# Security Incident Handling – Legal Considerations

Authors: Theodor Adam, Florin Andrei, Larisa Gabudeanu, Victor Rotaru

Copy Editor: Alexandru Mircea Rotaru

This article explores the various legal aspects that have to be taken into account when a security incident occurs, focusing on the evidence gathering and supply chain management perspectives. Other related aspects of concern covered here include information disclosure to the public, information disclosure to the data subjects, notification and cooperation with relevant authorities (including CERT-RO), and the attribution angles.

## 1. Supply chain management

In terms of incident notification, the contract and the operational steps between the organization and its IT solutions providers (referred to as provider in this article) must occur as soon as possible. At the end of these steps, organizations will have established a maximum timeline by which an incident notification must reach them. .

Of course, replicating this type of obligation and operational aspect throughout the supply chain will ensure that the organization is aware of security incidents throughout the supply chain.

The organization can then use this information to take the necessary steps internally to mitigate incident consequences and to prevent similar incidents from happening in the future. Furthermore, the organization can also use the information to fulfil all their obligations towards the relevant authorities and affected individuals/entities, per existing legal requirements, as well as to reduce the negative effects of the security incidents on the affected parties.

### 1.1 Incident notification

In order to provide the organization with enough time to analyze the incident and decide upon all the legal and operational steps to take, the Provider needs to notify the organization of any incidents as early as possible; generally, the contract includes a maximum period, which tends to be around 24-72 hours. Another option is to have the Provider notify the organization immediately upon learning of the incident. Nevertheless, a clear timeline is critical in such situations because every second gained in addressing a threat reduces its overall fallout, resulting in a lower level of damages the organization has to incur in its aftermath.

In terms defining what an ‘incident’ is, in this notification context, it can be viewed as a ‘potential incident’, respectively, a risk that an incident may have occurred, without clear

confirmation of this occurrence yet. Thus, the best approach to ensure proper compliance with legislation and swift identification of incidents (or, as mentioned under the GDPR, data breaches), is to have the Provider notify the company when they suspect an incident has happened, even if its occurrence has not been confirmed clearly.

Organizations can negotiate with their providers to have an obligation to promptly notify the organization about any identified vulnerabilities in the IT systems, as well as the Indicator of Compromise (IOC).

### 1.2 Assistance throughout the incident handling process

Including certain provisions concerning assistance from the provider (and its sub-contractors) will ensure that any incidents get investigated swiftly and that remedial steps get implemented quickly. This type of clause is generally heavily negotiated.

On the one hand, it is important for the organization to have its providers on standby in case of incidents (especially if caused by any of the providers themselves), in order to investigate the incident, to ensuring timely reporting toward authorities, and to swiftly remedy the root cause of the incident.

On the other hand, the provider has to have predictability when allocating resources and costs associated with a given contract. Having experts on stand-by 24/7 can be an unfeasible operational and commercial strain for certain providers. For this reason, providers often suggest limitations on their involvement and the time allotted for such tasks, and charging additional fees for such services.

At the same time, the organization may have certain data or metadata it retrieve. For example, in cloud services, certain types of logs are only kept by the cloud service provider. For this reason, it is essential to have specific contractual requirements for the provider to disclose data disclosure to the organization when incidents that require such information to be analyzed for mitigation purposes occur.

### 1.3 Interaction with authorities

Certain types of incidents, such as incidents occurring in certain sectors need to be notified to relevant authorities (e.g. data protection authority, banking regulatory authority). In this case, per the relevant legislation, authorities usually accept initial details on an incident with subsequent submissions completing the picture with more details and evidence, as they get discovered. Subsequent reports can include, for instance, details about the root cause, or mitigation measures to stop the consequences of the attack or future similar attacks.

Additionally, the respective authority may request more information on certain points relating to the incident, may perform an on-site audit of the situation, and/or may request that

the organization implements certain controls to address the incident. These aspects should be reflected in the contractual clauses with all providers, in order for said providers to assist on these points as well.

### 1.4 Implementing controls

Every organization must clearly define the scope of their mitigation controls, which aim to prevent future incidents from occurring. Certain mitigation controls may be required by law (or mentioned as guidelines by relevant authorities), which is why no organization should go without them. However, a provider may request additional fees for such actions, depending on their complexity and their utility for its other clients, so having too many controls of this type can become financially unsustainable. Hence, beyond the legal requirements, every organization should tailor its mitigation controls to the reasonably likely and highly damaging risks specific to their operations.

