WARDYNSKI & PARTNERS

Managing Ransomware and Data Breach Incidents

MAY 2024

Contents

Nature and scale of the threat

What is ransomware?

Ransomware is a kind of malicious software (malware) that prevents a user from accessing their files, systems or networks, designed to extract payment (ransom) from the user.

Such software can be downloaded for example by opening an infected email attachment or clicking an ad online, or because a vulnerability in software used by the victim organisation, exploited by hackers aware of the flaw. Typically, when downloaded or installed the malicious software encrypts all the files and information it can, making them unreadable to anyone but the owner or creator of the malware. The deployer then attempts to extract payment in return for a decryption key, allowing the victim access to the locked files and systems.

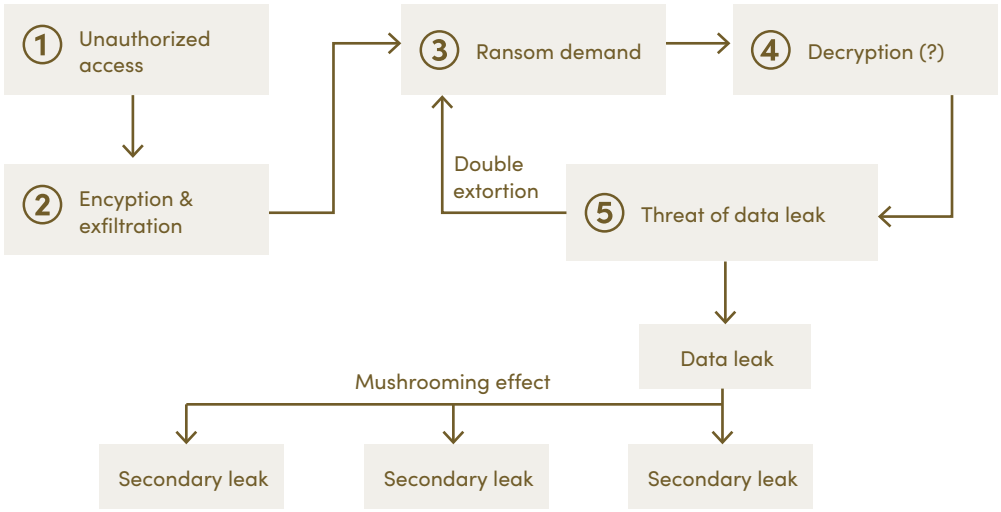
Evolution of ransomware: leakware and double extortion

Over time, this initial model has evolved greatly, especially as organisations have employed more sophisticated detection measures and more effective backup systems. The perpetrators shifted their focus from encryption of sensitive data to extortion of the data itself. Following an attack yielding unauthorised access to confidential data, the hackers inform their victim that the data was extracted to a controlled location, and if ransom is not paid it will be publicly leaked. The perpetrators usually use a "shaming site" on the dark web for this purpose, where the identity of the victim and a timer counting down to the payment deadline are visible and, if payment is not made in time, the actual data is made public. This newer variant of ransomware is called "leakware."

A hybrid model, involving both encryption and a subsequent threat of publishing the sensitive information, has also become popular. As in the standard ransomware model, hackers demand an initial ransom payment in exchange for providing an encryption key. But even if it is paid, they come back for more, informing the victim that they are still in possession of some form of confidential or sensitive information, which they will leak unless another ransom is paid. This variant is called a "double-extortion" attack.

Today, the basic model of ransomware is relatively rare in practice, with most attacks employing a hybrid approach. For simplicity, we will use the general term "ransomware" to refer to all possible variants.

Diagram of a typical double-extortion ransomware attack



Rising significance of ransomware and data breaches

Ransomware and related data breaches are one of the most significant cyber-threats faced by organisations globally, including in Poland and other EU countries. It ranked no. 1 in 2023 in the number of reported incidents according to the European Union Agency for Cybersecurity (ENISA), with over 30% of all analysed types of incidents that year constituting some form of ransomware.

The business model of criminals employing these attacks is evolving constantly, making them even more dangerous. Because of the rise of professional groups performing ransomware attacks in exchange for a fee ("ransomware-as-a-service"—RaaS) and the rising availability of ready-made "exploit kits," making such attacks simpler to carry out, even SMEs—offering lower payouts but often using less-sophisticated defences—are becoming tempting targets.

With ransomware and other types of incidents becoming ever more prevalent, the unfortunate truth is that it is only a matter of time before an organisation faces the consequences of this type of threat. Meanwhile, no technical or administrative security measures are foolproof. In the current hostile environment, to consider themselves fully prepared, organisations need to plan how they will handle a data breach if it occurs.

Preparation and planning

Appointing an incident response team

With any type of cybersecurity threat there is a temptation to view it solely as a technological risk. But this is a fallacy, as it leads to the erroneous conclusion that the prime solution to such threats is also technology. In many data breaches, the perpetrators are able to execute the attack not because they have overcome technical controls employed by the victim (devices such as firewalls and intrusion detection systems, or secure systems architecture), but by exploiting the human factor, through phishing or other forms of social engineering.

Since cybersecurity is primarily a people problem, it is only fitting to begin preparing for the worst with the people who will be responsible for handling the data breach—the members of the incident response team (IRT). After all, establishing a dedicated IRT (together with implementing a documented incident management policy and procedures) is considered one of the basic steps when preparing to handle information security incidents. But who should be on the team?

