Information Security in Legal Firms

Robert Pająk

1. Introduction

Law firms and lawyers have been an interesting target for cybercriminals for many years. This is particularly because they possess a considerable amount of valuable information (e.g., know-how, contract details etc.). This does not only refer to their own data (including that of their employees), but above all that of their customers[1]. However, the possession of interesting data is not the only reason. In particular, law firms are also increasingly becoming the indirect target of attacks as (legal) service providers. In this way, by leveraging the trust in such entities, cybercriminals can more easily get into the targeted company/person or gain knowledge to act against them.

The consequences of this type of action are obviously devastating. Starting from loss of reputation, through liability related to violation of the law (personal data, sensitive data, various types of information protected by secrecy rules), up to the lawyer's disciplinary liability. It should also be mentioned that law firms work under a special ethical and legal regime (attorney-client privilege), which further increases the seriousness of the problem of security attacks and information security breaches.

The aim of this chapter is to provide an introduction to information security and protection and to show where to begin in order to build protective mechanisms and how to start implementing recommendations from the list of so-called best practices. This will enable conscious and consistent management of the protection of information processed in a law firm, including its employees and associates. Additionally, this chapter aims to familiarize reader with the vocabulary used in the information security and protection industry, which will consequently allow to understand where and how to deepen your knowledge on this topic.

---

1 Donie O'Sullivan C, 'Hacked Celebrity Law Firm Says It Has Not Worked With Trump' (CNN, 17 May 2020) <https://edition.cnn.com/2020/05/17/politics/celebrity-law-firm-hacked-trump/index.html> accessed 17 August 2021.

Information security and data protection is a highly interdisciplinary knowledge domain - covering whole range of topics - from physical protection, through highly specialized technical matters, to policies, procedures, regulations, guidelines, and plans. A comprehensive coverage of such a broad topic would require a separate publication, so in this chapter we only provide an introduction to the problem. However, taking the challenge holistically - thanks to the systematic approach aimed at reducing some of the more complex topics, adding references to detailed guidelines and the introduction of aspects related to the concept and language of risk - it is possible to bring the subject closer to the reader and achieve the goal of increasing security in law firms and introducing best practices into the daily routine of this important professional group. This will also naturally increase the chances of warding off threats or minimizing their effects. Finally, it can also provide an opportunity to prevent the phenomenon of resignation or to analyse the issue of delays and to try to understand the common, yet incorrect, opinion that security must be very expensive and only large companies can afford it.

2. *The Concept of Information Security, Data Protection and Cyber security*

One of the most important steps in dealing with a new subject is to determine the meanings of the basic (key) terms and concepts that underlie it. In the case of information security and protection, however, it is difficult to find one coherent and exhaustive definition, especially one that would comprehensively convey the depth of the topic. A scholarly discourse would allow us to derive an understanding of the concept from matters of basic human needs ("overlaid" on modern information society) and would lead us to issues of etymology of the word itself. In this chapter, however, the focus is on the conceptualization and practical application. The challenge of finding the one unified definition is further complicated by semantic problems. It should be noted that a significant part of the terms in information security and data protection originate in English-speaking countries, where a distinction is made between the terms "security" and "safety[2], and they do not always find a proper translation in

2 Ludovic Piètre-Cambacédès and Claude Chaudet , 'The SEMA Referential Framework: Avoiding Ambiguities In The Terms “Security” And “Safety”' (2010) 3 International Journal of Critical Infrastructure Protection.

other languages[3]. Trying to look for a definitional consensus that would take into account the proper adaptation to our needs in the pragmatic field, we will quickly come to define the measure of security by distinguishing a number of criteria. Since the 1970s and the first studies of data protection, coming from the military domain and industry best practices and standards, the so-called "CIA triad" has been considered the primary criteria for information security. This acronym comes from the first letters of three main parameters: confidentiality, integrity, and availability. Confidentiality is the most intuitive attribute of information - it assures us that only authorized people can see the information. Integrity, on the other hand, indicates an important feature of information that is the need to ensure data consistency in the sense of absence of unauthorized changes. Availability of information - similarly intuitive - tells us that a person can access the information whenever he or she needs it.

