Introduction

Due to rapid increase covid19 cases, there are potential risks that have been accelerated and turbocharged by the pandemic while collecting data during this pandemic. The following report discusses the standard operating procedures and types of risk associated during collection of data during this uncertain times and further it discusses the best practices to comply with ISO 27001.

Standard set of procedures

The key steps or standard set of procedures while one needs to think of during data collection keeping potential risks in mind during this uncertain times are as follows:

1. The first thing to think of is what are the types of risks associated and risks to the common people during the collection of data?
2. Are there any solutions to above risks to make sure that no harm principle is honored during data collection?
3. If the answer is yes to above 2nd point, then what are the steps or measures taken during the whole process of data collection to make sure we do not harm anyone?
4. If the answer is no to 2nd point, then what are the steps or measures to confirm remote collection of data is as robust as possible?

In line with above protocols as shown above, we structure the steps as follows:

Assessment of risks

Examine the risks associated while collecting the data during uncertain times of pandemic to make sure protection of common, local people. Privacy rights risks and cybersecurity risks have been during the pandemic. The potential risks associated with each of them are as follows:

Potential risks with privacy rights:

1. Privacy data exploitation.
2. Differentiation of the people who are infected.
3. Bounded or restricted access to technologies and the internet.
4. Taking disadvantage of contact tracing apps.
5. Surveillance at the workplace.
6. Current rules that does not include the changes seen in collection of data during the pandemic.

Potential risks with cybersecurity:

1. Violation of data.

2. Disturbance in operations.
3. Newly built regulations on privacy and cyber security.
4. As remote working been increased, vulnerabilities regarding digital infrastructure increased.

Recommended ways to assess the risk factor based on type of data gathering

There are three ways that can help assess the risk while collecting data which are categorized as follows:

1. High Risk.
2. Medium Risk.
3. Low Risk.

The aim behind this ways of assessment of risks is to ensure 'duty of care' and 'not to harm'. the below table shows recommendation on collection of data based on three things such as analysis in context of operation, not to harm analysis and duty of care analysis. It is evaluated on per risk category. To give an example, if analysis in context of operation and duty of care analysis are categorized as low risk while not to harm analysis is categorized as high risk then the whole data collection should be tag as high risk.

Level of risk	Analysis in context of operation	Duty of care analysis	Not to harm analysis	Data collection type
Low risk	no cases at all at country level, less than 100 cases	Restriction on travel by public transport or not to share cab to go to work, Workforce is not from the areas affected by diseases, Workforce know the risks regarding coronavirus and the preventive measures associated with that.	Workforce don't show symptoms of coronavirus, Workforce restricted travel to areas which are affected, workforce not been in contact with positive individuals	Physically (Face to Face)
Medium risk	There are many cases in clusters specific to certain area, Established cases in the area where collection of data to be take place, successful implementation of physical distancing and prevention of	Workforce is from the area affected by diseases, workforce strictly follows social distancing measures while travelling through public transport or by cab to go to work, Workforce know the risks	Workforce don't show symptoms of coronavirus, workforce not been in contact with positive individuals, workforce been to areas which are infected. However they followed rules of quarantine for	Remote

	infection to prevent spread.	regarding coronavirus and the preventive measures associated with that.	fourteen days after which not found any symptoms of coronavirus.	
High risk	There is large outbreak of transmission locally with more than hundred cases	Workforce is from the area affected by diseases, workforce travels by public transport or shares a cab to go to work, Workforce does not know the risks regarding coronavirus and the preventive measures associated with that.	Workforce don’t show symptoms of coronavirus, workforce been in contact with the ones who tested positive, workforce recently visited infected areas	remote

The following below table categories risk based on cybersecurity domain:

Name of asset	confidentiality	integrity	availability	Overall risk impact	threats	Treatment or controls
laptop	Medium risk	Medium risk	Medium risk	Medium	Potential violation of information if stored in a local place, additionally hacking is one of the threat to the system	If not have antivirus installed, install the antivirus and update the antivirus if already have
website on mobile if used for covid reated jobs	medium risk	medium risk	medium risk	medium risk	Hacking or may be malware threat	Two factor authentication, antivirus update
Data storage as we are working	Medium risk	Medium risk	Medium risk	Medium risk	Violation of confidential information that would violate the	Privacy of data should be top most priority and store safely.