Some argue that the provider should implement such controls, as they are closely related to the software they provide to clients regulated by such specific legislation. Of course, this is closely related to tailoring the IT system to the client's needs. For instance, when the IT system is aimed at a specific sector, such as banking, this may be argued easily. For IT systems created per the client's instructions or off-the-shelf IT systems, it may more difficult to argue. For data protection aspects concerning privacy by design, it may be argued that the IT system should, from the outset, respect all privacy by design requirements without the need for specific requests from the provider's clients in this respect.

For this reason, the main aspects negotiated here (depending on legal requirements and needs of the organization) are the costs for assistance, the extent of the assistance, and the timing for response/implementation.

### 1.5 Confidentiality of data

Another point to consider is that concerning the confidentiality of the data obtained during the incident analysis, attribution, vulnerability identification, and mitigation. This confidentiality and any disclosure of such information has to be on a need-to-know basis (only to the individuals that need to have access to this in order to perform a specific task). Further, the information should be deleted once it served the purpose for which it was disclosed.

## 2. Forensic analysis and preservation of evidence

Forensics is an important part of incident handling. On the one hand, it can assist with identifying the root causes and the steps taken by attackers, which turns it into a valuable lessons learnt tool. On the other hand, it can be used as evidence before the courts of law in case of litigation concerning the incident.

When creating forensic copies of data, one should have in mind the following principles: the forensic copy should be admissible (comply with any legal requirements in terms of evidence gathering and preservation), authentic (ensured through the best practices used during the forensic collection phase and through the chain of custody implemented properly), complete (the entire context needed to analyze the incident and need for reaching a conclusion concerning the incident), and reliable (based on the forensic collection and preservation process used, which implements best practices in this respect). For this latter point, one should remember that, when performing forensic collection, the steps taken, when reconstructed, should lead to the same outcome.

For performing this type of activity, there are various tools that can be used in order to comply with best practices. We are mentioning below of couple of them that can be further explored depending on the needs of the organization:

- SANS - SIFT Workstation - https://www.sans.org/tools/sift-workstation/
- Autopsy - http://www.sleuthkit.org/
- FTK Toolkit - https://accessdata.com/product-download
- Caine - https://www.caine-live.net/page5/page5.html

### 2.1 Preparing for incidents

Having a forensic expert on stand-by is crucial in preparing for incidents, as they are able to preserve evidence that can be used in the future, before authorities or before a court of law. There are two options in this case: an in-house forensic expert or an external one. From a practical perspective, unless the organization requires frequent preservation of evidence, it may be useful to have a framework agreement for an external forensic expert.

For this situation, a confidentiality agreement and a data processing agreement should be in place with the external forensic expert, as they will have access to confidential information (which would most likely include personal data).

## 2.2 Handling of forensic and investigation work in parallel

From an operational perspective, once the incident investigation commences, the incident handling team should be able to investigate the incident without impacting on the evidence gathering process and without destroying potential evidence.

The best approach begins with the evidence gathering process, once the incident occurrence is confirmed or probable. This should abide by the best practices in the field, including in terms of various IT assets/devices to be copied and the types of data to be collected (including volatile data, such as data within the virtual machine).

## 2.3 Applying best practices in forensic collection

In order to ensure proper evidence gathering that can be used before the courts of law later on, one should use scientifically derived and proven methods for preserving, collecting, validating, analyzing, interpreting, documenting and presenting digital evidence. This allows events to potentially be accurately reconstructed in the future.[1]

Prioritizing data gathering must rely on best practices, such as starting with the most volatile evidence/data and working towards the more persistent evidence/data.

Generally, one should not shutdown or reboot the IT system before collecting evidence/data, as the evidence/data may be lost or altered. The same recommendation applies when copying or preserving a program on the IT systems- otherwise, the data/evidence can get altered.

In case of complex IT ecosystems and/or complex incidents, it is essential to work fast, which can mean, for instance, prioritize data collection based on most relevant IT systems and parallel copying sessions for multiple servers, devices, etc.