This minimum set of three criteria, described in detail in ISO 27001, has been expanded to include a number of other properties that define the crucial parameters of information security, especially in a communication context. While the above-mentioned three basic criteria suffice to define the problematic, it is worth looking at one additional attribute - accountability, an attribute of information that specifies that we can unambiguously attribute given actions to a specific user.

When thinking on how to protect a particular piece of information, we can consider the goals of securing it in the context of these criteria. It is worth remembering to look at the subject of information protection also beyond information systems - hence the reference in this chapter to more general concepts, i.e., information security and protection - rather than using the increasingly common concept of cybersecurity. In addition to linguistic purism, this is particularly important given the fact that there is still a significant amount of information that is not necessarily in digital form or exists in dual form. Similarly, the security of information in digital form may also require measures outside of information systems.

As an example, let's take a situation in which a law firm is attacked and, in addition to data on digital media, information is stolen, e.g., in the form of printouts - and the break-in itself occurs trivially by breaking a window and unauthorized access to the building. In this case, one can

3 Spyridon Samonas and David Coss, 'The CIA Strikes Back: Redefining, Confidentiality, Integrity And Availability In Security' (2014) 10,3 Journal of Information System Security <http://www.proso.com/dl/Samonas.pdf> accessed 17 August 2021.

clearly see the need to go beyond issues related to the digital sphere in order to comprehensively protect information stored and processed in law firms.

3. Information Security Planning to Secure Law Firm

3.1 General Comments. Sources of Information Security Best Practices.

Both the field of information security and protection, as well as adversarial hacking techniques are constantly evolving. Every day new methods of breaking control mechanisms appear, and media headlines describe subsequent incidents involving companies whose databases were hacked using these techniques. In this context, taking into account that focusing solely on the information security process is not the main goal of the business, which is after all focused on conducting and developing business in the legal area, the question of where to draw current sources of knowledge becomes justified. An equally important and serious problem is the phenomenon of outdated best practices in this area. The answer to these questions will be presented below, together with reference on particularly important and universally best practices.

As indicated above, one of the fundamental problems in information security and protection is the complexity of the subject matter. It makes sense, therefore, to refer to proven guidelines to make sure that none of the topics necessary for laying the foundations for security is overlooked. At present, however, there is a vast number of standards, norms, regulations, and guidelines available - dozens of different frameworks for security are readily identifiable. On top of that, some of them are less popular and recognizable only in selected geographic areas, and not necessarily tailored to smaller and medium-sized entities. Minding that (as an assumption) the subject of this discussion are typically relatively small organizational units (from individual practices to subject matter experts (SMEs)), and trying to reasonably minimize the complexity of the addressed topics (as reasonably structured a catalogue of guidelines as possible), we have to reduce such a large number of recommendations and indicate that the following standards, good practices and framework guidelines are worthy of particular attention: ISO 27001, NIST Cybersecurity Framework, CIS Controls/CIS Benchmarks and industry guidelines sensum largissimo.

3.2. ISO 27001

ISO 27001 is a norm created by the International Standard Organization. Its purpose is to standardize an information security management system. The standard is recognized globally (with particular popularity in the geographical area of Europe) and is the basis for many other guidelines and regulations that take it as their baseline/fundamentals. ISO 27001 allows to obtain certification of compliance with its guidelines - you can formally confirm that you are complying with the recommendations set out in the standard. Such certification can be done periodically by an independent auditor. Within the framework of the standards described in the 27000 series, it is also worthwhile to get acquainted with the guidelines described in ISO 27002; this standard is under continuous development.

