20 June 2025

Адвокатская газета
Орган Федеральной палаты адвокатов РФ

Information security in law firms

Ways to protect against data leakage

Fokina Daria

Legal tech leader, lawyer
"Tomashevskaya & Partners" Law Firm

Lawyer associations and law firms that work with confidential information are often targeted by cybercriminals.

As Bird&Bird partner Simon Shooter noted in 2016 in an interview with Legal Insight magazine, attackers evaluate potential victims by three key parameters: the ability to access data, the value of information, and the cost of effort required to obtain it.

Lawyer associations and law firms process significant amounts of information, including both publicly available data and restricted information. A striking example of vulnerability can be called the case of Mossack Fonseca in April 2016, when as a result of a large-scale cyber attack, more than 11.5 million documents that revealed details of offshore schemes got into the network. Leaks of confidential information entail not only financial losses, but also serious reputational risks, and therefore ensuring information security becomes a strategic priority for law firms.

A study conducted by CSI and Legal Insight in 2016 showed that 48% of respondents consider IT infrastructure security and information protection to be a top priority, while 51% noted that a full-time IT specialist deals with cybersecurity issues in the company.

According to the 2025 quantitative anonymous survey conducted by Tomashevskaya & Partners among law firms (hereinafter referred to as the survey), more than 62% of them do not have a person responsible for information security. Therefore, the first step to ensuring information security is to appoint an appropriate specialist. The survey also revealed the three most popular measures to prevent leaks in law firms:

- access control (87%);
- employee training (70%);
- data security policy (50%).

The least common but equally important measures are information security audits to identify security weaknesses and the implementation of DLP systems that analyze all incoming and outgoing information to track questionable transactions and identify leaks.

Protecting against physical data leaks is also important. The main risk factor is the human factor. Experts note that data is often read by photographing the screen of a computer, tablet or smartphone. To prevent such leaks, it is recommended to use special films that make the monitor invisible to cameras.

Alexander Sverdlov, in his book "Protecting a Law Firm from Hacker Attacks and Insider Threats," cited 14 elements of the firm's information security system, most of which were not identified by respondents in the survey. These elements are also largely applicable to lawyers and lawyers associations.

First element: manage passwords and access.

Many companies force employees to regularly change complex passwords, believing that this increases security. However, the opposite effect often occurs – complex passwords are difficult to remember, so people write them down (at the risk of losing or revealing access) or simplify them, negating all protection against cyber threats. Paradoxically, a password that seems complicated, such as" P@ssword123 " (with a capital letter, numbers, and more than 10 characters), can be considered safe in the vast majority of organizations: according to statistics, about 5% of employees use it. This means that an attacker can guess passwords from 5% of email accounts!

An effective solution is to use a corporate password manager. This is a system that automatically generates complex and unique passwords, stores them in a secure location, and allows IT administrators to access resources only through this system. It is important that all the company's assets are accounted for in the password manager, and employees do not have the opportunity to choose them themselves. This policy ensures a high level of security and reduces the risk of data leakage. Access rights differentiation, technical restriction of information processing, and the use of two-factor authentication significantly increase the level of protection.

Element Two: remote access.

Remote access to corporate resources is always risky. To minimize this risk, it is necessary to ensure that all connections are encrypted and implemented through a secure tunnel; that laptops, computers, and mobile devices are protected by a firewall, that they are regularly updated and that unwanted connections are rejected; and that additional authentication is provided.

In 2020, BA “Yukov & Partners” emphasized the importance of technical tools: secure remote access, encryption of traffic and communication channels, forced blocking of gadgets, the possibility of remote data deletion, checking email for confidential information and prohibiting its sending. LO «Koblev & Partners» noted that the number of attacks on law firms will grow, as they are the custodians of information about clients’ finances, transactions, trade secrets and evidence.

Third element: policies and procedures.

For effective protection against cyber threats, it is necessary to develop clear rules-policies and procedures. It is important that these rules are adapted to the specifics of the company and take into account the specifics of its activities.

These rules are usually based on:

- privacy policy: defines how confidential data is processed and protected.
- acceptable use of IT assets policy: sets rules for the use of computers, networks, and other IT resources.
- code of conduct: defines ethical standards and principles for employees in the field of information security;
- network protection policy: describes measures to protect the corporate network from external and internal threats.
- incident response policy: defines the procedure for actions in case of detection of a cyberattack or security breach.
- vulnerability management policy: describes the process of identifying, evaluating, and eliminating vulnerabilities in IT systems.
- endpoint protection policy: sets rules for protecting employees ' computers, laptops, and mobile devices.
- security enhancement policy: describes measures to improve the overall security of the IT infrastructure.
- asset management policy: defines the order of accounting and control of the company's IT assets.
- mitigation of the consequences of cyber attacks.

To understand how vulnerable a company is to cyber attacks, you should conduct a threat simulation. This is a process that helps identify security vulnerabilities. Threat modeling helps detect not only technical vulnerabilities in software and hardware, but also deficiencies in business processes, procedures, personnel training, and even in the physical security of the IT infrastructure. The essence of the analysis is to identify all possible ways in which an attacker (or even a random error) can harm the company. Through this process, you can identify priority areas for strengthening security and allocate resources efficiently.

