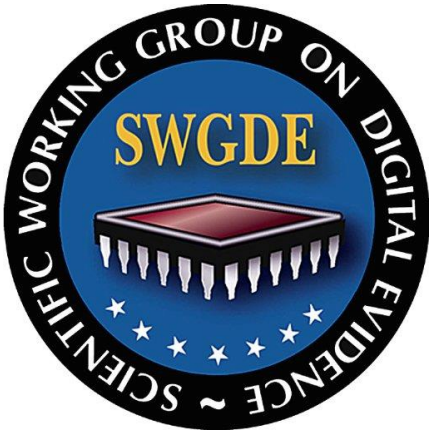

Figure 1 SWGDE logo

ACPO

ACPO (Association of Chief Police Officers) is one of the best practiced guidelines on digital evidence all over the world. Whenever there are computer-based evidences are involved, forensic experts adhere to ACPO guidelines. The digital forensic and technology community is changing day by day so the existing four main principles of ACPO isn't holding the current challenges faced during evidence handling for forensic practitioners. So, a new set of revised principles should be proposed in the upcoming summit to hold up the problems faced by forensic practitioners. (Horsman, 2020)

Despite so the current existing 4 main principles (in my own word) are summarized as:

- The investigating officer shouldn't do any unnecessary action that may change the originality of the digital evidence as it may later need to be submitted in the court of law.
- If the investigating officer finds it necessary to access the original digital evidence, then he/she should be an expert and capable to do so. Later on, in the court of law he/she should be competent enough to justify the action they did.
- The investigating officer shouldn't neglect their duties and keep track and records of their every action that they performed when handling digital evidence properly. If any other officer or another party analyze those records kept by you, they should get into the same conclusion.
- The investigating officer in charge must ensure that all these mentioned principles are followed.

These four principles must be followed during seizure and examination phase by the school investigator.

Figure 2 ACPO logo

GDPR

GDPR (GENERAL DATA PROTECTION REGULATION) is the primary law that protects individuals' privacy and regulates on data protection. GDPR is agreed by all member states in the EU and followed by all organization within the EU. Companies or organization within the EU should comply under EU if they don't and start to breach one's privacy then those companies have to pay heavy fines and penalties. So, organization cannot use one's data however they like.

So, the school also should comply to GDPR guidelines and be careful when handling staffs, parents and students' data. There are many guidelines, principles and articles when it comes to GDPR but the most needed one in our case that concerns about handling of collected data of individuals and the right provided to them are written below:

- GDPR Article 5 (1) (a) ensures that the collected data should be processed transparently, fairly and lawfully.
- GDPR Article 5 (1) (b) ensures that the collected data should be used for the original purpose or as it was said during the time of collection and shouldn't be used for other purposes.
- GDPR Article 5 (1) (f) ensures that the collected data by the company should be processed in such a manner that it doesn't neglect the security of their personal collected data.
- GDPR Article 12 ensures that the subject "Right to be informed" by the data controller whenever the subject's data is being examined.
- GDPR Article 13 and 14 ensures that an individual has right to access their data kept by the company.
- GDPR Article 16 ensures that an individual has the right to rectify their data kept by the company or even erase it.
- GDPR Article 20 ensures that an individual has the right to get copy of their own data.

So, the guidelines provided here shouldn't be violated or the school may face legal charges through GDPR. (*General Data Protection Regulation (GDPR) – Official Legal Text* n.d.)

Figure 3 GDPR logo

Introduction of BYOD policy and it's necessity

BYOD (Bring Your Own Device) policy is simply a set of rules that defines how a staff working in an organization should use their personal electronic devices such as mobiles, laptops, smart watches and so on within the workplace boundaries of the organization. Within BYOD policy staffs can bring their own personal gadgets in their respective organization and work from it which saves time and money. BYOD policy says that only work-related things should be done with the electronic devices and no personal works should be done from them. BYOD has its own advantages and disadvantages but more than negative side it has positive side. BYOD policy is necessary in the modern world as it has some of these advantages:

- The company doesn't need to buy hardware components in large bulk and place it in their premises as employees use their own device.
- It has been found that with BYOD policy the workflow and productivity of the employees increases due to adaptiveness of personal stuffs.