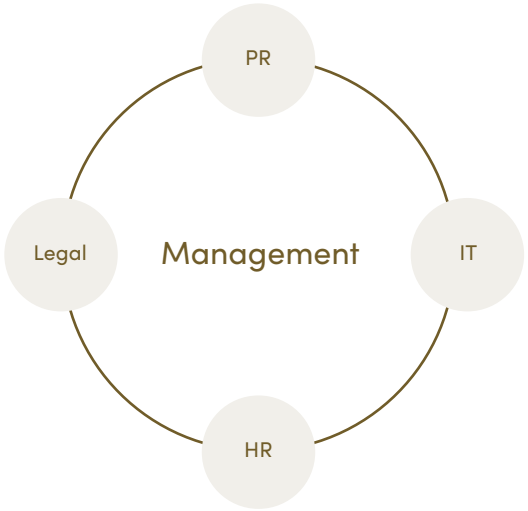
During the initial stage of a data breach, much of the burden is naturally on a company's IT staff or dedicated information security department, who are focused on countering the attack or restoring access to the affected systems and returning to normal operations. Technical staff are a necessary and significant part of any IRT. However, managing a data breach requires a broad spectrum of skills and competencies, not just raw technical prowess alone. For example, if the data breach involves employee records, HR must be looped into the decision-making process and focus on managing employee concerns. Once the breach is made public, members of the PR or communications team should focus on managing reputation risks and crisis communication with clients and other stakeholders. Finally, the legal department has an important role, considering the potential lawsuits and investigations waiting around the corner. Other personnel may be included in the team as well, for example the data protection officer or compliance officer.

The role of management

All these people have different roles and concerns in the case of a data breach, which sometimes can lead to conflicting priorities. For example, the IT staff will be naturally concerned primarily with restoring access to data and systems—that is their job, after all. Confidentiality, not so much, at least if it has already been breached. The legal department on the other hand usually focuses on issues of confidentiality of data, and potential consequences of breach of confidentiality, to the exclusion of other concerns. Furthermore, nearly all cyber threats, data breaches in particular, first and foremost pose a business risk. The unavailability of data and systems is problematic because it prevents normal business operations, while a breach of confidentiality can undermine the confidence of key clients and impact future revenue streams.

That is why it is critical that the IRT be headed by a sufficiently senior member of management, preferably someone from the management board—someone who can act effectively as a mediator between the different departments involved, accurately assess the impact of various aspects of the incident on critical business functions, and prioritise accordingly.

Composition of typical incident response team

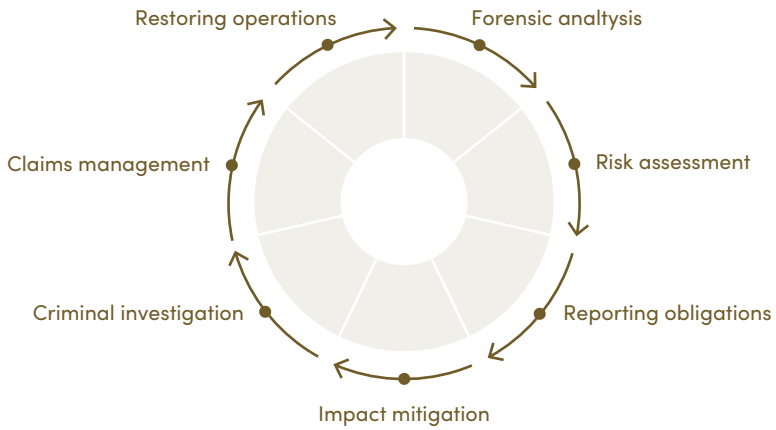


Overview of the incident management process

One of the more common approaches is to divide the incident management process into five phases: (1) Plan and prepare, (2) Detection and reporting, (3) Assessment and decision, (4) Responses, and (5) Lessons learned. While the ISO 27035 standard framework is a helpful tool in organising an incident management policy or procedure when considering a wide range of cybersecurity risks, it does not necessarily describe the process with sufficient granularity to help understand what needs to be done in the case of a data breach.

That is why we suggest looking at the incident management process from a different perspective—not necessarily as distinct phases occurring in a specific order, but by dividing it into discrete tasks or goals that must be addressed according to the priority decided by the head of the IRT. We have consequently devised the following incident management matrix, which breaks down the tasks that need to be handled in the process of managing a data breach:

Incident management task matrix



Each of these tasks is described in more detail in the sections below and should be covered in the organisation's incident management procedures.

Initial response—restoring operations and assessing risk

Restoring operations

Once it becomes clear the organisation is facing a ransomware attack, the most urgent matter is usually to contain the threat and restore affected systems to normal operations. This can involve anything from gradually restoring the relevant data from backup solutions and verifying its integrity, to preparing stopgap measures (e.g. temporary applications or scripts) allowing critical business functions to continue running while the full recovery efforts go on. This is obviously the primary concern of the IT or information security staff, and the most technical aspect of the incident management process. Restoring the availability of affected data and systems is crucial not only because it will allow the organisation to resume normal business operations, but also because it may be relevant from the perspective of potential liability towards customers or other stakeholders.