3.3. NIST Cybersecurity Framework (CSF)

These are guidelines created by the US National Institute of Standards and Technology (NIST). They were constructed for the private sector to assess the risks it faces when processing data in cyberspace. The guidelines remain internationally recognized, with a particular popularity in the US. The NIST CSF is widely regarded as a "lighter" version of NIST 800-53, and these guidelines provide the basis for requirements to be met for companies working with U.S. government entities. The framework is being actively developed and incorporates the needs of self-diagnosis. An additional plus is that they address vendor (supplier) management as a critical component of ensuring information security and protection. These issues are becoming increasingly important due to the increased use of trust relationships with companies that perform subtasks for other entities.

3.4. CIS Controls/CIS Benchmarks

The Center for Internet Security (CIS) is a non-profit organization that promotes open standards and guidelines related to information security. From the perspective of building security in a law firm, the most useful framework standards developed by CIS include CIS Controls - 20 guidelines that allow taking into account the most typical areas requiring security attention, and CIS Benchmark - a set of recommended settings and configurations for various systems and products. These tools will allow you

to verify the correctness of your assumptions and pay attention to most of the necessary elements important from the perspective of information protection.

3.5. Industry Guidelines

3.5.1. International Bar Association

The legal community, in response to the increasing number of threats, has reacted by creating catalogues of best practices. One of the very popular one is that created by the International Bar Association (IBA), an organization of hundreds of thousands of legal practitioners and organizations in the field worldwide. In 2018. IBA, pointing out that law firms are a significant target for attack, particularly due to not making cybersecurity a priority, created a task force to build a catalogue of best practices to help law firms protect themselves from information security and protection breaches. The result was the Cybersecurity Guidelines[4] report, which addresses both technological and organizational challenges. Certainly, noteworthy is the attempt to divide and prioritize requirements according to the size of the law firm and the inclusion of individual legal practices.

3.5.2. Council of Bars and Law Societies of Europe

The Council of Bars and Law Societies of Europe[5] (CCBE), as the association representing affiliated lawyers from 45 countries in the wider Europe, issued its recommendations in 2016 related to protection against unlawful surveillance. These guidelines were created both to protect against threats from cybercriminals and directed at protection in relation to threats from poorly regulated processes at the national level. Despite the specific focus, the recommendations refer both to the basics of information security and protection, including the aforementioned ISO 27001. Noteworthy is the

4 International Bar Association, 'LPRU Cybersecurity' (*Ibanet.org*, 2018) <https://www.ibanet.org/LPRU/Cybersecurity> accessed 17 August 2021

5 CCBE, 'CCBE GUIDANCE On Improving The IT Security Of Lawyers Against Unlawful Surveillance' (*ccbe.eu*, 2016) <https://www.ccbe.eu/fileadmin/speciality_distribution/public/documents/IT_LAW/ITL_Guides_recommendations/EN_ITL_20160520_CCBE_Guidance_on_Improving_the_IT_Security_of_Lawyers_Against_Unlawful_Surveillance.pdf> accessed 17 August 2021

recognition and strong justification of the criterion of confidentiality as paramount to the profession of legal practice, also indicating as an imperative the acquisition of skills in information protection and security.

4. Other Law Firm Information Security and Protection Challenges

4.1. Roles and Responsibilities

One of the most frequently observed mistakes connected with information security and protection is appointing one (the only) person, often performing at the same time completely different primary duties, responsible for this area. Undoubtedly, it is worth indicating who bears responsibility for a given subject - nevertheless, ensuring security should be a duty of every employee and it is both a basic and a necessary condition. Responsibility for information protection and security should be introduced into employee and other contracts, including contracts with suppliers whose services the law firm uses. However, it is worth noting that the responsibilities should also be accompanied by appropriate knowledge gained during training and education. These trainings should be conducted periodically (a significant facilitation may be the use of regularly updated platforms where employees can improve their skills in avoiding and repelling attacks). Investment in security knowledge becomes particularly important if we consider that social engineering attacks are still among the most popular methods of breaking into companies.

