Review of Guidelines 01/2021 on examples regarding data Breach Notification

Adopted on 14 January 2021

1. Table of Contents

2. INTRODUCTION AND CONCEPTS/RESOURCES THAT CAN AND SHOULD BE USED WHEN DESIGNING A PROGRAM

2.1. A privacy and security program (NIST CSF)

Ideally a program combines actions in all of the following domains:

Source: NIST CSF https://www.nist.gov/cyberframework

NIST CSF Defines these categories as follows (source NIST CSF):

2.1.1. Identification

Develop an organizational understanding to manage cybersecurity risk to systems, people, assets, data, and capabilities. The activities in the Identify Function are foundational for effective use of the Framework. Understanding the business context, the resources that support critical functions, and the related cybersecurity risks enables an organization to focus and prioritize its efforts, consistent with its risk management strategy and business needs. Examples of outcome Categories within this Function include: Asset Management; Business Environment; Governance; Risk Assessment; and Risk Management Strategy.

2.1.2. Prevention

Develop and implement appropriate safeguards to ensure delivery of critical services. The Protect Function supports the ability to limit or contain the impact of a potential cybersecurity event. Examples of outcome Categories within this Function include: Identity Management and Access Control; Awareness and Training; Data Security; Information Protection Processes and Procedures; Maintenance; and Protective Technology.

2.1.3. Detection

Develop and implement appropriate activities to identify the occurrence of a cybersecurity event.
The Detect Function enables timely discovery of cybersecurity events. Examples of outcome Categories within this Function include: Anomalies and Events; Security Continuous Monitoring; and Detection Processes.

2.1.4. Response

Develop and implement appropriate activities to take action regarding a

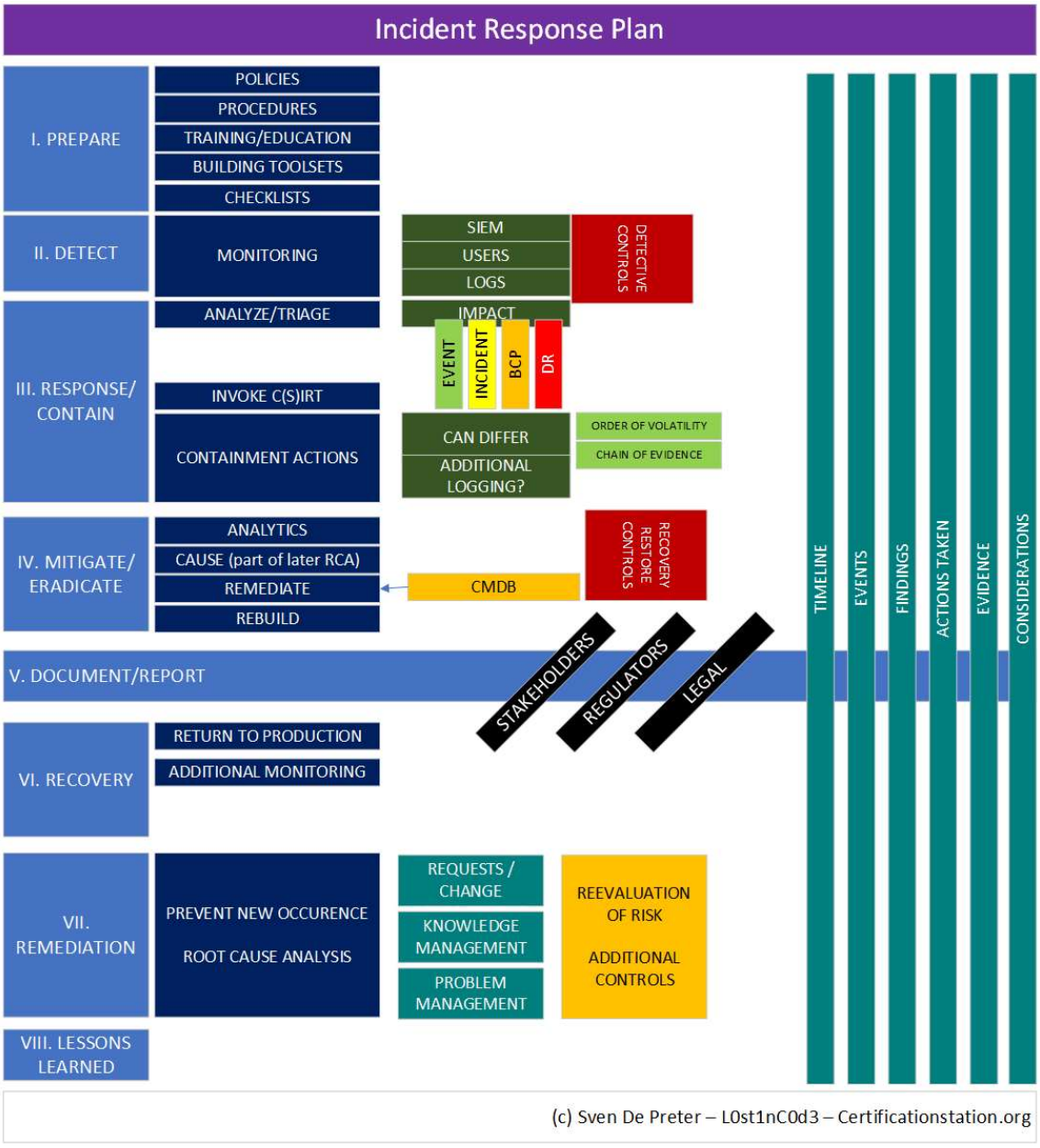
detected cybersecurity incident.
The Respond Function supports the ability to contain the impact of a potential cybersecurity incident. Examples of outcome Categories within this Function include: Response Planning; Communications; Analysis; Mitigation; and Improvements.

2.1.5. Recover

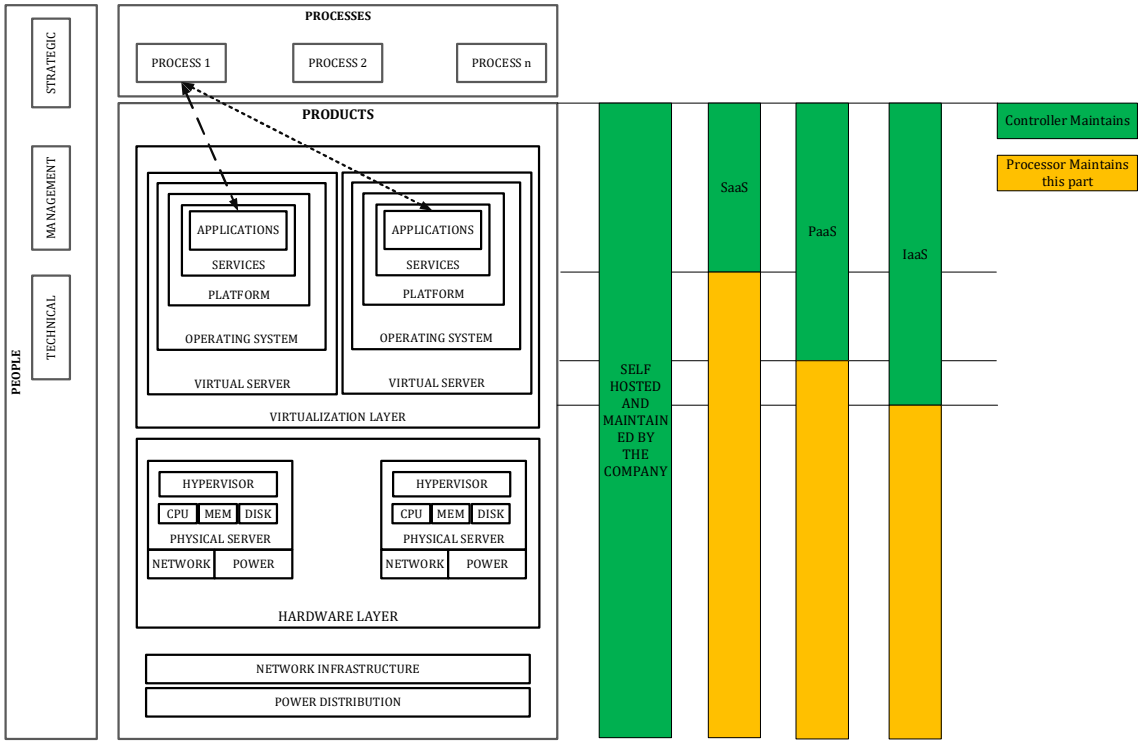
Develop and implement appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity incident. The Recover Function supports timely recovery to normal operations to reduce the impact from a cybersecurity incident. Examples of outcome Categories within this Function include: Recovery Planning; Improvements; and Communications.

2.2. Incident response

~~When studying for the CISSP exam, summarized~~ The Incident response plan as follows. It can easily be extended in order to also deal with privacy incidents. As the workflow is roughly the same. In order to get the most out of incident response, and mitigation strategies resulting from the lessons learnt, a Root Cause Analysis must be performed.



2.3. The environment



Understanding the infrastructure and the processes being run is crucial to designing a decent security and privacy program. Each block in the drawing above has specific vulnerabilities, requires patching and requires specific skills. In case of IaaS, PaaS, SaaS, parts of this diagram will fall under the responsibility of the cloud provider as illustrated above. The parts that are managed by the cloud provider (whether or not cloud is considered to be on-prem or somewhere on the internet, or in a remote datacenter), fall under the category of vendor and supply chain management. Roles, responsibilities, SLA's, and contracts must be in place. In a cloud model, not everything can be managed by the data controller. He trusts or makes agreements with the cloud provide or controller to make the necessary arrangements in terms of security and privacy. A breach in the section managed by the processor may not get "solved" by the controller.

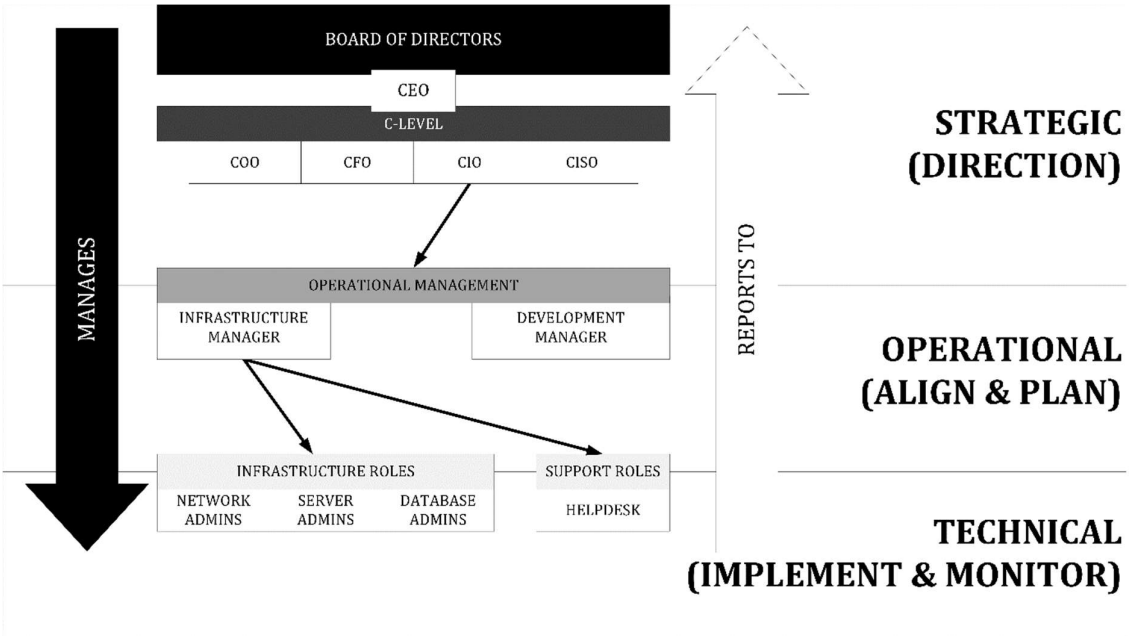
Another interesting point is that cloud-based applications can cause vendor lock-in. It is easy to get the data in, but nearly impossible to extract and move data to another system. Also, vendor lock-out can occur.