So it should come as no surprise that most cybersecurity experts and guides focus on this particular aspect of incident management. However, while restoring the availability of data, systems and infrastructure is obviously of huge importance, we believe that it does not necessarily require a great degree of input from senior management or other members of the incident response team. Hence our guidelines focus more on other aspects of the incident management process.

Forensic analysis

Usually, alongside efforts aimed at restoring operations, an equally urgent and important task involves forensic analysis of the affected data and systems, to establish what exactly has happened and the extent of the threat to the organisation.

While this can be done in-house by the internal IT team, consider hiring an external expert to assist with the forensic analysis. Unless your organisation has a dedicated information security department, distinct from the general IT department, the IT staff may be overwhelmed with the task of restoring operations and unable to effectively address other issues, such as securing and analysing available evidence of the attack. And internal IT staff may sometimes be wary of reporting flaws in existing security measures, which they

themselves have overseen. In general, a fresh set of eyes may help relieve the employees, and provide a much-needed perspective.

Cross-border data breaches

If a ransomware attack has had a cross-border effect, e.g. impacting not only HQ but also foreign subsidiaries, it is strongly recommended to hire a local forensic expert in each affected jurisdiction. They will be better placed to secure evidence quickly, and review it thoroughly, than sending in a team from afar. HQ can, and should, retain a "lead expert" to coordinate and supervise the local experts and their work product. Also be mindful of data protection regulations when forwarding data from local experts for subsequent analysis by the lead team, especially to countries outside the EU.

A proper forensic analysis should address as many of the following questions as possible:

- What was the attack vector? (How did the attackers manage to infiltrate or overcome the victim's defences? Did the perpetrators exploit a software vulnerability, or was phishing or other social engineering techniques the source of unauthorised access?)
- What was the timeline of events during the attack? (When did the perpetrators gain unauthorised access to the organisation's IT systems? When did they exfiltrate the data?)
- What "indicators of compromise" (IOCs—evidence that the intrusion has indeed occurred) can be uncovered and secured?
- What type of malware was used? Who or which group was responsible for the attack? Is a decryption key publicly available?
- What resources (networks, systems) were affected by the incident? What particular data may have been accessed or copied?
- If any data was copied, to what location did the perpetrators exfiltrate the data? Who hosts the server?
- What was the C2 (command and control) infrastructure used to coordinate the attack? Where are the C2 servers located, and who hosts them?

Sometimes not all this information will be obtainable (often, only a small part of it), but the more details can be obtained, the better the IRT can plan and execute the response. For example, it can help identify who was responsible for the root cause—the initial unauthorised access to the system. If the incident was made possible by vulnerabilities in software from an outside provider, the victim may have civil recourse against the third party. Similarly, if the initial breach is tracked to an employee who violated existing cybersecurity protocols, disciplinary action or civil claims may be in order. Details from the

forensic analysis can also assist local law enforcement in their investigation of the incident.

The results of this forensic analysis should be documented in a formal report, and any evidence gathered during the investigation should be appropriately secured, ensuring its integrity (e.g., the experts should prepare a so-called forensic image of the relevant IT assets). Occasionally, two versions of a report can be drafted: an abridged version for wider circulation among clients affected by the breach or the relevant authorities, and a full version solely for internal use.

Risk assessment and inventory of affected assets and parties

While the forensic analysis is ongoing, it is crucial to prepare an inventory of the affected data and any third parties that are, or will be, affected by the incident. Affected data should be assumed to include data that was encrypted or copied, or data which the perpetrators at least had access to. If it is not possible to identify specific data, as will sometimes be the case, identifying at least types or categories of data will be helpful. The list of affected data or categories of data should also help identify third parties potentially affected by the breach. These could include clients, with records of business with the victim, suppliers with similar concerns, or employees, whose personal information was stored as part of their application and employment.

This inventory of affected data and parties (together with the results of the forensic analysis) will allow legal advisors to conduct a thorough analysis of potential liability, and any claims third parties might have. Additionally, it will allow counsel to determine the scope of regulatory obligations and risks for the victim. For example, different types of compromised data carry different reporting obligations. Personal data breaches will likely require reporting to the national data protection authority or notification of the data subjects, whereas if any classified data was breached, the incident will need to be reported to national security or intelligence agencies. The more granular the inventory and the forensic report, the more actionable the subsequent legal advice will be.

Once the inventory and forensic analysis have been completed, the IRT (counsel in particular) can prepare an initial legal risk assessment and mitigation plan for the incident. The plan should address the remaining tasks from the incident management matrix (reporting obligations, impact mitigation, criminal investigations, and claims management), and assign priority to each of them.

Reporting obligations

The moment an organisation becomes aware that its data may have been breached, the clock starts ticking. Most jurisdictions have some form of obligation to report data breaches. Knowledge of the incident is vital for affected third parties (e.g. employees, customers and suppliers) to defend against the consequences of a leak. Thus the regulations often require victims to notify not only the authorities, but these third parties as well. The regulations usually impose tight deadlines for reporting, counted in days or hours, not weeks or months.

Personal data breaches

In Poland, as in other EU countries, the most common reporting obligations pertain to personal data breaches.