When mentioning roles and responsibilities, it is important to ensure that each employee (similarly, trainee, etc.) has access only to the information necessary for his or her job. The need-to-know principle, sometimes also called the principle of necessary/justified knowledge, allows to minimize the effects of security breaches. Additionally, all tools used should be configured in a way that enables clear identification of the person responsible for each action (see: accountability).

4.2. „Digital Hygiene"

In the age of the information society and increasing digitization, to avoid cybercrime problems, every law firm partner, employee, and associate should train a set of habits to safely navigate and survive in the digital world. It is not uncommon for cybercriminals to forgo breaking through

more complex security measures, focusing instead on areas that are not challenging and where there is less risk of identification or failure. These habits are forming into a kind of catalogue of behaviours that we can refer to as digital hygiene. In particular, we should pay attention to behaviours such as:

1) Regularly updating the operating system and software, both on computers and mobile devices, as well as any other electronic/IoT devices (smart TVs, "smart speakers", lighting controls, "smart light bulbs", sensors, weather stations, electronic locks, etc. - such devices can also provide an "entry" point for cybercriminals.
2) Encrypt data on all media and devices wherever possible, using proven algorithms and strong passwords (preferably keys).
3) Use two-factor/multi-factor authentication wherever possible:
   a) U2F tokens should be used where possible - these will also help in the context of preventing phishing - actions aimed at compromising security by impersonation methods,
   b) where possible, use authentication applications such as Microsoft Authenticator (instead of SMS codes).
4) Use of different passwords for each service/web page.
5) Use of "password managers" - special programs that allow storing and generating unique passwords for each website used and can additionally ensure that the password is entered only on the correct page. Some of them also inform about improper practices related to the use of passwords and their compromise/leakage.
6) Preventing the use of personal electronic devices by other people/third parties.
7) Preventing other people/third parties from attaching USB-type media - in particular, care should be taken to prevent of allowing plugging charging cables (something what looks like an ordinary USB cable may in fact be a specialized device designed to break security and gain unauthorized access to information stored on the device).
8) Refusing to request to make 'courtesy calls' to other people using personal telephone or other communication devices.
9) Consideration of setting up a separate wireless network for the needs of the chancellery and a separate one for the needs of clients and visitors; prohibition of the use of free public wireless networks.
10) When using Wi-Fi (wireless fidelity) technology, the need to ensure that the network belongs to the true and honest service provided, particularly if a message is displayed requesting the user to enter a password.

11) Use of VPN (Virtual Private Network) solutions - especially when travelling.
12) To refrain from passing on important information and data, even to those closest to you, e.g., by telephone while travelling.
13) Use of privacy filters (also for mobile devices), especially in trains, planes and other means of transport that allow work.
14) Providing solutions for secure data disposal, both in traditional form (shredders with appropriate certificates) and digital (tools for secure data disposal, encryption).
15) The need to configure security mechanisms when working in a cloud environment (the responsibility for configuring security mechanisms is usually shared/transferred to the end user - the so-called shared responsibility security model).
16) Making back-up copies and regularly verifying data on it.
17) Encryption of backup copies using appropriate algorithms.
18) Use of reputable services such as “Have I Been Pwned” to monitor if those accounts and password from various services have not been compromised by attacks.
19) To regularly complete and update knowledge of information security (e.g., by reviewing industry portals).
20) Use only devices (mobile phones/tablets/mobile devices) that have current manufacturer support for security patch updates.
21) Using a separate profile on your phone (or other phone/mobile device) for your private matters.
22) Limiting trust towards people/third parties initiating contact (e.g., via telephone, Internet).
23) Verification of requests for electronic favours (e.g., return contact to a 'friend').
24) Limiting the natural desire to help other people (e.g., not allowing people you don’t know enter into the building; the person may, for example, be faking an important phone call, have their hands "full", etc., in order to exploit the natural desire to help and get into the building without following security procedures/access badge).
25) Never open links with an offer that you have not previously ordered.
26) Turn off bluetooth (this recommendation may be difficult in an era of widespread device integration, e.g., car kits, smart watches, but it is worth remembering in special situations).
27) Using different browser to connect to the bank, law firm or websites where you have access to confidential data.
28) Prohibition on communicating login data, passwords and disallowing account sharing with anyone.

