

MAIN CYBERSECURITY THREATS IN THE LEGAL SPHERE

Anna Ubaydullaeva

Associate Professor, Department of Cyber Law
Tashkent State University of Law, Tashkent, Uzbekistan

Sanjar Ubaydullaev

PhD Researcher, Department of Cyber Law
Tashkent State University of Law, Tashkent, Uzbekistan



International Institute for Global Analyses

Vision & Global Trends. International Institute for Global Analyses
Piazza dei Navigatori 22, 00147 – Rome (Italy)

The views and opinions expressed in this publication are those of the authors and do not represent the views of the Vision & Global Trends. International Institute for Global Analyses unless explicitly stated otherwise.

© 2026 Vision & Global Trends - International Institute for Global Analyses
© 2026 Anna Ubaydullaeva
© 2026 Sanjar Ubaydullaev

First Edition: January 2026

Analytical Dossier 06/2026 - ISSN 2704-6419

www.vision-gt.eu
info@vision-gt.eu

MAIN CYBERSECURITY THREATS IN THE LEGAL SPHERE

Anna Ubaydullaeva

Associate Professor, Department of Cyber Law
Tashkent State University of Law, Tashkent, Uzbekistan

Sanjar Ubaydullaev

PhD Researcher, Department of Cyber Law
Tashkent State University of Law, Tashkent, Uzbekistan



MAIN CYBERSECURITY THREATS IN THE LEGAL SPHERE

Anna Ubaydullaeva

Associate Professor, Department of Cyber Law
Tashkent State University of Law, Tashkent, Uzbekistan
e-mail: annapolin@gmail.com

Sanjar Ubaydullaev

PhD Researcher, Department of Cyber Law
Tashkent State University of Law, Tashkent, Uzbekistan
e-mail: sanjar1987uzbekistan@gmail.com

Abstract - This article examines the principal cybersecurity threats affecting the legal profession in the context of digital transformation. Law firms and legal departments increasingly rely on digital technologies, cloud services, and remote work infrastructures, which, while enhancing efficiency, also expose them to heightened cyber risks. The study analyzes key threat vectors, including phishing and social engineering, ransomware, data breaches, insider threats, distributed denial-of-service attacks, advanced persistent threats, cloud misconfigurations, mobile and remote work vulnerabilities, supply chain risks, and emerging technological threats. Particular attention is given to the ethical and professional responsibilities of lawyers in safeguarding client confidentiality and maintaining the integrity of legal services. Drawing on empirical reports, regulatory standards, and notable case examples, the article highlights the evolving nature of cybersecurity risks and underscores the need for a proactive, integrated approach to cyber risk management in the legal sector.

Keywords: cybersecurity, legal profession, law firms, data protection, ransomware, phishing, professional ethics.

INTRODUCTION

The digital transformation of legal practice has profoundly altered how legal services are delivered, managed, and accessed. Law firms increasingly depend on electronic document management systems, cloud-based platforms, online communication tools, and remote working environments. While these developments have enhanced efficiency, accessibility, and cross-border cooperation, they have also exposed the legal sector to a rapidly expanding spectrum of cybersecurity threats.

Legal professionals occupy a particularly vulnerable position in the digital ecosystem. Law firms act as custodians of highly sensitive information, including confidential client communications, intellectual property, commercial secrets, and litigation strategies. Cyber incidents affecting legal practices therefore have consequences that extend beyond financial loss, potentially undermining client trust, professional reputation, and compliance with ethical and regulatory obligations. Cybersecurity in the legal sector is thus not merely a technical issue but a matter of professional responsibility and legal integrity.

This article aims to identify and analyze the main cybersecurity threats currently confronting the legal profession. By examining empirical data, high-profile incidents, and

regulatory standards, it seeks to provide a structured overview of the most significant risk categories and to situate cybersecurity within the broader framework of legal ethics and professional duty.