Under the GDPR,[1] in case of a personal data breach the data controller[2] is required to notify the breach to the competent supervisory authority without undue delay, not later than ***72 hours*** after learning of the breach (similarly, a data processor is required to notify the controller without undue delay). In Poland the competent authority is the President of the Personal Data Protection Office (PUODO). Notification can be done in several ways, including by completing an online form at: biznes.gov.pl/pl/opisy-procedur/-/proc/889

The notification should include, among other things, the following information:

- The nature of the personal data breach, including where possible the categories and approximate number of data subjects concerned, and the categories and approximate number of personal data records concerned
- The likely consequences of the personal data breach
- The measures taken or proposed to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects
- The date and time when the personal data breach was discovered
- Information about other authorities (including data protection authorities in other jurisdictions) who have been notified of the personal data breach.

1 Regulation (EU) 2016/679 of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation).

2 A data controller collects or possesses the data for its own purposes, as compared to a data processor, which is a third party engaged by the controller to process data for a specific purpose on the controller's behalf.

It is possible to submit a preliminary notification to meet the short 72-hour deadline, with further details added later as the forensic investigation yields more information.

If the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller is also required to communicate the personal data breach to the affected data subjects without undue delay. This is a particularly good moment to actively involve the PR team in the incident management process, particularly if the affected personal data belonged to people from outside the organisation, such as customers and suppliers.

Entity-specific incident reporting—NIS2 and DORA

Certain types of entities within the EU are also subject to a special cybersecurity regulatory framework with additional incident reporting obligations. This applies to "essential and important entities"[3] subject to the NIS2 Directive,[4] and financial entities subject to the DORA regulation.[5]

Under the NIS2 Directive (and implementing legislation in each EU member state), essential and important entities subject to it are required to notify without undue delay any incident that has a significant impact on their services, to the applicable, country-specific computer security incident response team (CSIRT). NIS2 provides for a complex multistep notification procedure, but essentially requires early warning of the incident to be given within ***24 hours*** from becoming aware of it, and a final detailed report submitted within one month after that. Much like with personal data breaches, NIS2 also requires essential and important entities to notify the incident to recipients of their services, if the incident is likely to adversely affect the provision of those services. In Poland, except for government and financial entities, most essential and important entities are required to report incidents to CERT Polska, which can be done at incydent.cert.pl

Similarly to NIS2, certain financial entities (such as credit institutions, payment institutions and investment firms, but also insurance and reinsurance intermediaries) are required by DORA to follow an analogous multistep notification procedure in case of major ICT-related incidents. The deadlines,

3 Including for example entities from the energy, transportation, and healthcare sectors.

4 Directive (EU) 2022/2555 of 14 December 2022 on measures for a high common level of cybersecurity across the Union (NIS2 Directive).

5 Digital Operational Resilience Act, i.e. Regulation (EU) 2022/2554 of 14 December 2022 on digital operational resilience for the financial sector (DORA).

which are defined in secondary implementing legislation (Regulatory Technical Standards (RTS) and Implementing Technical Standards (ITS)), are similar to those required by NIS2 (i.e. ***24 hours*** for the initial notification and no longer than one month for the full report). In Poland the regulator designated to receive major incident notifications from financial entities is the Polish Financial Supervision Authority (KNF).

Other possible reporting obligations

There are other types of notification requirements depending on the nature of the data or the status of the victim. One example pertains to classified government information (information deemed "restricted," "confidential," "secret" or "top secret" from the perspective of national security). Under Polish law (the Act on Protection of Classified Information of 5 August 2010), any breach of provisions pertaining to the processing of information classified as "confidential" or higher must be reported ***immediately*** to either the Internal Security Agency (ABW) or the Military Counterintelligence Service (SKW).

Additional incident reporting obligations may also stem from contracts with certain customers or suppliers, particularly with respect to any trade secrets or other confidential business information. That is another reason to determine which third parties may have been affected by the data breach, so the organisation knows which contracts to review for the existence of such clauses. If the organisation has insurance covering cybersecurity risks, it should also consult the policy to identify any independent reporting obligations.

Examples of data breach reporting obligations and applicable deadlines

Source	Scope of application	Deadline
GDPR (EU)	Personal data breach—notification to national data protection authority	**72 hours**
NIS2 Directive (EU)	Incident with significant impact on essential or important services—early warning to national computer security incident response team	**24 hours**
DORA Regulation (EU)	Major ICT-related incident—initial notification to national financial regulator	**24 hours**
Act on Protection of Classified Information (PL)	Breach of information classified as "confidential" or higher—notification to Internal Security Agency or Military Counterintelligence Service	**Immediately**
Contractual provisions	For example, breach of trade secrets or confidential information protected under an NDA	**Varies depending on contract**

Finally, the organisation may consider disclosing the ransomware incident voluntarily, for example to key clients or employees, as part of the crisis communication and reputation risk management strategy. Consult the PR team or external advisors on the best approach, taking into account potential legal considerations as well.

Impact mitigation

Another important task of the incident response team, which often needs to be carried out while also working on restoring the affected data, risk assessment and reporting of the incident, is to try to limit the impact of the breach. This can be done through a variety of means, both legal and technical. Often, organisations facing ransomware attack consider negotiations with the perpetrators and payment of the ransom as one form of impact mitigation, but that is debatable.

Responding to ransom demands

Usually, when an organisation discovers it was hacked with ransomware, the only file still accessible in the affected parts of the IT system is a small .txt file left by the culprits. This is the ransom note, explaining what the perpetrators have done and stating their demands or indicating channels of communication for negotiating those demands.