from home	🟧	🟧	🟧	🟧	rules of gdpr	
Wifi network As working from home	High risk	High risk	High risk	High risk	Hacking or may be malware threat	Scanning the network through antivirus to ensure it is secure and update anivirus

Contact tracing and surveillance:

For the sake of contact tracing, many businesses are collecting personal information. But they are advised to follow following steps while collecting data which is personal:

1. Only ask the necessary and needed information
2. Transparency should be there and the reason behind collecting the data
3. Data should be stored in secure way
4. There should be not use of data for marketing which is direct or data analysis.

Sometime organizations or businesses may need to rely on footage of surveillance for purpose of contact tracing to make sure that workforce are observing health and safety measures. It must be justified and necessary. The reason behind using the surveillance system must be communicated to workforce. The normal way to reflect this through privacy notice.

ISO 27001

ISO which stands for international organization for standardization is a global body which gathers and manages various standards for different things. If we talk in particular about ISO 27001, it is a framework for organization or businesses information security management system. For the organization to earn certificate for this standard, it is essential to maintain an ISMS that covers all dimensions of the standard.

Best practices organization or businesses could follow to comply with ISO 27001:

1. Yearly internal audits should be run in a recommended way.
2. Stay complaint by performing the required internal audits every 3 years.
3. Training sessions should be arranged quarterly to train new hires.
4. Having existing employees take and pass a yearly test.
5. Creating inter departmental iso task force, meet bi-monthly.

GDPR AND COVID-19

GDPR which stands for General data protection regulation, primary goal is to protect the personal data or information of an individual. Today every part of your life can be digitized, tracked and logged every picture every journey, even purchase and even your heart bit. More and more of your personal information is collected and stored, traded by companies and governments. The new gdpr regulations cover things that could identify us so your name, contact details, the location of your computer and personal data like race and sexual orientation. From now on organizations will have to prove they have a lawful reason for holding that kind of data and even more importantly show that they are keeping it safe. the section below will discuss the current data protection laws for protection of privacy during covid-19 and beyond it.

Our life has been greatly infected by coronavirus. we are entering the phase of new normal, as we started emerging from lockdown. The techniques such as monitoring of the workplace, track and trace are creating questions about the individual privacy and GDPR. Guidance has been published by data protection regulators internationally regarding protection of the data while dealing with coronavirus.

The important takeaways

1.Only gather and utilize what is essential:

The data protection laws would not create any concern if your approach is fair and reasonable to the condition.

2. minimizing data

Avoid gathering personal information that one's not needed. Some data need not to be hold for permanent, rather data can be check for that moment only.

3. provision for keeping individual data secure

All the individual personal data must be kept firm and only be kept for the time needed. There should also be policy that talks about retention which tells how and when personal data needs to be deleted, anonymized and reviewed.

4.Transparency

Organizations or businesses must keep transparency regarding processing of the personal information by making available clear, concise information to the subjects. privacy notices should be updated to show any new processing of the personal information which will take place due to coronavirus recovery plans.

Examples

1.Disclosing to other employees of the organization about one of the employee may have contracted coronavirus:

There is no restriction by the data protection law for keeping their employees updated regarding any potential cases of coronavirus within the workplace. The reason behind this business are legally bound to ensure safety of their staff. In line with data minimization and proportionality, which states that only gather and utilize what is essential. So when gathering the information of the individual that is personal which may incorporate symptoms of coronavirus or any outcome of the test, only essential data should be hoard and disclosed to other employees of the workplace or organization. But The colleague diagnosis information should be conveyed to members of team(immediate) for the purpose of contact tracing. The employee who is affected be alerted in advance with the help of communication that is verbal rather than writing. Suggestion is that this should be done on need to know basis. This will reduce the recording of the irrelevant health data, which come up with additional risks.

2. Messages related to health of the public

The NHS or any health professional should not do any direct marketing when sending health messages, may be an email or text. It is of utmost importance that this should contain messages, email or text related to health of the public for ensuring that they are not marketing in a direct way. Service messages which are considered true in nature should not come under direct marketing. However, if it incorporates some type of promotional content then it may come under direct marketing for the purposes of PECR 2003.