Fourth element: security awareness.

Employee training is a key element of protecting against cyber threats. It is important that the training sessions are regular, clear and accessible, and not just a list of technical terms.

An effective approach is to use practical examples. For example, the IT department may send out a phishing test email that simulates a real threat. If an employee clicks the link, the system automatically notifies the IT department. After that, a message is sent to the employee stating that this was a test and they need to re-pass information security training. This approach allows you to demonstrate the risks and consolidate the knowledge gained in practice. This is not just training, but a vigilance test that helps employees learn how to recognize real threats and prevent them.

Fifth: cloud security infrastructure.

Currently, most law firms actively use cloud services for storing data and running applications, and this is logical: no organization, even the largest, can match the level of investment in the security of giant companies. In this regard, the use of cloud providers is becoming the only realistic way for many law

firms to provide reliable protection against cyber threats. Economies of scale allow them to effectively resist a huge number of attacks, while an individual company often does not have sufficient resources.

A key aspect of protecting cloud services is protecting administrative access. You can't just rely on your username and password – you need to implement additional layers of security and strictly control who gets access to your data and when.

Sixth: protection of IT infrastructure within the law firm.

Security enhancements should be applied to all devices on the network, not just servers and employees' computers. Such seemingly "harmless" devices as printers are often overlooked.

Most IT administrators connect printers to the network using accounts, most often from the corporate Active Directory. However, even if the administrator logged in to the printer with their own account and then configured it with more restricted access rights, the device may still have the "fingerprint" or "hash" of this account. If it remains valid, an attacker can gain access to it and, accordingly, full control over the company's IT infrastructure.

Seventh element: vulnerability and patch management.

IT systems are a complex network of interconnected components. Fixing one vulnerability may inadvertently disrupt critical business processes. In this regard, vulnerability management and installing updates is a process that requires a systematic approach. It is important not only to identify and fix vulnerabilities in time, but also to motivate the IT team, monitor its performance and constantly improve the process.

Key performance indicators (KPIs) it is advisable to evaluate the individual performance of responsible employees (timely scanning, notification and correction of vulnerabilities) and the overall dynamics – for example, the decrease in the number of untreated vulnerabilities in each category (critical, high, medium and low) over time. This approach allows you to increase the level of security and minimize risks for the company.

The eighth: penetration testing.

Penetration testing (or "attack simulation") is a way to test a company's security by simulating the actions of a real attacker. The advantage of this approach is that testers use the same tools and tactics as cybercriminals, and often successfully penetrate the system. The resulting report allows you to identify and fix security vulnerabilities. However, it is important to keep in mind that penetration testing is not an exhaustive security analysis.

The tester, as a rule, stops at the first method of penetration found into the system, without wasting time searching for other vulnerabilities. It reports the found entry point, because it allowed it to achieve the goal of gaining access to the company's network. This means that there may be other undisclosed vulnerabilities in the system that can be used for unfair purposes.

The ninth: endpoint security.

Despite the fact that the administrator may feel like the "master" on his computer, he must comply with the same strict information security rules as any other employee of the company.

To increase security, we recommend creating two user profiles for each administrator:

- regular user: for everyday work (reading email, working together, and editing documents).
- administrative user (to perform tasks that require elevated privileges).

It is advisable for an administrator to use the “Run as”, or “sudo”, function to increase their privileges only when it is necessary to perform administrative tasks. This helps limit potential damage in the event of a compromised account.

Tenth element: security monitoring.

To ensure security, it is necessary to regularly monitor the activity of the entire IT infrastructure of the company. This includes monitoring network devices (computers, servers, and routers), as well as analyzing Internet traffic. Regular monitoring allows you to identify and respond to any suspicious activities or potential threats in a timely manner.

The eleventh: prevent, detect, and respond to incidents.

Prevention of information security incidents includes a number of measures – in particular, the prohibition of self-installation of software by employees, mandatory two-factor authentication for remote access to corporate resources, and encryption of all devices - from laptops to mobile phones.

The introduction of a security monitoring system can lead to a sharp increase in the number of alerts, including real-world incidents. Many companies are surprised by the amount of activity that they begin to record on the network when they get a complete picture of what is happening.

The task of information security specialists is to quickly detect hacks – both internal and external – and isolate intruders before they can cause serious damage to the company.

The twelfth element: email and communication security.

Two-factor authentication significantly improves security, but it doesn't guarantee full email protection. To ensure the confidentiality of important correspondence, we recommend using encryption so that only authorized recipients can access messages. In addition, you should use secure messengers instead of public ones to ensure the confidentiality of correspondence.

Thirteenth: security of web services.

There are many ways that attackers can attack a website, so it is important to pay attention to protecting against all possible vulnerabilities.

You can start by using strong passwords generated by the password manager for all accounts that require a password. This applies to remote access to the web server, databases, site management panels, user accounts that can edit content, and, most importantly, the backup system. Protecting the latter is just as important as protecting the web server, because hackers often choose the easiest way-hacking a backup copy to gain access to data.

Thus, strengthening information security is not just a necessity, but also a reasonable precaution.