Example of a ransom note from the Conti ransomware group

Whether and how to deal with the ransom demand is one of the most important questions faced by an organisation that has had the misfortune of falling victim to a ransomware attack. Paying the ransom might seem the quickest solution for restoring operations and avoiding the liability (and embarrassment)

connected with a data breach. Indeed, according to studies from 2022, ***a little over 50% of organisations*** affected by ransomware attacks chose to pay the ransom.[6] But the decision is not easy.

Currently in most jurisdictions, Poland included, payment of the ransom is not illegal as such. It is therefore mostly a business decision, although some legal considerations still apply. For example, the decision to pay the ransom could have insurance implications. Not all cybersecurity insurance policies include coverage of costs related to the actual ransom. Some insurers could also regard the circumstances connected with the payment of ransom (e.g., if the insured disclosed the contents of its policy to the perpetrators, or simply had any direct contact with the criminals at all) as potential grounds for denying coverage. Before deciding on payment, you should therefore review your insurance policy. Payment to an entity that is on a sanctions list—even if inadvertent—could also lead to a breach of public sanctions law, particularly if there are some indications that the group responsible for the attack on the organisation may be connected with a sanctioned regime (e.g. Russia or Iran).

The main consideration when deciding on payment of the ransom is practical, however. Namely, management should consider if paying the ransom will yield any expected results. It goes without saying that when dealing with cyber criminals, the organisation has no real means of securing the outcome of the "transaction" and no real leverage over its counterpart in the negotiations. Available statistics are not encouraging with respect to the cyber criminals' reliability—according to some studies ***only 1 in 7 organisations*** that chose to pay the ransom reported having access restored to all their data post-breach.[7] The outcome after paying the ransom is never guaranteed. The culprits might fail to send the decryption key or send one that doesn't work; they might retain access to sensitive information and threaten to disclose it anyhow. Management should be aware of these risks.

Finally, there are wider ethical and moral considerations. Do you want to help perpetuate the ransomware model? Do you know who or what you will be funding if you choose to pay? These questions should also be kept in mind when making your decision.

Nevertheless, there are also valid reasons to considering entering into negotiations with the perpetrators. Negotiations could prove a way of obtaining further evidence of the scope of the data breach, which can be particularly

6 Enterprise Strategy Group report "The Long Road Ahead to Ransomware Preparedness" (March 2022).

7 Ibid.

important if the forensic experts are having difficulty establishing this independently. Cyber criminals often agree to provide the victim with a sample of the files they managed to copy. They may sometimes even agree to decrypt several files, as proof that they have access to a working decryption key. Negotiations can also serve as a way of buying time, to carry out other urgent tasks as part of the wider incident management process. That is why during negotiations the victim should neither explicitly confirm nor deny that the organisation will pay the ransom, and under no circumstances mention that it has insurance coverage, as this may embolden the attackers. Try thinking of convincing reasons to ask for time extensions, such as the need to report to superiors, issues with obtaining the necessary funding, etc. Ransomware groups usually rely on economies of scale, hitting many targets at the same time, so if the victim makes the work too hard and the prospects of a payout appear low, the attackers may move on in search of easier marks. However slim the chances of this happening, we are aware of instances where the attackers did give up without carrying out their threats.

Blocking the initial data transfer

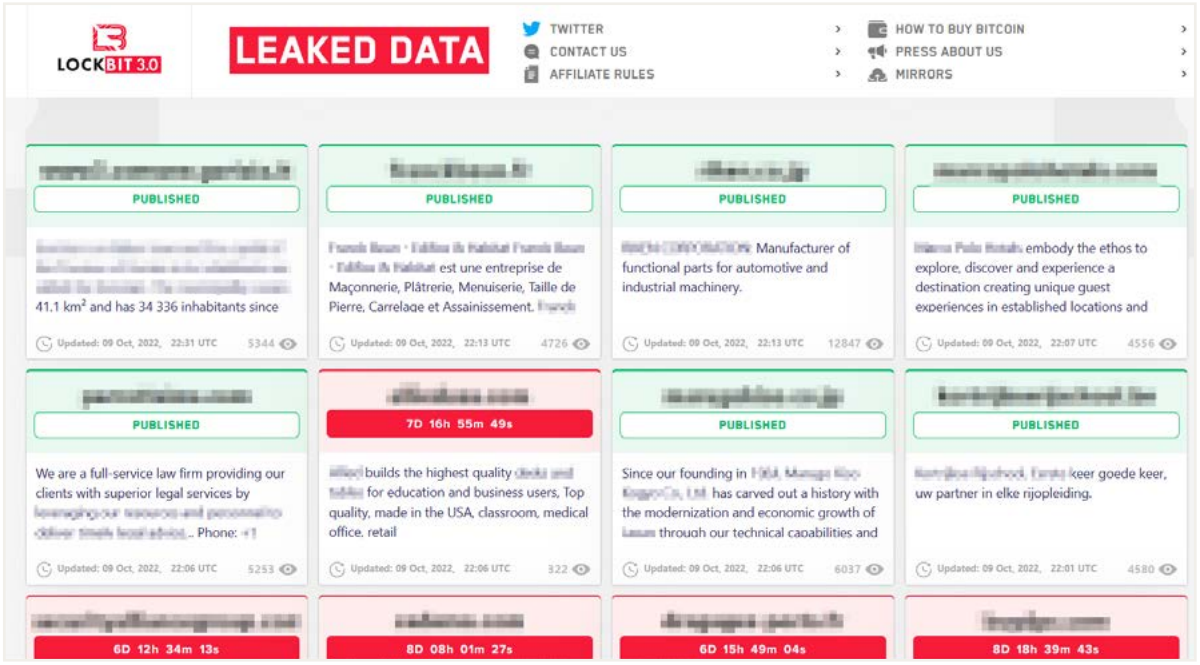
In most ransomware cases, after obtaining unauthorised access to the victim's system, the perpetrators will copy and collect any data deemed of value in a specific directory and then exfiltrate it by using a file transfer program (e.g. Cyberduck) to a location under their control. Often, they will use some form of legitimate cloud service to store the data at least temporarily, until it is transferred to a more secure location. If identified quickly as part of the forensic analysis, you could attempt to prevent the perpetrators from transferring the data further, by reporting the data as abusive and making a legal request to the cloud storage provider to take it down. Sometimes this can prove an easy solution to the risk of a data leak, though successful attempts are rare in practice. Often the hackers are too quick in transferring the data or exfiltrate it to multiple locations simultaneously to protect themselves against such actions.