Usually, the cloud provider also provides tools, to manage and monitor security and privacy.

Having access to the physical hardware or the operating systems, can result in the higher layers to become compromised.

Interacting with data/processes/applications/people (starting from the top), can lead to misuse and abuse, which in turn can lead to security issues that expose underlying layers too.

2.4. Corporate hierarchy

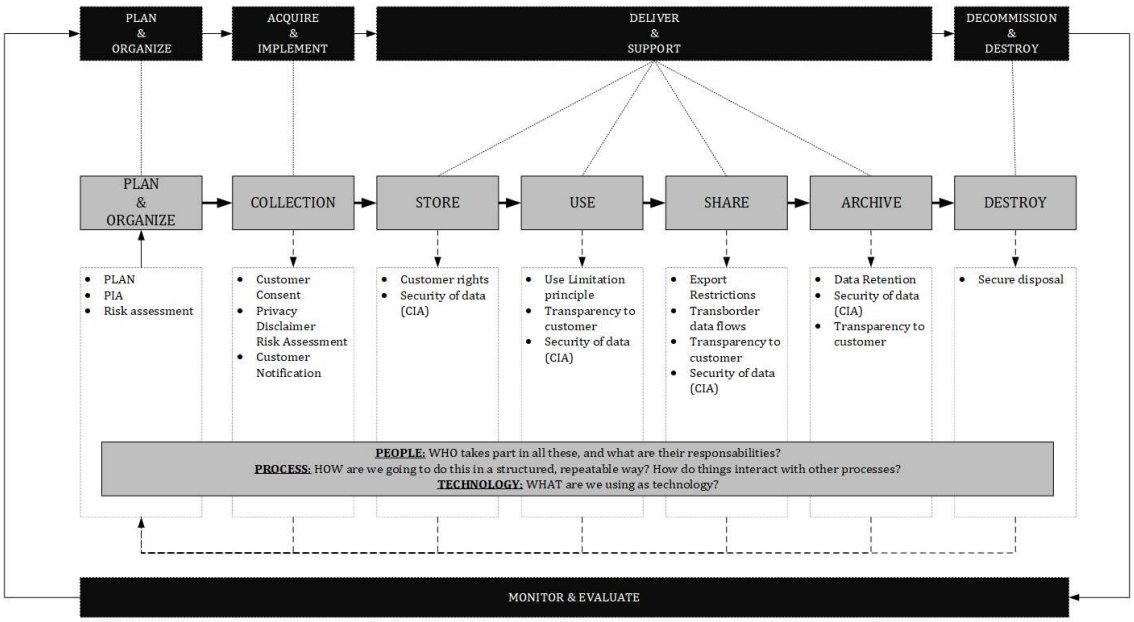


Data protection efforts should be driven by a top-down governance system, as in the end the strategic layer will be held accountable for breaches. The arrows going down, indicate the "team" members. The further down, the more technical it becomes. The strategic layer also drives the risk assessment, and takes decisions on the risk appetite, risk tolerance, and acceptability of risk. This also shows that in order for a plan to work, it should be seen as an effort that spans all layers of the organization. Having technical people make decisions on how to protect data, is not enough. Hence, just resorting to technical measures can and will cause problems later-on.

2.5. Lifecycle management

In order to create a decent privacy plan, it must be understand how the processes work, where data is used, where it is stored, when/where it is transmitted. When combining this with roles & responsibilities, or strategic/operational/technical layers, the base of any security/privacy program is formed.

Mapping Requirements to a lifecycle in order to build a program/plan.



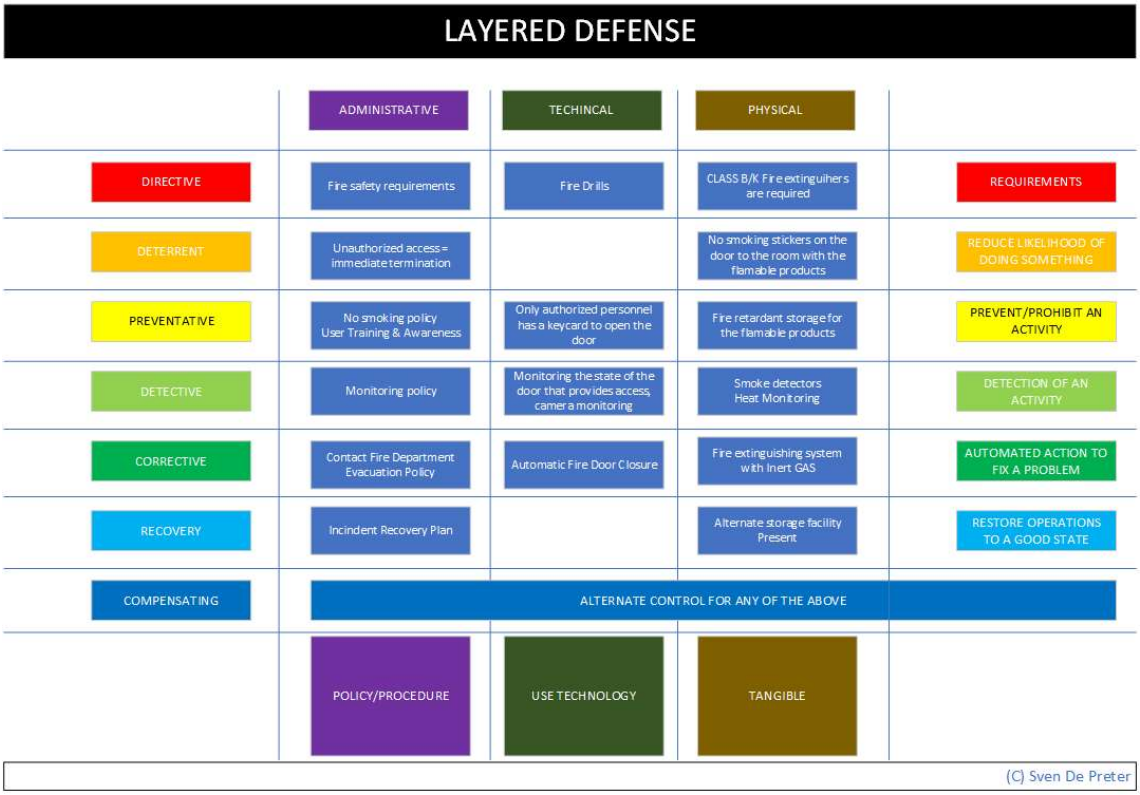
(C) Sven De Preter – L0st1nC0d3

Doing this exercise for processes involved with PII, facilitates the mapping of requirements and controls to the diagram. The controls can be defined in terms of functions and categories when using the NIST CSF. Other ways of adding more traditional controls include adding a control matrix as specified in the next topic, to each stage of the described lifecycle model.

In a 2nd faze a diagram of the process can be used and map the stages of the lifecycle to the actual process.
This may greatly help in designing processes that have “Security & Privacy by Default & Design”.

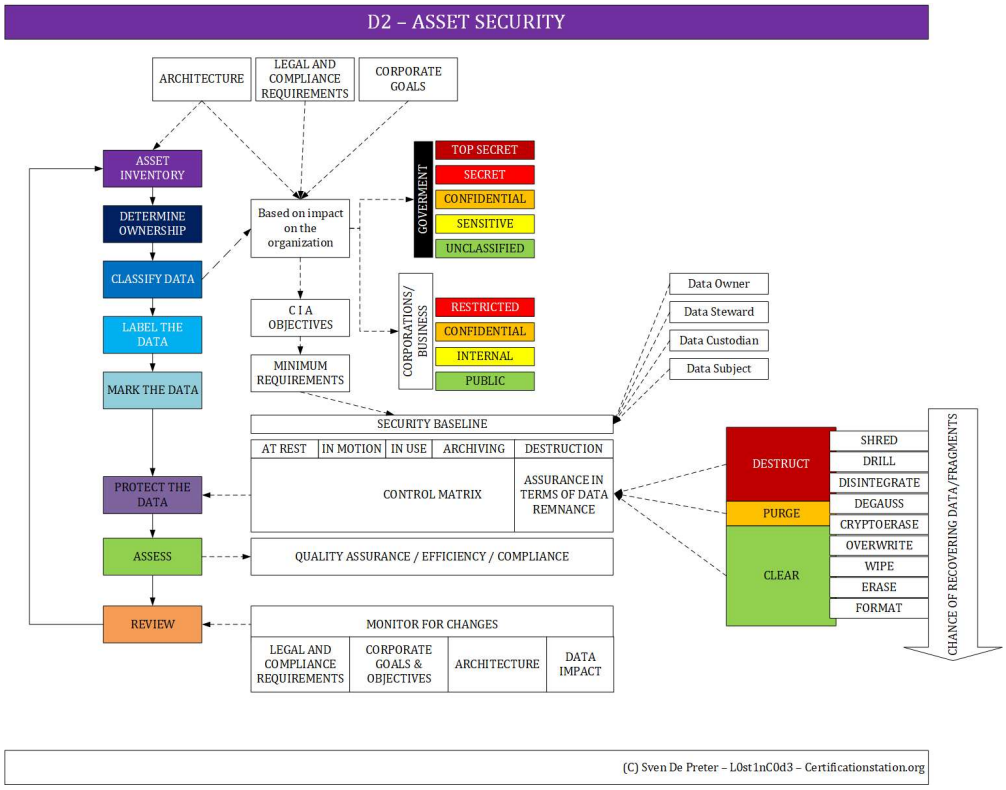
2.6. Defense in depth must be applied to come up with a complete plan.

The example below is about fire prevention and fire extinguishing. Matrixes such as these can be used to visualize our efforts. This can also help in detecting gaps in security/privacy control sets.
Ideally, matrixes such as these are constructed for each block of the lifecycle of the data.



2.7. Data classification

Data classification can be useful, as different data may require different protective measures. In terms of privacy, one could say that basic PII (such as name, address, country) can live with less protection than records about criminal offences.