- The company also doesn't need to hire a new set of employees for device management as the employees themselves manage their device if problems occur. (Botha, 2021)

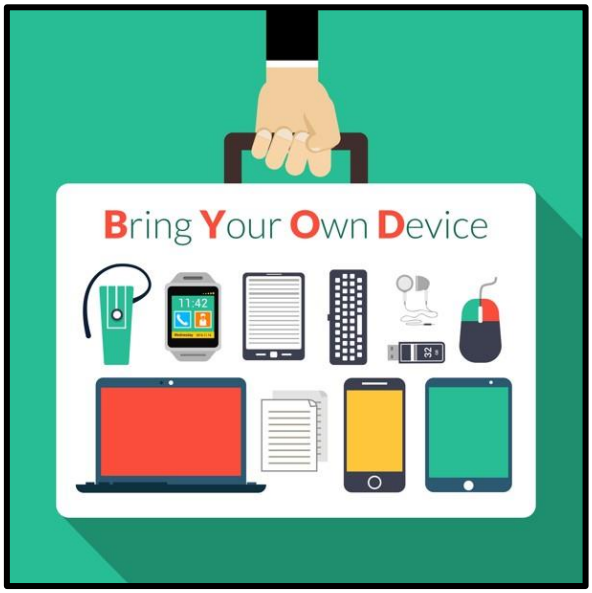

Figure 4 BYOD policies

A generic and security policies

BYOD policy help on determining how an employee should use their personal electric devices and what activities they do with it staying at the company premises or when connecting to company network. This school too has old BYOD policy but it isn't holding up with the new set of challenges of the modern world. And the staffs are continuing on breach it. So, it is revised under generic and security section or policies of this document which is given as:

Generic policies

- Devices used within the school premises that are the connected to the school network will be observed and monitored.
- If the device owner feel that they are targeted and monitored heavily then they can object by keeping the rules that they signed for in their mind.
- The school have the right to access the data collected for investigation and examining purposes.
- If the individual needs their copy of the data, then they need to write a letter to the information technology manager.
- The school won't tolerate if the employees are using apps that aren't approved by the school.
- The school won't tolerate if the employees are selling proprietary related data of the school to the highest bidder or third parties.
- Taking pictures and videos of not allowed zone within the school premises is prohibited.
- The employees aren't allowed to harass, do fraud, bully, illegal activities and so on with their owed devices.

Security policies

- The employees are prohibited for using rooted or jailbreaked phones.
- If the employees are using storage medium like pendrive or hard drive then they should be password protected.
- Systems should be automated so that display power can be turned off automatically within 30 sec of the device inactivity.
- Mobile phones and laptops should be password or pin protected.
- If possible, the files and folders on devices should be encrypted.
- The school can wipe out the data from individual device if they are found to be violating BYOD policy.
- Any device that is connected with the school network is subjected to BYOD policy so when the individual is asked to submit their devices after finding suspicious activity to the investigating officer they should do so willingly.
- The employees aren't allowed to visit uncertified website, down third-party apps and so on with their owned devices. (*Bring Your Own Device: Benefits And Risks | Nibusinessinfo.Co.Uk* n.d.)

Small Guidelines for parents/students

- Any form of misconduct such as hacking the college network for unauthorized use by the students will subject to suspension or even expulsion.
- Students are only allowed to use their devices for educational purposes in their respective classes.
- Students aren't allowed to use vpn to unblock restricted sites.
- If in case of damage, lost or theft of devices of students within or outside school premises then the parents can't blame the school wholly and take legal action against the school.
- Parents will be called if the devices are used by the students for entertainment purposes.

Investigation Methodology

All devices aren't investigated in the same way. Laptop need to be investigated in a certain way; mobile devices need to be investigated in a certain way. Even seizing and examination process of devices are different. Most of devices state also determines how they need to be investigated. So, the seizing and examination process guidelines isn't written in this document in a random way as ACPO and SWGDE principles and standards are followed. So, the authorities of the school need to follow the given seizure and examination process in this document to seize the suspected person device and examine it to find out more.

Seizure Process

- Examiners should be trained in accordance to "SWGDE/SWGIT Guidelines & Recommendations for Training in Digital & Multimedia Evidence." (*SWGDE Best Practices For Computer Forensics* 2013)
- Take necessary precaution to protect the evidence from dangerous substances and possible environmental harm like: dust, sun etc.
- Take multiple pictures of the found evidences from different angles. Also keep in mind to mainly focus to take pictures of the powered-on devices.
- Make sure to do labeling of all the cables found at the crime scene.