Monitoring data leaks and preventing proliferation

Once it becomes clear that ransom will not be paid (or the perpetrators decide to do so for some other reason), the data may be posted on the internet, i.e. leaked. Usually, the initial data leak occurs on a "shaming site" belonging to a particular ransomware group, but sometimes the data can be published elsewhere, for example auctioned on a forum, such as https://exploit.in/ or

an anonymous file-sharing site like https://anonfile.net/. Shaming sites are usually located on the dark web (part of the internet not indexed by standard search engines and accessible only using a special ToR browser). Hackers often let the victim know in advance of the location of their "shaming site," since it helps to exert pressure, but not always. One way of mitigating the impact of a data breach is therefore to engage dark web monitoring services early in the incident management process, which can allow for rapid detection of leaked information and the location, but also offer insights into how the data is being used, aiding in further mitigation strategies.

Sample of LockBit group's "shaming site"



Once the data is published on the dark web it proliferates rapidly, spread through the internet by individuals who are often not even connected with the group responsible for the initial attack. This includes proliferation on mainstream websites, which are part of the "clear web" accessible to the general public. This phenomenon is referred to as "mushrooming." Once this occurs, containing the breach becomes much more challenging. Organisations should establish a dedicated team or hire external services to monitor popular forums, social media platforms, and other websites where the data might surface. Quick identification of such instances is crucial, because once

a secondary leak has been identified, a legal request can be made to the owner of the website or services to take down the stolen content.

In the case of hosting providers, a simple notice should be sufficient to remove illegal content, per the notice-and-takedown procedures envisaged in the EU's Digital Services Act[8] or the US Digital Millennium Copyright Act. In the EU, all hosting providers are required by the DSA to put in place mechanisms allowing any individual or entity to notify them of illegal content and to remove or disable access to it. They usually provide a special form (often under the heading "report abuse") to submit takedown requests and respond expeditiously to those that are sufficiently substantiated. But the situation is more difficult if the stolen data is only temporarily stored by a caching provider, such as a content delivery network (CDN). Under the DSA, caching providers generally follow an "order-and-takedown" approach, rather than "notice-and-takedown." This means that a caching provider is essentially legally bound to remove or disable illegal content only if it has been ordered to do so by a court or administrative authority. A mere notice or abuse report will in most cases be insufficient.

If the data breach involved personal data (which is usually the case), a "delisting request" to search engine providers under the "right to be forgotten" should also be considered. Google and other such service providers are legally required in the EU to delist specific URL addresses if they link to personal data of specific individuals which is "inadequate, irrelevant or no longer relevant, or excessive."[9] While delisting does not remove or delete the stolen content from the internet, it can make it less accessible to the general public.

8 Regulation (EU) 2022/2065 of 19 October 2022 on a Single Market For Digital Services (Digital Services Act).

9 *Google Spain SL v AEPD*, C-131/12 (Court of Justice judgment of 13 May 2014).

Criminal investigations

Reporting criminal activity

Data breaches are a form of criminal activity penalised by most modern legal systems. But there is no legal obligation to report this type of crime to law enforcement authorities, at least not in Poland. Excluding certain especially egregious types of crime, such as murder, war crimes or taking of hostages, the duty to report a crime is only ethical.

Nevertheless, reporting the incident and initiating a criminal investigation is worth considering as part of the wider incident management efforts. Taking part in a criminal investigation can provide the complainant access to valuable information and resources which otherwise might not be accessible. The organisation can learn details about the breach it was unable to uncover in its private forensic analysis (e.g. by having law enforcement seek relevant evidence in the possession of third parties), as well as evidence that could prove helpful in mitigating the effects of the breach (e.g. information about the location of stolen data or access to a decryption key). Reporting the incident to law enforcement can also enhance the organisation's credibility in the eyes of critical stakeholders, such as customers, employees, the supervisory board and shareholders, signalling to them that management are proactive and diligent. This may also be viewed favourably by regulators such as KNF.

But remember that once the data breach is reported, the course of the subsequent investigation will ultimately be controlled by law enforcement authorities. Victims can have a big influence on the specific actions taken by the authorities in their investigation (details below), but the decision whether to continue the investigation and for how long is largely in their hands. The investigation could also potentially divert resources the organisation needs for other efforts at managing the incident, for example to address follow-up questions and requests from the authorities.