The image above is a generic (security/data classification) approach. It clearly illustrates, that data should be categorized based on the potential harm that it can bring (BIA vs PIA). This results in requirements in terms of confidentiality, integrity, availability. Those 3 components, can then be used to build a security baseline (where a baseline can be defined as a minimum set of security controls needed to provide sufficient protection)

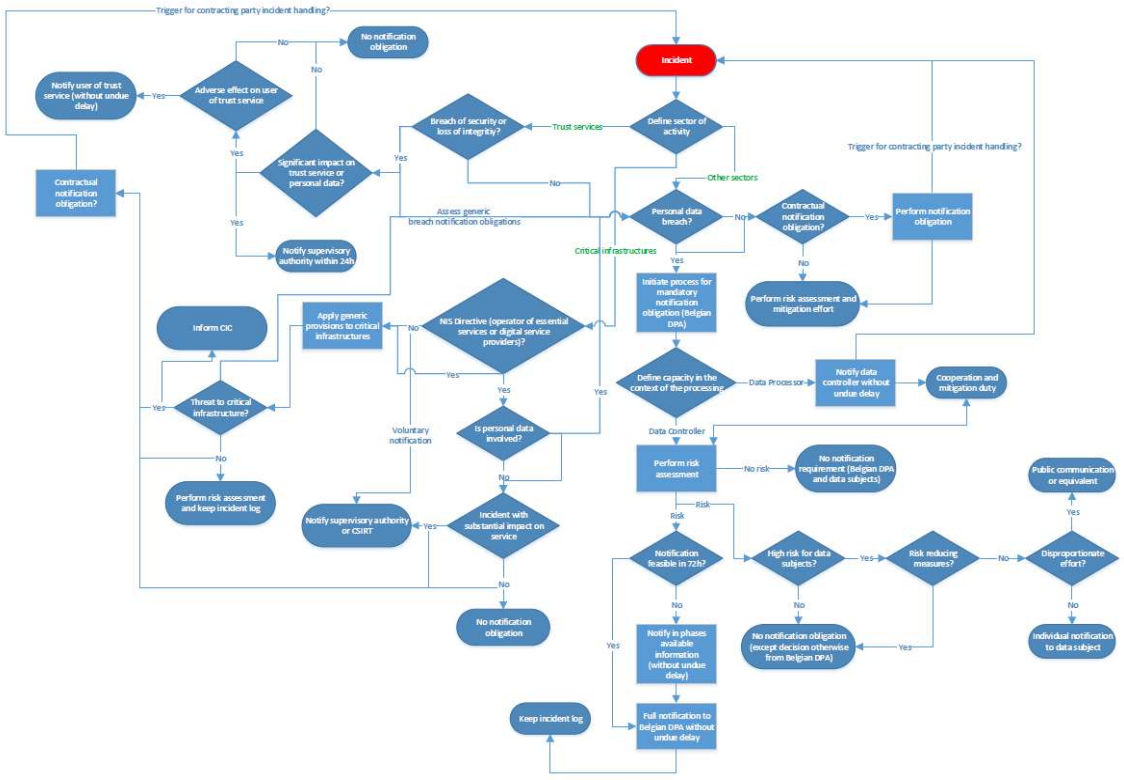
As described, the baseline aligns with the lifecycle model and the control matrix as it incorporates data at rest, data in motion, data in use, archiving and the destruction of data combined with preventive/mitigative/response and recovery controls. This also align perfectly with GDPR.

On the left side, you can see the colored boxes, that link assets and ownership to the data, as well as the importance of labeling and marking data.

Marking and labeling data can also be very helpful when installing Data Loss Protection software that link policies to data. For example, “the PII cannot be sent by email policy”, could add a filter on the email platform. This filter would then look at the metadata or data of an attachment/email and decide if it can be sent or not. If not, the action is logged, and the mail is not being sent. This brings us close to a full lifecycle approach. Which is what GDPR expects us to do.
Data can be (in terms of GDPR) be classified in terms of the risk it brings to the data subject.

2.8. Breach notification diagram

Data breach notifications under Belgian law (future situation: assumptions based on NIS Directive and GDPR included)



Source:
Johan Vandendriessche

Partner | Crosslaw Visiting Professor | UGent | HoWestj.vandendriessche@crosslaw.be | www.crosslaw.be

Version 1.2 - Last revised: 11 January 2017

The diagram illustrates the complexity of Data breach notifications.

2.9. Feedback on the issued guidelines in the introduction

2.9.1. Guideline 8 page 6

The paragraph references attack as the source of data breaches. Data breaches can be generated by other reasons – e.g. employees sending messages to wrong recipients by mistake, as detailed under Section 4 of the guidelines.

2.9.2. Guideline 9 page 6

The initial risk estimation may change as the investigation continues. Data breaches that initially were estimated as not having impact may be later considered to have an impact (or vice versa).

2.9.3. Guideline 10 page 6

In the case of risks that materialize (whether unlikely or not), the entire context of the situation should be assessed. For example, was the initial qualification of unlikely adequate for the risk? Was the risk addressed properly from a risk management perspective, considering the other risks identified by the organization?

2.9.4. Guideline 11 page 6

The data breach plans should reflect the NIST Incident Handling Steps outlined in SP 800-61, as these are applicable also in case of data breaches: detection and analysis, containment, eradication and recovery, post-incident activity.

2.9.5. Guideline 12 page 6

The trainings should be tailored for the specific job description of the employees (e.g., for accountants the receipt of phishing emails with invoices).

There should also be an annual walk-through of the data breach plan in order for each employee to learn better his/her role and the steps to be taken.

The trainings should be regular (as mentioned), but it may be worth adding the during induction training for new employees, data breach training should also be included.

3. RANSOMWARE

3.1. CASE No 01: Ransomware with proper backup and without exfiltration

3.1.1. Initial thoughts when reading the case context

Without even looking at the prior measures and risk assessment, the case is presented in such a way that it raises multiple concerns & thoughts. It is purely brought from a privacy impact perspective but does not account for security breaches leading up to the privacy breach. (While a privacy breach is suggested to be the result of a security breach).

Article 4(12) as: "a **breach** of **security** leading to the accidental or unlawful destruction, loss, alteration, unauthorised. disclosure of, or access to, personal **data** transmitted, stored or otherwise processed".

3.1.1.1. Investigating logs was done by an external party.

As an external party is brought in, one could speculate about who performs maintenance on the system that was compromised. As this example is a small manufacturing company, the systems may be rented, or other services may also have been outsourced as lack of it skill is present.

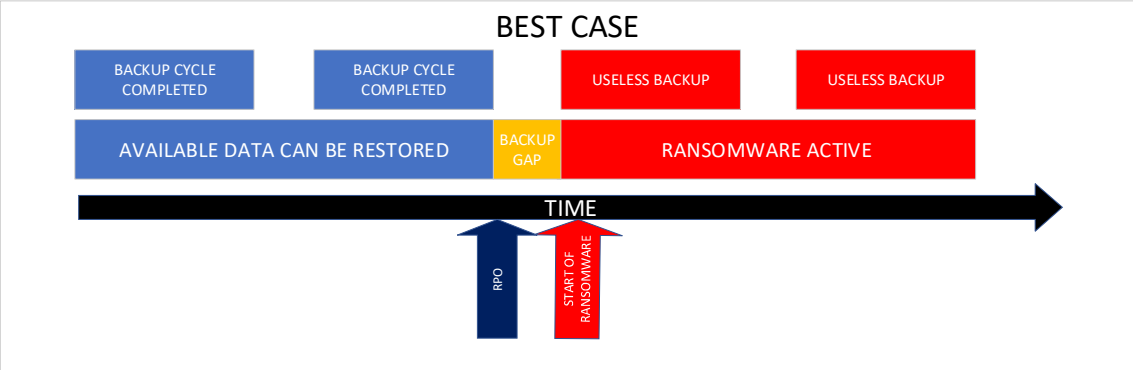
When talking about an external cybersecurity company, should there be any requirements for such a company? For example, a required certification?

If the IT services were not outsourced, who defined what should be logged and where should it be logged? How are the logs maintained? How can the organization ensure the integrity of the logs that they weren't changed during the ransomware attack?

3.1.1.2. A Backup was used to restore the system to a last known good state

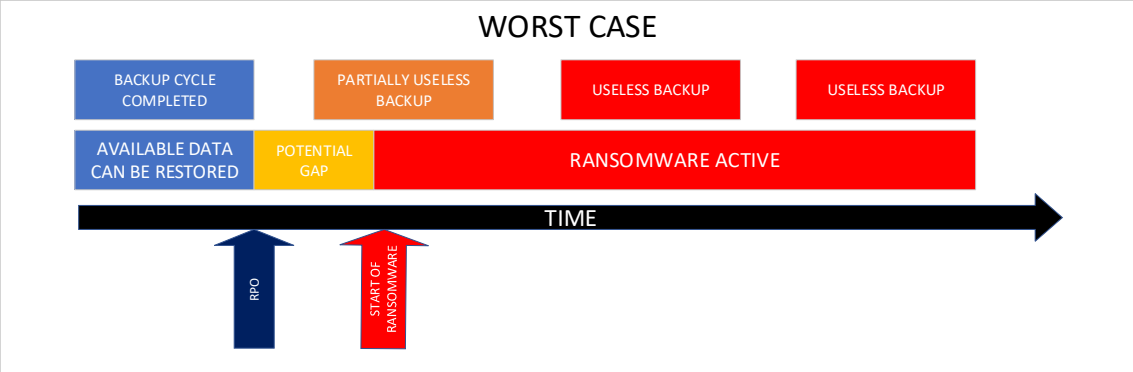
Having a backup is great. Being able to restore it is even better. However, when the backup timing is examined, the following is revealed:

In a best-case scenario, backup cycles completed before the ransomware attack. As in most cases backups do not run continuously, a gap can be seen between the data that can be restored and the data that was present once the ransomware started encrypting files



In another scenario it is shown that the backup was not fully completed at the time the ransomware started encrypting files. This makes that backup rather useless, as files will potentially be restored that have already been targeted by the ransomware. Hence an older

backup needs to be restored. A larger gap now exists between the data that can be restored and the data that was present.



The size of the gap defines the data that will never be available again. When looking at this from a privacy perspective, changes made by the customer, completed transactions, proof of payment, … may no longer be present. Resulting in the company not being able to fulfill its contractual obligations towards their clients.

Companies may try to "reconstruct" the data that is lost in the gap, they can try and find paper documentation, use their memory to recall changes, contact customers, etc. However, there may be little confidence in alternate data sources.

It is true that a backup will resolve the issue, but it doesn't prevent the ransomware from encrypting data, nor does it prevent a ransomware from being installed on the system.

3.1.1.3. The mystery of the logs

At this time, it is clear that there was some system of logging which keeps track of inbound and outbound data flows. This is assumed to be some form of firewall. As this implies that this is network traffic (between the internal network and the internet), there might not be an understanding regarding what happened on the servers.

As the servers were attacked with ransomware, the odds are that some of the logs on the server may also have been encrypted, rendering them useless in terms of investigating what went wrong. When using a backup to restore the server to a last known good state, those server-logs will also be reverted to the last known good state. As the backup preceded the ransomware attack, there would be no indication in the server logs anymore after the restore.

It also seems that even though there were logs available, time nor skill was present to do a regular or automated review of these logs. In this case, it can be said that logging is done so it can be used in a post-mortem analysis.

The analysis of the log shows no signs of data exfiltration. Which is quite normal. If a hacker is active, he/she will use an encrypted communication channel with his target. All that may be visible is that there has been a lot of communication/data flowing between 2 endpoint IP addresses… As the channel was encrypted, traffic analysis is limited.

3.1.1.4. The mystery of asset ownership

Even though the company that was attacked with ransomware is ultimately accountable, it is interesting to see who owns/maintains the infrastructure. What type of company is this? Is it a small manufacturing company with just a handful of customers and staff, do they rent equipment? Or do they buy equipment?