Nevertheless, the data collected should be proportional to the purpose for which it is collected. Thus, no more than the data needed for the incident investigation, reporting to authorities and for potential legal disputes on the matter should be collected.

Further, any forensic collection should be made in close correlation with the Security Operations Center (SOC) team actions (either internal or external) and investigation phases for the incident. In addition, if specific actions have to be taken, per legal requirements, quicker than the forensic data collection can be finalized, alternative solutions should be analyzed in order to ensure both actions get completed successfully. Given the number of parties involved

[1] Gary Palmer, A Road Map for Digital Forensic Research, DFRWS 16, 2001, http://www.dfrws.org/2001/dfrws-rm-final.pdf , last accessed on 8 June 2021.

in the process when such correlations occur, there must be periodical drills that ensure everyone involved knows what to do in case of an incident.

Additionally, during the forensic copying of the data, data handling and corruption of original data should be minimized. This can be ensured by using best practices and a methodology for forensic data collection.

In terms of legal compliance, the forensic collection scope and limits should be clear for the organization and for the forensic professional. It is important to collect only the data needed, but sufficient data for further analysis, especially in terms of context and the IT system's state. As a court of law may request details on the collection process, a specific clause should be included in the forensic services agreement concerning the forensic professional testifying before a court of law, if needed.

### 2.4 Preserving data

After data collection, data preservation is also important. The organization can keep the forensic copy internally, with proper security and chain of custody rules in place which ensure that no tempering occurs. Alternatively, it can be kept with a third party at their location, with the same principles in place.

In general, it is preferred to have the original intact and not tempered with, with Forensics making available copies of the IT system (e.g. bit-by-bit, a snapshot at a given time). If this is not possible, the forensic copy should be prepared based on the forensic best practices and kept securely as per a well-documented chain of custody processes. Further, any subsequent analysis should not be performed directly on the forensic copy, but on secondary copies thereof. These secondary copies, of course, should be created based on forensic best practices, as the initial forensic copy was created.

Further, it is recommended, if possible, to maintain also the original (e.g. in case of laptops) or an auditable copy (i.e. forensic copy as per best practices) in order for a court appointed expert to be able to re-perform the incident analysis.

For this forensic copy, as per data protection requirements, a retention period should be established, with the data being deleted afterwards.

### 2.5 Data sharing

In terms of sharing the forensic copy or data from the investigation, this can be shared with specific provider for certain aspects. With the provider that provided the services/IT system under investigation, it may be useful to share certain data or, even, a forensic copy of the relevant data in order for this provider to analyze the data and identify the root cause of the incident, for instance. Another situation of data sharing might be towards a security incident

investigation company, in order for this company to provide information about the incident after investigation. For any such scenario, the organization has to apply the data protection requirements, starting with proper data processing agreements in place, minimization of data being disclosed, and deletion of data once it is not needed by the provider.

## 3. Role of relevant departments within the organization

The organization should have in place procedures that outline the role of each department in case of a security incident. For instance, the operational departments can be guided by another department – e.g. the security investigation department. It is essential to identify and involve all relevant departments from the outset – e.g. legal, data protection, risk. The internal procedure should also ensure that the key employees needed for the incident investigation and remediation steps are on stand-by or easily reachable.

Further, management should be informed once sufficient information to qualify an event as potential incident and should be kept informed about subsequent information gathered, incident reports prepared.

All notifications towards third parties should also be sent as soon as sufficient information has been gathered. This might be the case for individuals affected by the incident, companies using the services offered by the organization and subject to the incident, etc.

In addition, once an initial report about the incident consequences and root cause are prepared, this should be shared with key departments for they input on mitigation measures, containment measures, notification of authorities, etc., depending on the specifics of the department and of the organization. Mitigation steps are to be decided as per the usual internal rules of the organization – e.g. security team, management team.

At this stage, depending on the type of incident, the organization can consider if witness statements can be useful for future litigation. If yes, these should be obtained as quickly as possible from the relevant individuals.

After the incident has been mitigated to prevent similar incident from occurring in the future, it may be useful to re-check the affected IT systems, with external auditing or penetration testing, in order to ensure that the mitigating controls have been implemented properly and that no additional vulnerabilities were generated by the incident.