The decision to report a data breach as a criminal offence requires careful consideration of these factors, balancing the benefits of law enforcement assistance against the potential drawbacks.

Overview of criminal investigations in Poland

Criminal investigations in Poland are conducted by the police and the prosecutor's office. The police are responsible for taking most of the regular investigative actions, such as questioning witnesses or collecting documentary evidence. The prosecutor supervises the police and is responsible for the more critical decisions and actions, such as presenting charges to the suspect, issuing arrest warrants, and deciding whether to open an investigation in the first place.

After a report of a possible crime is submitted, the prosecutor assigned to the case needs to issue a formal decision whether to open an investigation. The test applied to start an investigation is whether the prosecutor has due cause to suspect that a criminal offence could have been committed. The prosecutor will indicate in this decision the possible legal classification of the act, setting the scope for the future investigative activities. It is considered good practice for the complainant to provide the prosecutor with a written summary of the suspected crime in the crime report, together with all available evidence (e.g. the report from the forensic analysis), to assist the prosecutor in reaching the decision as quickly as possible.

Throughout the investigation, the prosecutor and the police can, among other measures, question any persons with potential knowledge relevant to the case and call on any individuals, institutions, and commercial entities to present specific documentary or electronic evidence and information. However, if the holder of relevant evidence is outside of Poland, the law enforcement authorities will need to make use of a mutual legal assistance treaty (or a European Investigation Order) and international cooperation procedures to obtain such evidence, which can be quite time-consuming. Some major digital service providers, such as Facebook and Apple, provide online access to a secure law enforcement requests (LER) portal,[10] to expedite the process in cross-border instances. But often it will be faster for the organisation to engage counsel in the relevant jurisdiction directly and secure evidence there under local regulations, for subsequent submission to the Polish law enforcement authorities conducting the main investigation.

Poland is a relatively good jurisdiction for pursuing criminal investigations in data incidents, because of the wide range of rights and access to information enjoyed by the victim. An individual or organisation considered a direct victim of the offence has the right to peruse the prosecutor's case file, containing all collected evidence, submit requests to collect other types of

10 See e.g. Facebook's online law enforcement request site.

evidence deemed relevant, as well as participate in any investigative activities conducted by the prosecutor, such as questioning witnesses or experts. Consider listing the specific investigative measures you think should be taken by the authorities in your initial report or subsequent submissions. While Polish law enforcement authorities are quite competent in investigating cybersecurity incidents, they are overwhelmed with cases and will appreciate any efforts at lightening their workload.

It is good practice not only to provide law enforcement authorities with specific and detailed suggestions of investigative measures at the outset of the investigation, but also to assist them on an ongoing basis, for example by reviewing collected evidence and providing conclusions and further recommendations resulting from analysis. If you decide to report the crime and initiate an investigation, you should be prepared to take a proactive and collaborative approach to ensure that it yields results.

Investigative leads in data breaches

There are three types of leads that can be followed by law enforcement authorities when investigating a data breach:

- Forensic evidence resulting from the initial attack
- Forensic evidence from the subsequent data exfiltration and leak
- Evidence from the "money trail."

Claims management

A data breach is essentially litigation in nascent form, with several contentious situations potentially arising from it. The incident response team, particularly the lawyers on the team, should be prepared to handle all possible claims (both outgoing and incoming) and regulatory investigations pertaining to the incident.

Below we describe some of the more common legal issues following a data breach which the IRT should address in the risk assessment and mitigation plan.

Liability for the source of the data breach—perpetrators

Depending on the circumstances of the breach, the organisation may consider pursuing legal action against individuals or entities who caused the attack or helped make it possible.

Claims for damages against the actual perpetrators are legally viable and can be pursued both as part of pending criminal proceedings and in separate civil litigation. Realistically, this scenario is feasible only if the investigation identifies the persons behind the attack, which unfortunately is rare in practice (most criminal investigations into cybersecurity offences are considered successful if law enforcement is able to charge at least the middle tier of intermediaries). And even if pursuing claims against the actual culprits is possible, in practice they may have insufficient assets to cover much of the damages, making the litigation futile.

Liability for the source of the data breach—third parties

Alternatively, you could consider the liability of third parties who may have somehow contributed to occurrence of the attack. There are several such scenarios, depending on the specific attack vector (see section on forensic analysis above), but the two most relevant options are:

- *The human factor*—the data breach happened because someone in the organisation fell for a phishing attempt or other form of social engineering
- *Technical vulnerability*—the data breach happened because the perpetrators exploited a vulnerability in software or an IT device used by the organisation.

In scenario (a), you could theoretically consider holding your own staff legally responsible for the incident. Some type of disciplinary measures may be justified in cases of gross negligence or non-compliance with internal security policies, but pursuing claims for losses suffered by the organisation would in most cases be excessive and unlikely to recoup much of the actual loss. In general, we consider positive reinforcement a far more successful approach to raising cyber-awareness among employees. In any case, whether employees can be held responsible for losses resulting from successful social engineering techniques is uncertain. Attempts to test it in court have been relatively rare. A good example of these issues is a Scottish case where the court dismissed claims against a former employee for damages the employer suffered as a result of cyber-fraud she enabled through lack of care.[11] The court held there was an insufficient causal link between the employee's lack of care and the loss: "The loss was exceptional and unnatural because she was ignorant of the fraud being perpetrated on her and on the pursuers."