It can be interesting to see as it opens a discussion on vendor and supply chain management. Also, when infrastructure/software is rented, there should be a contract that defines the responsibilities of each party. If proof can be delivered that contractual obligations were not met, things can unfold differently when starting legal procedures.
It is true that the company is to blame, however they had a contractual agreement with the vendor. However, this also brings up a discussion about "monitoring contractual performances."

3.1.1.5. The mystery of the ransomware entering the server

As there is no real indication in the case on what preventive measures, they had in place to protect from ransomware, it would be interesting to see how it reached the server.

Traditionally ransomware enters an organization through:

Social engineering: "Hi, I'm Bill from Microsoft, please install this software so we can resolve your server issues."

Malicious downloads: Here is a nice tool to install on the server. It seems legit but may act as a trojan that unleashes a ransomware. This also includes scenarios as has been seen with the SolarWinds case. A "modified" patch was inserted in the system and was propagated to all clients.

Connection with an infected device: In the ideal world, all devices that enter the company and connect to the corporate network, are managed by the company. However, at times suppliers/customers/guests may connect to your network. If at some point these "guests" have an infected device, they could spread any malware onto your network.

Portable media: The use of portable media imposes dangers as well and can be the source of an infection.

Hacker: In most cases the hacker would need access to the system (direct or via internet), and escalate privileges from user to administrator, prior to releasing the malware. Such attacks can be scripted. These scripts can potentially target the entire internet.

As 5 different entry points have now been defined, several weaknesses can be seen, only one of which, points to a skilled motivated and malicious person who took time and effort to bypass security measures. In the latter case, it should be considered if those activities will be in "traffic logs (2.1.1.3)". It also opens a discussion on the use of IDS/IPS. (Intrusion detection systems/Intrusion prevention systems).

There is no case for zero risk. There will always be some residual risk. Even when protecting against ransomware to the full extent possible, there will always be new viruses, malwares, trojans, ransomwares. At some point in time, when released in the wild, they are known as Zero-days, as they cannot yet be detected by traditional endpoint protection.

3.1.1.6. Endpoint protection

At this point it is unclear if endpoint protection was installed on the impacted servers. If malware protection was installed, the ransomware could have been detected and stopped before it caused any damage (except of course when speaking about zero-day malwares).

If endpoint protection was installed, there is also no clue about the frequency of updates.

3.1.1.7. Patch management/vulnerability management

The case does not specify details on the presence of a vulnerability or patch management program. Keeping 2.1.1.4 in mind, as outsourced services or rented equipment are a possibility.

The ransomware could also be a result of a malicious patch. This has happened in the SolarWinds case.

Even with a perfect patch & vulnerability management plan in place, there is still the risk of z-day exploits.

3.1.1.8. Risk management

When reading the case, it is not discussed how the risk assessment was performed, hence there can be no determination as to adequate measures were in place. However, it can be concluded that small companies are usually seeing security and privacy as a cost, not as an enabler.

As only a few dozen individuals were impacted, it could be stated that adding additional preventive measures was deemed non beneficial in terms of cost/benefit. That is, the cost of additional measures would exceed the potential benefit. Hence, they accepted this potential risk.

The cost aspect can be split into 3 components: People, Processes, Products

ENISA provides great advice and guidance on how to classify privacy risk. In its document: "Recommendations for a methodology of the assessment of severity of personal data breaches – Working document v1.0, December 2013"

It defines 4 categories:

Severity of a data breach		
SE < 2	Low	Individuals either will not be affected or may encounter a few inconveniences, which they will overcome without any problem (time spent re-entering information, annoyances, irritations, etc.).
2 ≤ SE < 3	Medium	Individuals may encounter significant inconveniences, which they will be able to overcome despite a few difficulties (extra costs, denial of access to business services, fear, lack of understanding, stress, minor physical ailments, etc.).
3 ≤ SE< 4	High	Individuals may encounter significant consequences, which they should be able to overcome albeit with serious difficulties (misappropriation of funds, blacklisting by banks, property damage, loss of employment, subpoena, worsening of health, etc.).
4 ≤ SE	Very High	Individuals may encounter significant, or even irreversible, consequences, which they may not overcome (financial distress such as substantial debt or inability to work, long-term psychological or physical ailments, death, etc.).

Src: ENISA (**www.enisa.europa.eu)**

3.1.2. Feedback to the "prior measures and risk assessment" for this case

3.1.2.1. Guideline 18

While the point is acknowledged, organizations can add an infinite number of security layers, and build a fortress. However, the key question here should be "How much is enough?", and when does the risk become "Acceptable". Do note that budgets with the SME may not be as large as those in a multinational corporation.

Also keep in mind that some companies still use software that is no longer supported by the vendor. Yet, substantial investments have been made for integrating this software with other components. Also, some software packages do not support encryption of PII. Can you really forbid SME's to use such applications (based on the category of PII they store)??

When interpreting this, the SA can always say that you have been negligent, didn't practice your Due Care nor Due Diligence, resulting potential fines and warnings.

The backup plan should include periodical testing for restoration of the data/IT systems. Further, in certain cases, there is only a back-up of data (e.g., databases) and in other cases there is a back-up of the IT system itself (e.g., application server). When a malware entered the organization system and there no way to be certain that all malware was eradicated from the system, the back-up IT system will be used in the future and not the potentially compromised one.

3.1.2.2. Guideline 19

It should be considered that once breaches occur, logs may get altered or destroyed. Even though there is no indication in the log of data exfiltration, it certainty cannot be eliminated as a possibility. Customers should be notified. When keeping 2.1.1.2 in mind notification of customers can also help in reconstructing the gap.

3.1.2.3. Guideline 20

If the infection happened through the use of an infected USB flash drive which was connected by a user there is an entirely different situation than when considering a remote malicious hacker, breaching an enterprise system, installing malware and asking a ransom.

This brings us to 2 distinct cases:

- Deliberate actions – pay the ransom or lose the data!
- Accidental cases

Another question to consider. If a malicious actor was on our system, escalated his/her privileges to administrator or system level, wouldn't this person be able to scan the memory/storage for potential decryption keys? Would it be noticed if the attacker moved lateral from server to server?

- When taking this into consideration, there could be a 3rd case. Use ransomware to mask data theft/exfiltration.

- If this actor was on the system, he could have had access to the data over some secure channel. As those channels are hard to inspect (because of their encrypted nature) one can wonder about the visibility of data-exfiltration in the logs.

3.1.2.4. Guideline 21 page 8

Please define the concepts of “impact” and “severity” used in this paragraph and what is the difference between them.

3.1.2.5. Guideline 22 page 8

Even though this case has a rather happy ending, it could have been a lot worse. Even within a similar scenario. Consider the fact of having more staff, more customers, and a backup that runs every day 23:00 till 2:00.

Different impacts, outcomes can happen based on when the ransomware strikes.

- If it strikes at 12:00, there is potentially have 10hrs of data loss. (gap between time of backup and the time the ransomware started encrypting files)
- If it strikes at 22:00, there is potentially have 23hrs of data loss.
- If it strikes at 23:04, there is potentially have 48hrs of data loss.

Depending on the industry or sector, the impact can vary.

Another set of cases can be investigated, as this mainly concerns on-prem servers. What if this was infrastructure running in the cloud? How would the use of IaaS/PaaS/SaaS influence the outcome of this case in terms of notification? (As at that point the breach can be seen as being initiated at a processor’s infrastructure)

3.1.3. Feedback to “Mitigation and obligations”

3.1.3.1. Guideline 23 page 8

When fixing vulnerabilities 3 domains must be considered. However, organizations should start with a root cause analysis. If the root cause cannot be determined, additional controls may be employed that do not prevent/mitigate an attack that is conducted in a similar way.

Eg. If it cannot be established that the problem occurred because someone was tricked into installing a malicious software, what would be the additional value in providing training on how to recognize malware and social engineering? (in the context of this problem)

Eg. If it can be established that someone performed a server update using a USB flash drive (which was infected), actions can be taken such as “disallowing the use of USB devices”. These technical decisions can also be enforced.

Doing so also provides a lesson learnt section, which is later used to re-evaluate risk and associated preventive/mitigative/restorative controls.

The option of “resetting” and IT system is not necessarily the one to be used. This depends on the way the recovery and eradication can take place. Using back-up IT systems may be needed rather than using the existing ones which may continue to be compromised.

3.1.3.2. Guideline 24 page 9

This case is quite simple as the time of infection is easy to determine, because the ransomware started encrypting files. There is a noticeable effect as files become useless. There are however other malwares and system compromises that take much longer to detect. In some cases, especially when speaking about small size companies, they will never be detected.

The reason here is mainly lack of skills, budgets, awareness. On average, it takes over 100 days before a breach is detected.

Please detail in which conditions related to severity the 72h terms are considered unsatisfactory. The wording under the GDPR seems to indicate that notification should be done earlier when it is feasible.

3.1.3.3. Guideline 25

As customers are not notified, consideration should be given to transparency promises made to the data subjects. It is not because data exfiltration was not proven that it did not happen. There are many ways to do this in a cover way.

The customer should be notified. Notification can also be combined with a request to verify their data for accuracy.

“The organization may also need to update and remediate its organizational and technical personal data security handling and risk mitigation procedures”.

Basically, this states that the SA will define what “acceptable” risk is… (post-mortem). How does this fit in to the cost/benefit model, which is extremely important in SME style companies?

Yet again, “how much is enough?”, “what is acceptable?”

3.2. CASE No 02: Ransomware without proper backup

This case is quite like CASE 01. Yet a backup of the data missing and encryption at rest was not used. Data restoration took 5 days. And most data were recovered from paper backups.

As in the case above, it should be assumed that data was exfiltrated. Just because there is no proof in the logs, that does not mean it has not happened.

The main difference here appears to be that encryption was not used for the data at rest. Even though the data itself contained no special categories, the assumption of data exfiltration is still there. If not, there would not be a reason to report it to the SA.

The data being restored from paper backups, leads to another discussion, being the protection and handling of those paper documents and the protection thereof.

Point 28 here is quite interesting. And in fact, also applies to Case No 01. The only difference here is that it would be harder to decode the encrypted data.

When extrapolating this, it seems that the general rule is:

- Data encryption used => no need to report
    - When using data encryption, due care must be exercised in protecting the encryption keys too!
- No data encryption used => everything must be reported to the SA, no matter what the impact to the risks and freedoms of the Data Subject is. (Mainly due to data exfiltration of human readable data was possible)
    - This also opens up a discussion on which controls should be in place if encryption cannot be implemented.

It is not agreed that the Data Subject must not be informed. While this may be correct from a privacy point of view, not being able to fulfil contractual obligations will cause a different set of problems and claims. The risk must be analyzed.

Notification of the data subject can help in reconstructing data, which in turn will result in being able to fulfill that contractual obligation. Transparency is all about being honest to customers. Using that transparency and communication can also result in trust, as assurance can be provided that no data was lost as well as an indication of the risk to the rights and freedoms of the data subject.

In this case it can also be said that not having a backup, can be seen as negligence as it undermines the core principle of Availability.

Not sure if this scenario is comprehensive and good. Which systems / data location was affected? It took several days to restore a few dozen individual's information and caused a minor delay in delivery of orders. Why should this be reported to SA, since no GDPR related information were stolen? The TOM´s and the company risk register as in section 3.1, regardless the fact that the customer needs to be informed about the delay in the delivery.