29) Verifying account numbers on invoices (they may be false) and requests to change contractor numbers etc.
30) Prohibiting leaving devices, media, documents, and other items containing data in a car or other risky location.

4.3. Insider Threats

Insider threats is also an important, but not easy and usually a rather sensitive topic. We are talking here about both current and former employees, trainees, persons, and companies cooperating with and having regular access to the office/data, etc. In the context of threats, we are talking about both intentional and unintentional actions caused by insiders. According to research[6], more than half of organisations are confronted with this type of phenomena, and most are in no way prepared for it. The difficulty in dealing with this type of problem stems from several reasons - both the delicate nature of (inter)employee relations and legal constraints (verification of an employee's background, scope of control possibilities, etc.). The ease of access from the inside also encourages cybercriminals to use this method - after all, there's nothing easier than turning up for an internship or job interview and gaining virtually unlimited access to the inside of an organisation, if only for a moment.

In order to efficiently deal with insider threats, it is worth preparing a detailed security plan, taking into account such mechanisms as: limiting privileges in the access to information to a necessary minimum (taking into account the above-described principle of indispensable knowledge), full accountability of actions while processing information, auditing and monitoring systems taking into account the detection of unusual events. Additionally, awareness-raising activities and open communication in the above-mentioned scope should be conducted. Particularly sensitive data should also be marked, and attention should be paid to their flow within the company (and external systems, e.g., cloud systems used by it). These topics are important not only because of cybercrime, but also because of the potential for conflicts of interest.s

6 Crowd Research Partners and Cybersecurity Insiders, 'Insider Threat Report 2018' (Crowd Research Partners, 2018) <https://www.veriato.com/resources/whitepapers/insider-threat-report-2018> accessed 17 August 2021

4.4. Multi-layer Security

In the process of building security, it is also worth mentioning a principle which definitely works well in the practice of a lawyer, especially when we regularly see security mechanisms being broken and newer and newer attack techniques. We are talking about building multi-layered security mechanisms - even if we already have one layer of protection for a given system/information, it is also worth building and including all other available mechanisms. Such an approach allows you to protect yourself from an attack when a single protection mechanism is breached. It also gives a chance to avoid unauthorised access to the information through an additional control mechanism that may not have a publicly available "weaknesses" at the time.

4.5. Outsourcing

Considering the complexity of the subject of information protection and the rapid development of this area and juxtaposing this with the above-described fact of business priorities, it is worth considering whether all identified risks and designed security mechanisms can be implemented and supervised in-house. Many even large enterprises do not necessarily have (want to have) the necessary staff to create and maintain security measures - outsourcing may be a strategy in such a case. It should be remembered, however, that not every type of mechanism can be implemented externally (just as not every risk can or should be transferred outside the organisation). The unquestionable advantage of outsourcing part of the security elements is the automatic scaling along with the growth of demand/development of the organisation, as well as greater daily and knowledge coverage in the case of specialised entities. Often this type of investment allows us to see how regularly security attacks are attempted.

5. Summary. Security Is a Process.

Summing up the considerations related to information security in a law office, it is important to mention that security is by no means a fixed state once and for all - we can only talk about managing it as a process and it should be regularly evaluated, monitored, and developed. Also, a proper understanding of audits and reviews will help us avoid erroneous

loss of vigilance - a security assessment only gives us a kind of "snapshot" for a given moment in time, and by no means a guarantee of security until the next audit. The current approach to security compliance increasingly points to the sensibility of developing continuous monitoring of the required security parameters, often combined with mechanisms for implementing changes, software, etc., rather than conducting only periodic audits.