In scenario (b), the organisation might consider pursuing claims against the provider of the vulnerable software or device. Indeed, software vulnerabilities are one of the more common attack vectors, alongside phishing/social engineering (and according to some statistics account for over half of all analysed ransomware attacks). For example, there have been cases of ransomware attacks made possible because the VPN software used by the victim was vulnerable to a technique called "SQL injection," allowing the hackers to obtain security credentials and unauthorised access to the victim's IT infrastructure without its knowledge. So far, cases involving liability of providers of various IT products for security vulnerabilities are few and far between. One of the main obstacles holding down the number of such cases is the standard liability limitation clauses included by most software providers in their end user agreements, which usually exclude any form of liability for their products, including for damages related to any corruption or loss of data. But there are new European regulations in the pipeline which may greatly alter the legal landscape in this respect. In particular, the proposed Cyber Resilience Act[12] and the revised Product Liability Directive[13] may make it much easier for victims of cybersecurity incidents to pursue claims against software providers, by introducing a set of clear obligations concerning cybersecurity of digital products and strict product liability for losses resulting from vulnerabilities, which the parties cannot exclude by contract.

11 *Peebles Media Group Ltd v Reilly*, [2019] CSOH 89.

12 Proposal for a Regulation of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements, COM/2022/454 final.

13 Proposal for a Directive of the European Parliament and of the Council on liability for defective products, COM/2022/495 final.

Liability of the organisation for consequences of the data breach

Unfortunately, an organisation that has had the misfortune of falling victim to a ransomware attack can in some instances itself be held liable for the consequences.

In particular, a risk of litigation against the organisation arises when a data breach involves personal data. Under Art. 82 GDPR, any person who has suffered material or non-material damage because of an infringement of the GDPR has the right to receive compensation from the controller or processor of the data. A controller or processor is exempt from liability if they prove that they were not in any way responsible for the event giving rise to the damage. Keep in mind though that this provision looks at a data breach from the perspective of non-compliance with data protection regulations. Liability under Art. 82 stems from an infringement of the rules in the GDPR, rather than from the data breach itself (e.g. a controller or processor of data could be held liable if the data breach was possible or caused damage to data subjects because of failure to implement technical and organisational measures ensuring an appropriate level of security, or to notify the data subjects of the breach in a timely manner).

Other possible grounds for liability of the victim organisation may stem from contractual instruments. If the leak included business secrets of customers or suppliers, they could decide to pursue claims for breach of any confidentiality clause covering the data. This is why it is essential in the risk assessment and inventory (see above) to consider which business partners may have been affected by the breach, so you know which contracts should be reviewed in detail to assess possible exposure to such claims. An obligation to ensure a certain level of data security or to report incidents could be included in the data processing agreement (DPA) that often accompanies other types of contracts related to data transfers. It is also becoming more common in practice for larger companies to require their vendors to sign cybersecurity-specific agreements with similar provisions, or even more stringent ones, for example requiring vendors to implement a document information security management system compliant with ISO 27001, or provide employees regular training in cybersecurity and awareness. Indeed, some entities may be required by law to conclude such agreements with their vendors (for example, essential and important entities covered by the NIS2 Directive). If you have customers subject to such statutory requirements, be particularly diligent when assessing the risk of potential liability.

Regulatory investigations and sanctions for non-compliance

Finally, a data breach event will naturally draw the attention of regulators tasked with ensuring data security. Investigations or audits may become particularly likely if a secondary victim (e.g. clients or employees whose data was leaked) decides to report the incident themselves or allege that the organisation failed to comply with relevant regulations.

In most cases, the most pertinent regulatory body to launch investigations or an audit following a data breach is the national data protection authority (in Poland, PUODO). If the investigation finds non-compliance with the GDPR, the organisation could face potential fines as high as EUR 20 million or 4% of its annual global turnover. In practice, the penalties imposed for infringements related to data breaches are usually lower, at least in Poland (the highest penalty for a data leak imposed so far by PUODO, for failure to perform a personal data risk assessment and encrypt sensitive data, was PLN 3.8 million, or less than EUR 1 million). Nevertheless, the sanctions for non-compliance are quite severe, and any audit or investigation should be handled with due care. Bear in mind the potential for future investigations when notifying the data authority of the incident. Any misrepresentation of facts in the notification could be easily discovered and lead to severe consequences.

Other regulators may also become involved, depending on the legal status of the organisation. For example, with a financial entity subject to DORA requirements, its conduct before and after a data breach could also be scrutinised by the financial authority. The same could occur in the case of an essential or important entity covered by the NIS2 Directive. Some regulations, in particular NIS2, provide for sanctions that can be imposed not only on the organisation, but also personally on top management if they are responsible for any irregularities.

Contact

Jakub Barański
adwokat, partner
jakub.baranski@wardynski.com.pl

Łukasz Lasek
adwokat, partner
lukasz.lasek@wardynski.com.pl

Wardyński & Partners
Al. Ujazdowskie 10, 00-478 Warsaw
Tel.: +48 22 437 82 00, +48 22 537 82 00
Faks: +48 22 437 82 01, +48 22 537 82 01
E-mail warsaw@wardynski.com.pl