3.3. Organizational and technical measures from preventing/mitigating the impacts of ransomware attacks

This entire topic should be rewritten as it only focusses on a few well know concepts that each tackle a part of the problem. This section feels like they have specified the quick fixes. The measures described here are basically technical measures, and a few pointers towards education.

The description is also written in a "policy" style. This particularly makes it hard to implement for small size companies (as in the first 2 cases of the ransomware), as those companies usually lack skills/assets/resources to do this properly.

> Try telling a farmer: "Design and organize your processes so they implement privacy and security by design and by default", without knowing what his infrastructure looks like. He may, just use a simple desktop pc for his day-to-day administration, combined with a USB flash drive on which he regularly copies data. His disk may be encrypted, yet booting the system, decrypts the disk as it would not be usable otherwise. Once the system is booted, he can still be the victim of a ransomware attack.

Never is there a discussion on how much is enough, nor is there a discussion on how specific controls reduce the risk.

In an ideal world, the EDPB/SA would consult businesses, learn from them, and come up with some form of control matrix (As NIST did on several occasions). Such a framework could then use "risks & freedoms risk tiers" and provide guidance on how to do a proper implementation.

Just presenting cases, which are poorly formulated and provide poor context, followed by pointing out legal requirements is not going to help anyone. Especially not the small to medium size enterprises.

When reading something at the start of the GDPR that came from ENISA or CNIL, they defined the different degrees of harm that could be caused by PII leakage. They defined about 5 categories leading from CRITICAL (can lead to death/special categories) to MINOR (issues that can be overcome by the data subject with a minimum of efforts)

In doing so, it can allow them to come up with a control matrix such as defined in the NIST SP800-53 Rev 5. Where based on the risk tier, a determination is made in terms of controls and guidance that can help you build a program. This will not only help people understand what is expected, it will also provide them additional guidance.

However, not every company has the same resources/budgets. This will complicate everything.

Even though encryption is the de facto standard solution that should be implemented according to the guidelines, not all applications/software facilitate the use of encryption. In case encryption cannot be used, alternate controls must be defined.

In general, it will boil down to small companies being forced to spend lots of money on professional assistance and guidance. Money that they would have rather invested in their products, manufacturing, delivery etc. Which in turn may even slow down economic growth.

When looking at the NIST SP800-53 Rev 5. One could be looking into those categories and controls when it comes to dealing with ransomware.

Other actions (not limited to this list) that can also help in the detection/prevention/mitigation of ransomware.

- **Access control & identity management**:

  - If a ransomware is inadvertently installed by a user, it will run in the user context, with the rights and privileges that the user has.
  - Segregating data, and adding different permission requirements to them, can in fact help reducing the damage.
  - This also implies that administrators should have 2 accounts.
    - 1 for their basic day to day work like reading mail and typing documents.
    - 1 for their administrative needs
  - As an account should be personal, not shared, it will be easier when going through server logs, trying to figure out who released the malware.
  - Identity management and account provisioning can potentially start during the onboarding of employees. Once an employee stops working for the company, his account should be disabled. If not, he can potentially still use a VPN, release a malware or ransomware, delete files … and cause harm in many other ways.
  - Data should be accessible on a need-to-know basis.

- **Planning & Testing**
  - Patches or software are preferably tested on non-production infrastructure.
  - How to deal with faulty patches that cause system malfunctions?
  - How to deal with cases like “SolarWinds”? Where the vendor had an issue, that allowed an attacker to propagate malware to customer devices?
  - Updates should be announced and performed during times when they can cause the least harm. How about upgrading a database during the busiest hour of the day?
    - Not only will it disrupt business, but it can also have an impact on the data.
  - When and why should people think about Penetration testing?

- **Vendor/Visitor management**
  - What is the privacy risk when vendors/visitors/guests can physically move through the company unattended?
  - What risk does a supplier/vendor bring when he connects his laptop to your enterprise network?
  - What about vendors/suppliers performing actions on your systems?
    - What are the roles & responsibilities?
    - What protections do you have?
  - What about IaaS/SaaS/PaaS? Even though a person is accountable as a “consumer”, there are parts they cannot control. A person must accept those potential risks, or they cannot use the environment. This opens a discussion on vendor management and supply chain.
- **Training**
  - Based on which risks, likelihoods and impacts will you design your SETA program?
  - Who will provide the training?
  - How does social engineering relate to the installation of ransomware?
  - What is the process to detect and respond as a first line responder when you notice files are being encrypted?
  - How is evidence preserved that can later be used during root cause analysis?

        - This could be important evidence that can be used to show a vendor did not comply with his contractual obligations, which in turn resulted in lack of protection from the malware.
- **Network and data segregation**
    - Different physical or logical networks/servers/shares, could be used that have different degrees of protection based on the protection the data requires.
    - Access can be granted based on a need to know, while implementing least privilege.

Feedback on the guidelines issued

3.3.1.1. Guideline 39 page 11

The conclusion about notification of data subjects does not reflect all possible scenarios. It mentions data subjects currently in the hospital and the ones that came to the hospital 20 years ago. However, based on what criteria should others be notified individually? Based on the period of the time which has passed since they were in the hospital? Based on the potential impact of their health data being known by third parties. e.g. data about HIV patients may be relevant even after 10 years.

*"Direct communication to the other patients **some of which may not have been in the hospital for more than twenty years** may not be required due to the exception in Article 34 (3) c)"* Article 23 (3) c) refers to communication to data subjects when it would involve disproportionate efforts. The details in bold may act as a distractor as it unintentionally may suggest the inactive relationship between the controller and data subject as the exception. Also, this guideline states that *"data relating to all patients treated in the hospital during the last years has been encrypted".* This implies that the sensitive data of these other patients who *"may not have been in the hospital for more than twenty years"* was unencrypted. Thus, the ransomware attack involved a breach of confidentiality, although no factual exfiltration was detected. Conclusively, it is recommended to remove the bold text or clarify when the efforts to communicate with other patients may be deemed disproportionate; generally, a breach of confidentiality of sensitive data is not something to be taken lightly.

3.4. Alternate cases that can be worth investigating

For the entire ransomware section, it could be interesting to see how the EDPB would respond to the following cases:

3.4.1. Ransomware with proper protection

Computer systems of a small manufacturing company were exposed to a ransomware attack, and data stored in those systems was encrypted. The data controller did not use encryption at rest. Multiple layers of protection were in place.

- Endpoint protection was in place and contained the most recent signature files.
- Intrusion Protection Systems were in place to prevent harm to the legacy software systems as they are designed to stop attacks.
- The systems are patched to the latest levels one month after the release of a patch. The reason is that they test the patch during one month on a few servers, to see if it causes any incompatibilities. Once the testing is concluded and the patch is authorized, the patch is installed on production systems.
- Due to the nature of the business, older software is still in use. Heavy investments were made in the past to integrate this software with the manufacturing systems. The vendor can supply a new version of the software, yet all investments in the integrations with the manufacturing systems would need to be redeveloped, retested, etc. The software contains customer PII and does not support encryption.
- Systems were also hardened using the CIS Benchmark standards.
- Log items are forwarded constantly to a central repository (SIEM).
    - Issues detected are displayed directly on a dashboard.
    - Upon detection of issues, the local staff starts the incident response procedures.

During the breach, the attacker only had access to unencrypted personal data.

The company is using the expertise of an external cybersecurity company to investigate the incident. Logs tracing all data flows leaving the company (including outbound email) are available. After analysing the logs and the data collected by the detection/prevention systems the company has deployed, an internal investigation supported by the external cybersecurity company determined with certainty that the perpetrator encrypted data. It is unclear if the data was exfiltrated or not.

The personal data affected by the breach relates to clients and employees of the company, a few dozen individuals altogether.

A backup readily available took place. However, an older backup must be restored as the latest backup was started right before the ransomware started encrypting data. The reinstallation of the compromised systems took 2 days. The backup that was restored, leaves the company with a 24hr data-gap (when comparing the data that was present, to the data in the backup). This results in several new customers not being present in the database, several orders are missing, several orders that had received payments now have an unpaid status. Only a handful of customers was impacted. No significant impact

was detected on the employee payments, as the missing data (absences) could be reconstructed, using the paper-based approval forms.

Presenting a case like this provides more context, and shows a number of preventive/mitigative controls, which illustrate that a company is exercising the necessary Due Care & Due Diligence. It also illustrates why the risk of not updating the software is based on a business decision. Even though it would be best to upgrade the system, doing so could cause massive harm to the business itself, as all the work that was done previously should now be completely redone.

This case can be reevaluated when looking at it from the viewpoint of different organizations.

- How would the response of the SA/EDPB change if?
    - The company was providing (lifesaving) medical equipment?
    - The company is a start-up. The customers are basically other institutions funding the research/development/prototype manufacturing that the company is currently doing.
    - What if the company provides work to ex-convicts/handicapped people (in for example the assembly line)?
    - What if the customers (PII) that are impacted are:
        - In the special categories section
        - High stakes CEO's from other companies
    - The infrastructure that was impacted was rented (such as an IaaS/PaaS/SaaS solution that was placed on-prem)
        - Would the response change if it was in the cloud?
    - The IPS (Intrusion prevention system) stops known malwares and ransomwares by default and proof can be provided that it actually works as it is tested on a regular basis. However, this one got through.
        - How would the response change, when considering:
            - There are known ransomwares with known signatures.
            - There are new ransomwares, whose signatures have not been created by the vendor, hence they cannot be detected/mitigated upon entering the network/server.
    - Would this layered approach contain enough alternate controls to replace the "encryption requirement"?
- Reviewing such cases can provide a better indication on "How much is enough?", "What is acceptable?"

3.5. CASE No 03: Ransomware with backup and without exfiltration (healthcare)

3.5.1. Considerations

When looking at this case, one can also say that the privacy regulation extends the "patient-doctor confidentiality principle".

It is only logical, that based on the increasing level of risk, and the variety of patient categories (minors, special categories, evidence of criminal activity), record quantities, should require better levels of protection than when just names, addresses and emails are gathered.

The integrity and availability aspect are even more important than the confidentiality.

Availability breaches may lead to the highest level of risk, being death … as critical procedures may not be performed due to the lack of availability of the required data.

Integrity is critical, as errors in the patient records may result in an erroneous treatment, medication that does not take allergies into account, etc. They may also lead to deaths.

The confidentiality factor is critical as well, but it can be considered if the same degree of damage can occur, when comparing with integrity or availability breaches. It is true that violations of confidentiality can cause other risks. (e.g. Loans/jobs can be refused based on the current medical state of a person). When looking at records about allergies, they too can lead to deaths.

When looking at breaches, the SA is probably not the only party that needs to be informed, as hospitals or the medical sector can be due to comply with different regulations. (HIPAA, JCI, and others ….). Also, other interested parties are linked to the hospital such as medical insurance providers, institutions performing research, external laboratories …. Often there is a form of data exchange between those companies. A breach in one company could cause additional damage to the records hosted somewhere else too. It can also be established that financial data, id numbers issued by the government are present in the dataset.

Breaching this set, could potentially also lead to identity theft & financial damage.

As this is a wide network, it would be wise not to just notify the SA, but also al the stakeholders that are involved.

Point 42 states: "*This breach concerns not only data availability, but confidentiality as well, since the attacker may have modified and / or copied data from the server. Therefore, the type of the breach results in high risk*."

- Confidentiality was breached in order to gain access to the data.
- Being able to modify the data is an INTEGRITY violation if the records have been changed. (for example, allergies were removed from the patient file)

The Case 03 – mitigation and obligations only illustrate the obligations. It does not present any preventative or mitigative actions.