3.Working from home and security

Today most of the employees are working from home, although some are returning to the offices. One needs to act in accordance with same security measures as one would follow in circumstances which is normal according to GDPR security requirement. It is essential considering elevated number of cyber-attacks during pandemic, as hackers try every other method to influence people to take more risks than normal circumstances.

What new powers do you get as an individual?

If a company has to ask for permission to store your data, they will have to be much more upfront, so no more check boxes with confusing questions designed to make you give away more information than you want or let us say database of a site you use is hacked and the information is stolen, the organization that was storing information on you will have to tell you about the hack with 3 days and now you have the right to see your own personal data. If you think some company is holding information on you, you can demand that they handover everything they have, as well as this right of access as a right to be forgotten.

Description of the attack

The world of cybersecurity was just getting recovered by solar wind attack and then in month of april 2020, a major cyberattack was discovered. This time the attack was made on Microsoft exchange email server (i.e. it is used for emailing, schedule, collaborate) which is very popular, well known in the industry and its been used by many of the organizations all over. If one is working in corporate setting or organization which includes almost all the industries, there is a high probability that your company uses exchanges to manage the emails. According to the details, attackers hacked the email servers of hundreds of thousands of organizations. These hackers exploited the four security flaws present in Microsoft exchange email software and with the help of access that hackers got through exploiting the flaws, they created many backdoors on the server. The news came into light on March 2020, when Microsoft company officially announced that exchange email server has been hacked and the hackers behind this attack are from china linked hackers named as hafnium.

About Hafnium

Microsoft named the hackers group as hafnium and alleged that the group is from china and they are sponsored by the state. They have targeted many organizations and firms ranging from law firms, non-government organization, the researchers of the disease which are infectious, educational institutions and many more. Since 2010, the group named as hafnium exploited multiple vulnerabilities that are zero day which were there in codebase of the exchange. As mentioned, the group belongs to china and it consist of individuals who are extraordinary in their skills and they run their harmful operations through virtual private servers that are on lease in the United States. The hack on exchange email server was found to be thousands times more ruinous as compared to the solar winds attack. The reason behind this is that they targeted enterprises on a small and medium scale as they lack the capability to conduct a security posture.

Vulnerabilities exposed

CVE's which stands for common vulnerabilities and exposures also known as proxy logon. Majorly exchange server 2013, 2016, 2019 got impacted by these vulnerabilities. There are basically four security flaws or cve's that made an impact which are named as follows:

1. CVE-2021-27065: it is arbitrary file which write vulnerability in path or exchange after post authentication.
2. CVE-2021-26858: it is arbitrary file which write vulnerability in path or exchange after post authentication.
3. CVE-2021-26857: it is deserialization vulnerability which is insecure in exchange unified messaging service.
4. CVE-2021-26855: it is server side request forgery vulnerability.

The attack chain includes all of the above vulnerabilities to exploit the system. Using all of the above bugs, the attacker which is not authenticated can write files by remote code execution through web shell which will give access to exchange server. The two other products of Microsoft namely cloud 365 and exchange online which are cloud products hosted by company itself remained safe during this attack. security flaws have been there in exchange email server version only and as explained cloud products remained unaffected.

Losses incurred

After Microsoft disclosure about the attack, many other hackers group started attacking exchange software and wherever they found flaws, they started exploiting it without any fear. According to estimates, about thirty thousand institutions or organizations got hacked in the united states while sixty thousand exchange users has been hacked all over the world. The ones who got hacked are among the following:

1. Researchers of diseases
2. Law firms
3. Higher education institutions
4. Small businesses, towns, cities and local governments.

European banking authority which is one of the recognized organization disclosed on march 8, that it is also the victim of exchange hack. Domestic users got no problem with this attack and they were safe during this hack. According to the details, hackers have stolen the email conversations of thousands of organizations which includes the above list. Apart from that, the backdoors which has been installed by attackers gave them access to more data.