- Look at the surrounding carefully as you may found passwords of the devices as the school as enabled BYOD policy. So, people tend to write it off near their surroundings.
- According to the order of volatility seize evidence. So, seize memory first rather than storage devices. Also, doing imaging consider order of volatility. If possible, also generate hash values. (Forensics, 2016)
- If the device is powered off then put it in the Faraday bag as some bags have charging functionality. Furthermore, these bags help to prevent data modification.
- When mobile devices are found put it on flight mode it helps to solve battery drainage problem and also remove sim cards and put it in a faraday bag as it blocks wireless connection.
- If error occurs when you are doing your work then document that error. Not only that document your each and every step taken during seizing process. (*Best Practices For Seizing Electronic Evidence* n.d.)

Examination Process

- Examiners should be trained in accordance to "SWGDE/SWGIT Guidelines & Recommendations for Training in Digital & Multimedia Evidence." (*SWGDE Best Practices For Computer Forensics,* 2013)
- Conducting examination on the original evidence shouldn't be done instead examination process should be carried out on the forensic images.
- Examiners should review the documentation made during seizure process and determine which process to take to properly complete the examination.
- Examiners should properly be familiar with legal compliances i.e., GDPR, ACPO and SWGDE.
- Examiners should be familiar with vast majority of forensic tools and commands and should know what tools to use on what platform, what commands to use on which OS.
- Using third party software and tools should be avoided and only licensed tools should be used during examination.
- The evidences found should be examined in such a way that a third party should conclude the same result.
- Keep records of the images, videos, SMS and so on found in mobile devices and analyze them.
- The perpetrator might have done sandboxing, stenography and may have used other anti-forensic technique on the found mobile devices so the examiner should be competent enough to not to get derailed.

After the examination process is done the examiner can prepare a complete documentation which can be presented in the court of law. So, the school administration can get into conclusion after examination process is carried out and determine whether the suspected individuals are guilty of misconduct or not.

Disclaimer

The guidelines, policies and legal compliances presented in this document has been agreed by all the parties i.e., staffs, school administration, parents and students. So, any devices used within the school premises are subjected to the presented compliances. Even outside the premise if the devices are connected with the school network, then it is subjected with the school rules and compliances. This document is no means a final version but a draft that has to be agreed and signed by all parties in the school.

Conclusion

So, a document on different guidelines and standards was drafted. Legal compliance such as GDPR restricts the organization from freely using individual data and being more transparent about it. At the same time, ACPO and SWGDE tell us about standards and guidelines on handling digital equipment and data and also help us during the seizure and examination phase. The BYOD policy of the school wasn't holding up, so a new set of revised policies were prepared, which should help the school for better productivity and efficiency. Finally, this document is prepared by keeping best practices followed worldwide in mind, which should help the investigating officer later on.

References

Focus, F., 2020. *Community In Collaboration: The Scientific Working Group On Digital Evidence - Forensic Focus*. [online] Forensic Focus. Available at: https://www.forensicfocus.com/articles/community-in-collaboration-the-scientific-working-group-on-digital-evidence/ [Accessed 17 February 2022].

Horsman, G. (2020) "ACPO Principles For Digital Evidence: Time For An Update?". *Forensic Science International: Reports* [online] 2, 100076. available from https://www.sciencedirect.com/science/article/pii/S2665910720300220 [17 February 2022].

General Data Protection Regulation (GDPR) – Official Legal Text (n.d.) available from https://gdpr-info.eu/ [17 February 2022].

Botha, C. (2021) *BYOD Policy: A Step-By-Step Guide On How To Set It Up* [online] available from https://www.dialpad.com/blog/byod-policy/?experiment=3022&variant=2 [17 February 2022].

Forensics, C. (2016) *Order Of Volatility - Computer Forensics Recruiter* [online] available from https://www.computer-forensics-recruiter.com/order-of-volatility/ [17 February 2022].

Adv Prashant Mali, P. (2021) *Guidelines For Search & Seizure Of Electronic Devices By Police : Karnataka HC Case Law* [online] available from https://cyberandprivacylawyer.blogspot.com/2021/06/guidelines-for-search-seizure-of.html [17 February 2022].

Best Practices For Seizing Electronic Evidence (n.d.) 4th edn. available from https://www.cwagweb.org/wp-content/uploads/2018/05/BestPracticesforSeizingElectronicEvidence.pdf [17 February 2022].

SWGDE Best Practices For Computer Forensics (2013) 3rd edn. available from https://athenaforensics.co.uk/wp-content/uploads/2019/01/SWGDE-Best-Practices-for-Handling-Damaged-Hard-Drives-090514.pdf [17 February 2022].

Bring Your Own Device: Benefits And Risks | Nibusinessinfo.Co.Uk (n.d.) available from https://www.nibusinessinfo.co.uk/content/bring-your-own-device-benefits-and-risks [17 February 2022].