3.6. General Comments

Ransomware attacks are becoming more complex as the involvement of third parties gaining popularity among data controllers. There are three important trends, involving third parties, as follows:

a. **'Cyber Liability Insurance'** – the insurance cover usually includes the cost of investigating a cybercrime, recovering data lost in a security breach, extortion payments demanded by hackers, and notification costs, in the case you are required to notify third parties affected.
b. **'Legal Advisors'** – represent data controller being held hostage and negotiate and execute ransom payment. Sensitive organizations, restricted by law to deal directly with hackers and pay extorsion money, are appointing third-party legal advisors to deal with hackers on their behalf.
c. **'Decryption Service Providers'** – claim to have skills and capabilities to decrypt data for multiple ransomware variants, whereas it is learnt that they simply pay the criminals themselves and pass the cost to the victim at a massive profit margin.

At the outset, the third-party involvement may elevate following concerns:

- Implications if the data controller has appointed legal advisor due to regulatory restrictions and required to report data breach to SA or to data subject.
- Investigators from insurance agency may also get involved in breach investigations and try to influence the risk/impact assessment outcomes (to safeguard their vested interest), and subsequently influence the decision to report the breach to the SA or to data subject.
- Involvement of decryption service providers in crisis situation, without any agreement on non-disclosure/confidentiality of the data, may significantly increase data confidentiality concerns.

Recommendation:

Undoubtedly, guidance for data controllers on engaging third parties is beyond the scope of this guideline document. However, the use-case on third party involvement may be considered in EDPB guidelines as it redefines the data controllers' mitigation approach and obligations.

3.7. Organizational and technical measures for preventing / mitigating the impacts of ransomware attacks

It appears that three critical controls are missing:

- Data at rest encryption to prevent the extraction/usage of PII/PHI
- segmentation of the LAN/Corpnet into VLans with definition of security zones to prevent access from compromised systems to all other IT-systems
- need-to-know principles to avoid that attacker gain access to all data with normal users accounts

The following clarification should be added (marked as bold) similar to Case No. 2 on page 9:
"The server of a public transportation company was exposed to a ransomware attack and its data was encrypted **by the attacker** ".
This clarifies that the data was not encrypted prior to the attack by the public transportation company.

3.8. Feedback on the guidelines issued

3.8.1. Guideline 49 page 13

3.8.1.1. Bullet 1, page 13

Suggest avoiding technical jargon where possible; remove the abbreviation “LAN" and replace it with "network".

3.8.1.2. bullet 2

Authorization and authentication mechanism in order to ensure that, if one account/device is compromised, this is not propagated to other accounts/devices automatically/easy. In addition, for admin level/privileged accounts, additional segregation steps are to be taken.

3.8.1.3. Bullet 3

Walkthrough of the data breach process and testing retrieval of the data/IT systems from back-up.

3.8.1.4. Bullet 4*:*

Threat hunting, identify potential threats based on the cyber kill chain, log monitoring through SIEM solutions, network monitoring tools (e.g. for anomalies), e-mail filtering.

3.8.1.5. Second bullet, page 14

In reference to the No More Ransom project, it should be stressed that once the data is retrieved via such a recovery method, it remains vulnerable to a subsequent attack if the root cause of the initial ransomware attack has not been detected and eliminated.

3.8.1.6. Fourth bullet, page 14

Avoid the use of technical jargon where possible; remove the abbreviation "2FA" and replace it as follows as done in bold: "Strong encryption and **(multi-factor)** authentication (..)".
It is advised to a note making readers aware that their government may have published guidelines on preventative and mitigating measures against ransomware attacks. The Netherlands has this 1, the UK, Belgium, and most likely, also other European countries. Perhaps this could be included in the disclaimer prior to the list of recommended measures.

4. Data exfiltration attacks

4.1. Case No 05: Exfiltration of job application data from a website

4.1.1. Thoughts when reading the case

When considering what types of data that were on the website, would it be possible to reconstruct these data, based on what can be found on social media? The personal data that were submitted might also be found on a linked in profile

Although in this case the scenario is about a job application website, a threat that the current employer can find out that the employee is looking for a new job can be added. An ethical dilemma rises, can the current employer fire an employee because the employee has applied to another job? Can the employer open a discussion with the employee on the subject? Or would this be invading privacy?

What level of risk is there for the data subject?

There is a vulnerability, but nothing defines how the vulnerability was exploited. There are many layers in the technology stack that could have led to the breach. SQL injection is just one way. It could also have been that the server was configured in an insecure manner. For example, there were ways to get console access, which led to full system access.

Another thing to consider is, whether or not the web-platform was created/built/maintained by the organization. Were IaaS/PaaS/SaaS solutions used? Were vendors involved? Were external developers involved? How mature/secure was the software/platform?

The case, a backup and upgrading the systems is proposed as a fix. This a temporary fix, as it does not involve a decent security plan, with regular updates, penetration testing, vulnerability management, user education nor the implementation of DevSecOps, or even supply chain and vendor management if cloud platforms or infrastructure was used.

When notifying the data subject, the organization needs to present measures that can reduce the potential impact, or measures that the data subject should take. In this case one can wonder about what the best advice would be in terms of “potential job loss, if the current employer finds out you were looking for a new position.”

4.1.2. Mitigation and obligations

Which secure backup database shall be used in this scenario? The system was for one month compromised and the infiltrator could even make changes to provided data AND the system. The only valid option would be to contact all applicants to re-enter their information into the (clean) system.

4.1.3. General notes on the guidelines issued

4.1.3.1. Content

" 213 such forms are possibly affected (...)". The 213 seems like a typo that must be fixed.

4.1.3.2. Guideline 51 page 15 and 70 page 18

It may be worth mentioning in this paragraph the governance side as well: security by design and privacy by design, as well as best practices to be had in mind from NIST, ENISA, CISA, ISACA, ISO. Additionally, the following may be mentioned: token management for authentication/authorization, monitoring tools – e.g. SIEM solutions.

4.1.3.3. Guideline 51, page 15

The comma *"(..) brute force, attacks (..)"* should be removed here. Considering escaping and sanitizing is explained here, it seems appropriate to address what a brute force attack is as well.
This will also clarify why *"a limited number of attempts to login* " (guideline 58, page 16) is an appropriate countermeasure.

4.2. Case No 06: Exfiltration of hashed passwords from a website

4.2.1. Thoughts when reading the case

The use of email addresses was discouraged, doesn't prevent email addresses from being present. The data can do damage. Hence what the actual risk is.

As basically any category of users can subscribe to the website (including ex-convicts, handicapped persons, minors), how is the "user category" defined?

As data subjects are informed via email (which was discouraged?), wouldn't the SQL injection attack also result in the email-addresses being exposed?

As this clearly is a system that uses hashes and salts, why are there no recommendations on MFA? (it may be overkill, but it is supported by a lot of web-applications such as Jooma, WordPress, Hum Hub…)

As SQL injection is used, there is always a possibility that other data have been exfiltrated as well. (AS it is easy to get the usernames & passwords, it will also probably be easy to use the same technique to gain other information). This potentially allows for the full disclosure of entire user profiles.

The case just talks about the passwords… but what if SQL injection also allows for getting data on food-allergies that are stored in a user profile?

At this time SQL injection is used to gather data, using a SELECT statement. SQL also allows for data deletion and modification. Hence, there can also be issues in terms of data integrity & availability.

The response of notifying the data subject should always occur.

Based on the additional questions, one can wonder about the requirement to notify the SA, as potentially other data was accessed as well.

4.2.2. Prior measures and risk assessment

Risk assessment should be expanded. A privacy officer or data protection officer consulting this guideline may have limited technical knowledge and may not be aware that exfiltrated hashed, yet unsalted passwords could be reversed engineered through rainbow tables. If the username were to be subject to a confidentiality breach, more personal could be exfiltrated by the attacker through impersonation by logging onto the website with the username and the reversed engineered password.
Frequently, people think it is safe when passwords are encrypted. It is important to address the effects of a strong password and multi-factor authentication here. This may also provide clarification on the seventh bullet in guideline 49 on page 14.
Something that should be addressed is that SQL injections may potentially also yield data integrity and availability breaches as such rights may have been made available to the attacker as well.

4.2.3. Feedback on the guidelines issued

4.2.3.1. Guideline 61, page 16

The verb is missing. Add it as follows as done in bold; "The breach should be documented in accordance with Article 35 (5) but no notification or communication **is** needed."

4.2.3.2. Guideline 70, page 18-19

The link to the referenced OWASP page is outdated. It has changed to simply: https://owasp.org/
(Seventh bullet, page 18) this text should be copied to the fifth bullet found on page 14 for consistency purposes.

4.3. Case No 07: Credential stuffing attack on a banking website

Not determined if this case is relevant. Banking sector also is a highly regulated sector, that faces with constant audits. The notifications and advice of the privacy regulator may be quite insignificant compared with the input of other regulators and authorities.

4.4. Organizational and technical measures for preventing / mitigating the impacts of hacker attacks

Missing IAST/SAST/DAST testing for the developing of the website components

5. Internal Human risk source

5.1. Case No 08: Exfiltration of business data by a former employee

The case should distinguish between two things:

- Data was exfiltrated while the employee was still at work and used post-firing of the employee.
- Data was exfiltrated occurred post-firing of the employee.

It opens up a discussion on:

- the HR onboarding/deboarding procedures
- the acceptable use & ethics policies
- the requirement to be able to copy data to potential unauthorized devices
- the use of unauthorized devices (such as perhaps usb flash drives)
- the authorization of BYOD devices (personal devices used for corporate purposes)
- the inventorization of materials used by that employee, the management and recollection of these devices

These cases span quite a few layers of the organization and require a great amount of processes & procedures for implementing a successful plan.

Multiple weaknesses can be identified in terms of these processes and procedures.

It should be considered if this discussion is about “privacy”, after all, there is a much bigger impact on the business. As the data exfiltrated was already known to the employee, the relevance and risk in terms of privacy could be questioned? They will still be contacted by the same person (even though he is now employed elsewhere). It is however true that there was a breach of confidentiality as those data were meant to remain “corporate property”.

5.2. Case No 09: Accidental transmission of data to a trusted third party

Accidents can always happen, and people can receive information that was sent by accident.

The best actions that could be taken are:

- Notify the sender, if emails were received by an unintended recipient. This allows the sender to check and resend to the correct recipient
- Delete the message instantly.
  - Even if data would be present, and they would be of value to you, you would still need consent to use them.

Regarding accidental use, it can be leveraged to promote awareness. The statement that this type of breaches can be avoided, would be saying that the risk level can be reduced to 0. Practically this is only possible in “utopia”. Accidents will always happen. In terms of accidents, the best way to handle them is through the incident response process.

Theoretically, data subjects should be notified as there is a threat that the data will be misused. Also, depending on the type of data, one should be contacting the regulator.

The context does NOT define the type/classification of the data involved. What if the additional data was about minors or people that need additional protection? When keeping this in mind, a discussion on the necessity of notification can be started, based on the potential risk each of the forementioned categories.

5.2.1. Prior measures and risk assessment

In order to avoid possible mistakes when a document in shared via email, USB, shared link, etc., it's necessary to use Information/Digital Rights Management so, if someone makes a mistake sending/sharing/delivering a document to a wrong person you can remove the rights for that particular person in real time, no matter where the document is. Even if you want to remove the rights for whatever reason, it's possible do it whenever, wherever the document is.