Illustration of the attack and tools used

Microsoft premises is the only one so far that has been affected so not the Microsoft 365 or the exchange online but on premise instances are susceptible to a vulnerability that allowed attacker to do a server side request and from there it allowed them to read, email and all they have to do is know the inbox they are looking for and from there they can chain the attack into remote code execution using web shell and potentially take over the box and then pivot from there to other boxes so pretty dangerous and from all accounts that we have read online and from the alerts that we have been getting its takes almost no effort to exploit this vulnerability, we don't know what is the proof of concept look like, but at that time it is been exploited and there is no authentication needed right so an unauthenticated attacker can basically send http request to the exchange server which allowed it to authenticate as the exchange server an then from there they can grab the mailbox information for whoever they are looking for. Web shell is the tool that hackers used to do arbitrary remote code execution. For those who are not familiar, a web shell is a malicious web document and when I say malicious, it is not malicious in nature, it is basically doing known commands that you know built into these different web servers but what they do is they leveraged this web commands in a way that allowed them to use the system in ways it wasn't intended it to be right. I see it is not exploiting anything on the web server but it is basically allowing you to take advantage and set up like an admin type console on the box but in a web programming format you can hit this web page which is your web shell and then from there you can issue commands to the actual server itself. There are number of aspx web shells that have been identified, I would not say that you would expect to have the same names found on your server but the thing the places you can look at are various paths that you can look on exchange server that are going to be running under Microsoft.

Timeline of the incidents

During the start of the year 2021, The first two companies who alerted Microsoft company about the exploits at first were volexity and devcore. To be precise it was first discovered by devcore and then by volexity. In no time near to February 26, the exploitation turned into global mass scan where hackers started creating the back doors on vulnerable servers at an increasing speed. In response to the situation, Microsoft released the patch earlier on march 2nd which was scheduled to be on march 9.

Mitigation

1. One of the way that you can protect is to switch to any of the other two products (i.e. exchange online or office 365).
2. So just a quick mitigation is to if you close off access from the internet then those request obviously are not going to go through, one quick way to fix this.
3. If your exchange is not back doored, then apply the patch. Verification can be done by running the script that Microsoft has provided.
4. If exchange server has been affected, then you need to rebuild your exchange server from scratch using backups.

REFERENCES

Ribeiro-Navarrete, S., Saura, J.R. and Palacios-Marqués, D. (2021). Towards a new era of mass data collection: Assessing pandemic surveillance technologies to preserve user privacy. *Technological Forecasting and Social Change*, [online] 167, p.120681. Available at: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC8019834/ [Accessed 17 Dec. 2021].

Zwitter, A. and Gstrein, O.J. (2020). Big data, privacy and COVID-19 – learning from humanitarian expertise in data protection. *Journal of International Humanitarian Action*, [online] 5(1). Available at: https://jhumanitarianaction.springeropen.com/articles/10.1186/s41018-020-00072-6 [Accessed 17 Dec. 2021].

BEAUMONT, A. (2020). *Staying GDPR compliant during Covid-19*. [online] People Management. Available at: https://www.peoplemanagement.co.uk/experts/legal/staying-gdpr-compliant-during-covid-19 [Accessed 14 Dec. 2021].

Ico.org.uk. (2021). *Data protection and employee data during coronavirus - six data protection steps for organisations*. [online] Available at: https://ico.org.uk/global/data-protection-and-coronavirus-information-hub/coronavirus-recovery-six-data-protection-steps-for-organisations/ [Accessed 17 Dec. 2021].

HARWOOD, S. (2021). *Data protection and coronavirus: what you need to know*. [online] Shlegal.com. Available at: https://www.shlegal.com/news/data-protection-and-coronavirus-what-you-need-to-know [Accessed 14 Dec. 2021].

DIGITOOL (2018). *GDPR 2018 Summary | Digitool*. [online] Digitool. Available at: https://godigitool.com/gdpr-2018-summary/ [Accessed 17 Dec. 2021].

PETTERS, J. (2020). *What is ISO 27001 Compliance? Essential Tips and Insights | Varonis*. [online] Inside Out Security. Available at: https://www.varonis.com/blog/iso-27001-compliance/ [Accessed 14 Dec. 2021].

reachresourcecentre (2020). *SOPs for Data Collection during COVID-19*. [online] *reachresourcecentre.info*. Available at: https://www.reachresourcecentre.info/wp-content/uploads/2020/05/DataCollectionSOPCOVID-19.pdf [Accessed 14 Dec. 2021].