5.2.2. Organizational and technical measures for preventing / mitigating the impacts of internal human risk sources

5.2.2.1. Information rights management / Digital Rights management

Information rights management (IRM) is a subset of digital rights management (DRM), technologies that protect sensitive information from unauthorized access. IRM is a technology which allows for information (mostly in the form of documents) to be 'remote controlled'.

5.2.3. General comments on the guidelines issued

5.2.3.1. Guideline 74 page 19

Until detected there is no way of knowing that this was the only data copied or the only use for this data so the controller must be under the opinion that further breaches are possible until proven otherwise. Companies are under the requirement to assume the worst possible circumstances until they can provide certainty.

5.2.3.2. Guideline 76 page 20

It may be worth including: alerts when large amounts of data are extracted from the database (as this should not be done during usual business practices), monitoring printed materials to identify anomalies, DLP solutions, contractual obligations in place for employees (including confidentiality clauses) may prove good deterrent controls. A more complete solution would be accurate classification of data and protection mechanisms in place to prevent unauthorized ex-filtration of sensitive / critical information. DLP, UAM, PUAM etc. The level of data 'stolen' in this case shouldn't allow for a more relaxed response to the identified data. The actions in relation to the SA are acceptable. Only the last sentence makes sense. Put a clause into the contract.

5.2.3.3. Guideline 77 page 20

Why informing the SA is mandatory, but not the data subjects in this case? The company didn´t do anything wrong, but an ex-employee did.

5.2.3.4. Guideline 78, page 20

It may be worth mentioning that these kinds of breaches may also be mitigated throughout the implementation of a data loss prevention system. However, it would require some explanation of what that is. It can be noted that some non-security people generally are not aware of such a solution like this exists and may be valuable to point out...

5.2.3.5. Guideline 84, page 21-22

The use of anti-glare filters to avoid internal shoulder surfing could be added to this list, as also mentioned in guideline 105, page 25 (firth bullet). This list has many entries, but no real solution. The right thing to do is to implement Data Leakage Prevention tools for workstations and network to identify / notify / avoid the leakage of information.

5.2.3.6. General comment

It seems that there are plenty of departments who have little regard when onboarding new tools where the personal data of data subjects are processed. It is important to preach data minimization and data retention practices. Perhaps a final notice or reminder should be made at the end of this overall guideline on data minimization and data retention as general principles on preventing and mitigating the impacts of a data breach (and always to perform a root cause analysis).

6. Lost or stolen devices and paper documents

6.1. Case No 10: Stolen material storing encrypted personal data

6.1.1. Prior measures and risk assessment

It's necessary to deploy a security policy in the tablets regarding to when a password in set X times wrong (for example 10 times) the information in the tablet is erased.
To activate a GPS localization in order to find the tablet due to somebody move it to other site in the facility

6.1.2. Mitigation and obligations

If you send a command to erase the information in the tablet but the table never get coverage again, the command will not have any effect and with that mitigation the thief could break the password using brute force.

6.2. Case No 11: Stolen material storing non-encrypted personal data

6.2.1. Mitigation and obligations

It's necessary to deploy a security policy in the tablets regarding to when a password in set X times wrong (for example 10 times) the information in the tablet is erased.
To activate a GPS localization in order to find the tablet due to somebody move it to another site in the facility

6.3. Case No 12: Stolen paper files with sensitive data

6.4. Organizational and technical measures for preventing / mitigating the impact of loss or theft of devices

- To use devices with the feature "erase the information after 10 failed tries."
- To use devices with the localization features (GPS o similar)

6.5. General notes on the guidelines issued

6.5.1. Guideline 95, page 24

It is unclear on what is a considerable number of concerned individuals, e.g. that this generally is the case when >1k individuals are affected. A lot of people struggle with determining this.

6.5.2. Guideline 103, page 25

The scope of the paper logbook is unclear to me as it is referred to "a" logbook. This may imply that it is not possible to determine who the affected data subjects precisely are. Thus, it may be recommended to provide notification to all patients. Especially since there was no access control regime nor any other safeguarding measure, prior confidentiality or integrity breaches may have materialized.
The capital letter "C" is missing in one of the table headers.

6.5.3. Guideline 105, page 25-26

(Second bullet, page 26) Avoid technical jargon where possible; remove the abbreviation "LAN" and replace it with "network". Taking dumpster diving into account, it is advised to also include means of safe disposal of documents, such as using shredders that do not allow reconstruction. Why three product names for device encryption are listed here? There are many other solutions available. This should be deleted. Multifactor authentication to log-on to devices? What´s about biometric measures?

7. Mispostal

7.1. Case No 13: Snail mail mistake

Snail mail mistake: clear but as said in the previous global remark, explicating why this case is not a high risk for the customer (likelihood of the recipient using it for fraud) could be beneficial.

7.2. Case No 14: Sensitive personal data sent by mail by mistake

As for security measures, Information Protection tools that immediately classifies documents containing personal data as internal and therefore any email containing such data could be a good security measure.

7.3. Case No 15: Personal data sent by mail by mistake

7.4. Case No 16: Snail mail mistake

The reason for not communicating to data subjects should be made clearer

7.5. Organizational and technical measures for preventing / mitigating the impacts of mis postal

Additional measure: Information protection tools offering automated classification documentation and associated encryption for high risk data

7.6. General comments to the guidelines issued

7.6.1. Guideline 111, page 27

Advise adding the example of identity fraud as a possible risk in relation to the confidentiality breach of the social security numbers. Previous cases throughout this guideline have emphasized such risks before as well.

7.6.2. Case No. 06, page 28

A reference is made to "Article 9 GDPR" whilst the rest of this guideline does not add "GDPR" after each reference. Suggest consistently adding or removing this throughout the entire guideline.

7.6.3. Guideline 117, page 28 & guideline 123, page 29

"Bcc" and "'bcc'" is used inconsistently.

7.6.4. Guideline 123 page 29

The option of automating the emailing process may be included – e.g. through RPA, thus avoiding manual errors.

7.6.5. General comment

"E-mail" and "email" is used inconsistently throughout the entire guideline.

8. Other cases – social engineering

8.1. Case No 17: Identity theft

Clear. However, offering an out-of-band multi-factor authentication to all clients seem quite a pricey solution, other solutions like extra questions, snail mail to home address, multi-factor through a registered device could be also advisable.

8.2. Case No 18: Email exfiltration

8.3. General comments to the guidelines issued

There are no organizational and technical measures listed? Training (best ones are red team followed by debriefing with the end users), secure email gateway solution, DMARC DKIM, updated systems.

8.3.1. Guideline 128 page 30

For case 17 communication to data subjects is needed because the possibility of identity theft or because of the data disclosed to the impostor? It is not clear from the text.

8.3.2. Additional cases:

- mispostal: the use of online sharing tools has been recently intensified; an easy mistake would be to copy paste a file into the wrong channel. There are measures in Microsoft tools to authorize the exchange of documents only to whitelisted domains.
- for social engineering it could be interesting to add an example where notification to data subjects is not necessary
- internal human risk source: a case of exfiltration from an employee where all the data has been recovered before it could be sold to other parties would be interesting. It seems the notification to Authorities is mandatory but not the interested parties.

9. Another discussion – publicly available data aggregation can form a similar risk.

When looking at the risk to the rights and freedoms of the data subject one can also open up a discussion on the responsibilities of the data subject. Humans will always be the weakest link in the security/privacy chain.

After all, what if data is collected (such as name, address, date of birth, …) which are also publicly available when browsing social media. That is, why should the organization notify the SA/EDPB when low risk data is breached. Data that can be derived from browsing social media or simply searching the web? After all, these data are not encrypted either.

This discussion can be extended, as multiple publicly available data sources from different social media can be combined.

An example:

Targeting an individual or company is quite easy

- Run the name through google.
- Run the name through Facebook
  - Social connections
  - Birthdate
  - Possible holidays and dates can form patterns, which could be analyzed and used as timing for an attack.
  - Profiles contain information that can be used to trigger social engineering malpractices.
- Run the name through linkedin
  - Corporate information
    - Running the company through google may also reveal additional contact details (address, phone number), customer details (as in success stories), affiliations.
    - Combined with the information of people connected to the company, individuals or groups of individuals can be targeted too. To some extent this may also allow for impersonation attacks which can cause different levels of risk for the individual.

At this point, when combining all the data found, one can construct a dataset that can bring bigger harm to the rights and freedoms of the data subject than the customer data hosted in our database.

When aggregating such datasets, malicious emails could be started, phishing campaigns, malware, targeted advertising, etc.

Therefore, the legal aspect can be seen as using different weights and measures. Corporations are punished for not complying with privacy, while the data subject is permitted to spread his PII everywhere (some people are not even aware of the dangers).

Combine this with potential password breaches on these social media, and even more potentially harmful situations can be exposed in terms of security & privacy risk.

If due to the information that is found online, systems can be breached, or people can become the victim of well-designed social engineering does that mean the company that does it's best to protect the PII of data subjects should be held accountable?
In theory yes … but in practice? Was the company negligent? Or was the data subject negligent?

In terms of legal proceedings, this can lead to interesting discussions. Security and privacy measures always have a weak link. The weak link could be at the company side, but it could also be at the data subject side.

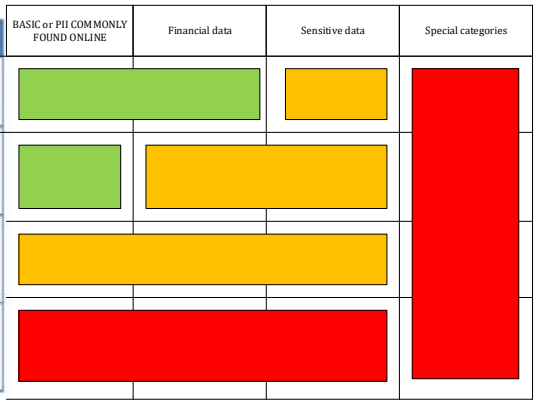
Even though this is out of scope for these guidelines, it should be considered in terms of whether the SA should be notified, as well as in when considering potential damage claims and fines.

10. Deciding on notification

Based on the risk definition provided by ENISA, should the decision on who should be notified can be reduced to a simple matrix, that uniformly defines which actions should be taken.

An example of such matrix can be seen as follows:

Severity of a data breach		
SE < 2	Low	Individuals either will not be affected or may encounter a few inconveniences, which they will overcome without any problem (time spent re-entering information, annoyances, irritations, etc.).
2 ≤ SE < 3	Medium	Individuals may encounter significant inconveniences, which they will be able to overcome despite a few difficulties (extra costs, denial of access to business services, fear, lack of understanding, stress, minor physical ailments, etc.).
3 ≤ SE< 4	High	Individuals may encounter significant consequences, which they should be able to overcome albeit with serious difficulties (misappropriation of funds, blacklisting by banks, property damage, loss of employment, subpoena, worsening of health, etc.).
4 ≤ SE	Very High	Individuals may encounter significant, or even irreversible, consequences, which they may not overcome (financial distress such as substantial debt or inability to work, long-term psychological or physical ailments, death, etc.).



When looking at the colors, a scheme can be created that combines the risk severity, with the type of data involved. Such guidance would make the expectations clearer and would provide more guidance on the levels of risk that each category poses. Currently, everyone is trying to re-invent the wheel.

The columns basically determine the data type, classification, and minimum protection that should be present in the 5 domains:

- Identify
- Protect
- Detect
- Respond
- Recover

Based on the color coding, uniform guidance can be provided on who to notify, ….

- SA/EDPB/Regulators
- DS
- Other authorities

Green could be:

- notify the DS (mandatory)
- notification to the SA (not mandatory)

Orange could be:

- notify the DS (mandatory)
- notification to the SA (can be mandatory, could depend on the volume of data, or the impact of confidentiality/integrity/availability impact)

Red could be:

- notify the DS (mandatory)

- advice must be requested from the SA prior to using these data categories (mandatory)
- notification to the SA is mandatory.

Such matrix could make it easier for small size corporations to understand what the GDPR/EDPB expects them to do. After all, if 100 people are asked to assess a risk, they will all do it in different ways, and come up with different results.

Minimum set of protective measures that are recommended can be linked to the severity of the data breach columns. Most frameworks use this type of tiering for specifying controls that apply.

Also, guidance on alternate controls should be provided, combined with guidance on how to build, manage and maintain a program.

Topic 5.4 will also illustrate the vagueness and subjectivity of the regulation.

11. General considerations

11.1. Choice of the title

The title of the document causes confusion. One expects to see less information on the actual preventive and mitigative controls, and more on the breach notification as well as an elaboration on the degree of risk for the data subject.

11.2. Choice of content

The document itself bounces between control sets, breaches and notification, based on vaguely formulated cases. The “outcome” is formulated, yet almost no information is available on the preventive/mitigative controls present. This can lead to the assumption that there were no controls in place.

One thing that is interesting is that in the end the SA will define what acceptable risk is, and whether the organization has provided enough means for protecting the data.

In the notes Encryption is used as the “buzzword” that solves each problem as it makes data unusable for non-authorized people.

The recommendations made, are not based on decent root cause analysis of the cases. As a real root cause analysis (as discussed in the review of the cases) could show different series of events, that lead up to the same issue. Even though the advice posed be correct, it is far from complete, and mainly resorts to technical measures and SETA.

11.3. Choice of cases

Even though the cases are interesting, they have been presented in an overly simplified manner. A decent amount of context is missing, making their recommendations in the prevention and mitigation section, being the “answer” to such cases. In a way, it provides some guidance on when to contact the SA.

Yet, it seems to be missing a lot of information about the actual incident management process and how breaches should be reported. Also, information on how the breach notification will be handled by the SA is missing.

It is true that they are an authority, but what if you disagree with the “recommendations”. After all their van be business reasons that can justify this. In result, it can be said that when done properly security and privacy can enable a business. When security and privacy need to be designed as add-ons, they can cause conflicts of interest between the EDPB and the company.

- the enforcement of certain controls by the EDPB may not be feasible (due to historical decisions/investments), yet they are deemed mandatory for protecting the data and avoiding breach notification to the SA. The impact of alternate controls is not discussed, and the use of such alternate controls may still trigger a breach notification to the SA)
- When doing the actual breach notification, and presenting the actual controls in place, is it possible to do a decent assessment of the impact of such controls, or if they will point one yet again towards the controls they deem to be the solution to every problem. (encryption)

Another thing that strikes me is that there is not a word about the controller/processor notification. After all, if you have data exchanges in place between a controller/processor, an integrity issue in the dataset of the controller may also get replicated to another processor.

There is also no case present where the breach occurred at a processor. (Who is basically responsible for notifying the controller. However, resolving the problem is a part of the processors duties). This raises interesting questions in terms of the use of cloud-based solutions, vendor management, supply chain, contractual obligations and roles & responsibilities.

The WHEN is defined in the legislation as 72 hrs post-breach detection.

What information do they expect? How should it be formatted? Where can you find help & guidance?

11.3.1. Infosec vs privacy

It is true that the GDPR mandates that adequate security is in place, so that the rights and freedoms of the DS are protected. However, one can wonder about whether the EDPB is the right party to formulate advice on processes, procedures and technical measures.

If their advice is considered binding, one can also wonder how this will impact companies that strive for ISO 27001/27002/…. security/privacy compliance.
Key here could be that those companies face audits and have decent programs/procedures and policies in place. It can thus be assumed that they have adequate protections in place. Notifications to the EDPB could then also be “accidents” that have happened.

However, small size companies may not always have this in place as budgets and resources are not present for such a devious task. At this point, I’m not sure if the advice of the EDPB is enough, comprehensible, usable for such organizations. After all, there is always room for improvement. The influence advice of the EDPB may result in forced expenses in security (which have a minor benefit to the organization), and which may thus inhibit growth.

Instead of reciting articles one should comply with, it may be advisable to create some form of “free advice” center, that works on decent guidance for different organizational branches, based on the data that is used.

Compare this to the following:

- In Belgium, when a person fills in their tax forms, they can make an appointment with the tax department to receive help filling in the form, or even have it done for them. Based on the information and documents provided them. As the legislation becomes more and more complex, it has become quite difficult for normal people to know what they can and can’t do. This is all done free of charge.

Based on the requirements (security/privacy), a crew of experts would be able to help design/implement/manage your program. A restriction that could be imposed is that this “free” service is available for companies with a maximum revenue of x euro. This is a very valuable service for people starting an organization.

As actual cases, with actual context are presented, handled, it could also result in documents such as this one, where a full approach to the case is presented. Also, cases such as described

in this document can be given a proper content. Improvements on controls can be formulated, as well as reasons on how certain controls do not apply, or provide less benefit in the context of a given topic.

11.4. General remarks

The paper would benefit from explaining why the data breach is likely to result in a risk to the rights and freedoms of the data subjects. When comparing cases that need a communication to data subjects, it appears the difference is not clearly stated: for instance, 5.2 vs. 6.1 in both cases personal data including names, surnames, addresses were leaked. The differences are regarding:

1) volumes (5.2 10000 and 6.1 2)
2) other personal data (5.2 including sex and birth date)
3) intention (5.2 voluntary and 6.1 by mistake)

What are the criteria that made 5.2 mandatory for a communication to data subjects and not 6.1? The paper only concludes on the level of risk but not how the analysis was made. Perhaps it has to do with the likeness of the data being used and the impact it would have but concrete examples would help. As a customer even if it is an error, the impact of sending the data to someone who could use it against me is important, so is the likelihood =factor 3 the only factor in this context?

If another document from EDPB is focusing on this element, the introduction should refer to it. The document “Guidelines on Personal data breach notification under Regulation 2016/679” is a bit more explicit but ideally a list of all criteria that should be considered could be very helpful.

It is suggested to add example cases where a processor/vendor has experienced a data breach that affects a controller. The world is becoming more and more dependent on thirds-parties. Guidance should be provided how a processor and controller should act in such a situation. Additionally, add an example on how a controller determined that a vendor had implemented appropriate technical and organizational protection measures.

The responses/actions generally are sufficient from a pure privacy regulation point of view. However, in practice more actions may be required due to additional legal agreements made. This may be disregarded by accident and therefore adding a general notice to this guideline is by no means exclusive and the reader may need to address additional considerations that may apply to them as well (e.g. customers may always want to be notified of a breach regardless of the risk and within 24 hours)..

On that note, it is advised to highlight that the examples within the guidelines are simplified and in a similar way, the considerations made during the risk assessment and mitigation may differ in your situation. Especially when it comes to cybersecurity; a subject matter expert should be involved. E.g. this guideline overall seems to heavily rely on logs to determine the impact on data subject while it's common for attackers to modify logs.

Add an appendix with a brief flowchart on how the data breach notification process generally works. The Dutch DPA provided a chart in one of their guidelines on adopting the GDPR and it helped me to easily navigate a colleague on what considerations must be made.

Overall, the community looks forward to the formal publication of this entire guideline as it sufficiently addresses various scenarios that may be slightly adopted to be relatable to various organizations.

Levels of probability and impact of misuse/negative consequences may be useful to be included, with examples (as in the CNIL guidelines). There are examples of degrees of impact/probability mentioned in the document, but without reference to an objective rating matrix that can be used.

11.5. Notes from the IAPP CIPP/E handbook

Source: European data protection- Law and practice and iApp publication (iapp.org)

11.5.1. Art 33 – notifying the regulator

"Once a suspected breach is detected the controller needs to determine whether it meets the definition of personal data breach and if so, whether it is of a kind that is likely to cause risk to the rights and freedoms of individuals. "

*"Controllers could easily get lost in their deliberations about whether the breach is or **is not likely to result in a risk to the rights and freedoms of individuals**, but the language used in Article 33 seems to set a very **low bar for notification**. This is because the concept of risk is not subject to a severity threshold and because the concept of rights and freedoms is exceptionally broad." (page 178 – 10.3.2)*

This makes the risk assessment a rather subjective exercise, as there is no "official" taxation of the risks involved. When considering how the breached data could be consolidated with other sources, it even becomes more guesswork.

Yet *Recital 76 states that the likelihood and severity should be assesses objectively*.

Although the intent is present, considering all possible scenarios on how data (and data aggregation) can impact rights and freedoms is a cumbersome task that will probably have a subjective outcome.

11.5.2. Art 34 – communicating the breach to the data subject

"Article 34 requires controllers to inform data subjects of personal data breaches if those breaches are likely to present high risk to the rights and freedoms of individuals. "(page 179 – 10.3.3)

"Article 34 (3) sets out an exception to the notification rule. The first exception is where measures have been taken to render personal data unintelligible, for instance by the use of encryption. This is often called the 'encryption safe harbor' because application of a security control releases a controller from notification obligations" (page 179 – 10.3.2)

"Article 3 : the communication to the data subject shall not be required if the following conditions are met:

a) The controller has implemented appropriate technical and organizational measures and those measures were applied to the personal data affected by the personal data breach, in particular those that render the personal data unintelligible to any person who is not authorized to access it, such as encryption.
b) The controller has taken subsequent measures which ensure that the risk to the rights and freedoms of data subjects is no longer likely to materialize.
c) It would involve disproportionate effort. In such case, there shall instead be a public communication or similar measure whereby the data subjects are informed in an equally effective manner." (GDPR)

This also implies that the use of encryption is the easy-way-out. However, there are several additional controls that are needed to protect the encryption keys. A failure to implement such controls may also provide an attacker with the encryption keys, allowing him/her to make the unintelligible data usable once more. Hence, is "the use of encryption" (which is heavily promoted by the EDPB) is really the god-like solution?

Another thing to consider is how to define "appropriate technical and organizational measures". This can only be determined by skilled security and privacy professionals. Hence it may require an investigation by an independent auditor.

There are a few questions that rise yet again:

- What is acceptable and where can one find the middle ground between the legal aspects and the practical aspects?
- What is appropriate? That is, how much security is required in order to create an appropriate security plan for the PII.
- What is mandated?
    - *This refers back to Article 5(1)(f), which states that personal data must be "processed in a manner that ensures appropriate security of personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures ("integrity and confidentiality")"*
    - *Encryption is the easy way out.*
- As many companies appoint an internal person as DPO (specially in the SME companies, is he the right person for the job? Ais the company working towards a paper based compliance as they "do their best", since the risk impact determination is subjective)
- What is technically and economically feasible?
- Who determines the standard?
    - When doing a proper implementation frameworks and certifications could be used. Getting a certification may entitle you to a quality label.
    - This also raises concerns about the financial impact on a company as well as on the resources and skills that would need to be present.