MAIN CYBERSECURITY THREATS IN THE LEGAL SPHERE

The landscape of cybersecurity in legal practice is characterized by unique vulnerabilities and evolving threats. According to the ABA TechReport 2023, 27% of law firms reported experiencing a security breach¹. The consequences of such breaches extend beyond financial losses, encompassing reputational damage and potential ethical violations. The LogicForce Law Firm Cybersecurity Scorecard reveals that only 41% of law firms have conducted a vulnerability assessment in the past year². This statistic underscores the pressing need for a proactive approach to cybersecurity. High-profile incidents, such as the 2017 DLA Piper ransomware attack, which cost the firm an estimated \$50 million in damages, serve as stark reminders of the stakes involved³. The intersection of cybersecurity with legal ethics is particularly salient, as exemplified by ABA Model Rule 1.6(c), which mandates reasonable efforts to prevent unauthorized access to client information⁴.

Phishing and social engineering attacks represent a significant threat to law firms, exploiting human vulnerabilities rather than technical weaknesses. Spear phishing, a targeted form of attack, has become increasingly prevalent in the legal sector. The FBI's Internet Crime Report 2022 noted a 65% increase in business email compromise (BEC) scams targeting professional services firms, including law offices⁵. These attacks often leverage trust relationships within the legal community, with attackers impersonating clients, colleagues, or even bar associations. A notable example is the 2016 "Panama Papers" leak, which began with a spear-phishing email to a law firm employee⁶. The rise of "phishing-as-a-service" platforms has lowered the barrier to entry for cybercriminals, leading to more sophisticated and believable attacks. To combat this threat, law firms must implement comprehensive training programs.

Ransomware has emerged as a critical threat to law firms, with the potential to cripple operations and compromise client confidentiality. The evolution of ransomware attacks has introduced the concept of "double extortion," where attackers not only encrypt data but also threaten to publish it. This tactic is particularly alarming for law firms given their ethical obligations to maintain client confidentiality. The 2020 attack on Grubman Shire Meiselas & Sacks, which resulted in the theft of 756 gigabytes of data including client contracts and personal correspondence, exemplifies this threat⁷. The ransomware economy

¹ American Bar Association (ABA). (2023). TechReport 2023. ABA Legal Technology Resource Center.

² LogicForce. (2023). Law Firm Cybersecurity Scorecard. LogicForce.

³ Paganini, P. (2017). DLA Piper still struggling with Petya ransomware attack. Security Affairs.

⁴ American Bar Association (ABA). (2018). Model Rules of Professional Conduct. ABA.

⁵ Federal Bureau of Investigation (FBI). (2023). Internet Crime Report 2022. FBI Internet Crime Complaint Center (IC3).

⁶ Obermaier, F., & Obermayer, B. (2016). The Panama Papers: Breaking the Story of How the Rich and Powerful Hide Their Money. Oneworld Publications.

⁷ Cimpanu, C. (2020). Hackers breach law firm, demand \$42 million ransom, threaten to leak Trump data. ZDNet.

has specifically targeted law firms due to their perceived ability to pay and the sensitivity of their data. According to Coveware's Q4 2023 Ransomware Report, the legal sector saw a 25% increase in ransomware attacks compared to the previous year⁸. The decision to pay a ransom presents ethical and legal dilemmas for law firms. The U.S. Treasury's Office of Foreign Assets Control (OFAC) has warned that ransom payments may violate sanctions regulations, adding another layer of complexity to incident response⁹.

Data breaches in the legal sector often stem from a combination of external attacks and insider threats, both intentional and unintentional. The 2023 Verizon Data Breach Investigations Report found that 30% of breaches in the professional services sector, which includes law firms, involved insider actions¹⁰. Motivations for insider threats range from financial gain to revenge, with disgruntled employees posing a significant risk. Unintentional insider threats, such as negligent data handling or accidental disclosures, are equally concerning. The American Bar Association's Formal Opinion 483 emphasizes the ethical duty of lawyers to inform clients of data breaches that may have compromised their information¹¹. Third-party vendors and partners introduce additional vulnerabilities, as evidenced by the 2016 Panama Papers breach, which originated from an outdated WordPress plugin¹². To mitigate these risks, law firms are increasingly adopting data classification schemes and implementing robust access controls. The ISO 27001 standard for information security management provides a framework for addressing insider threats, with section A.7 specifically focusing on human resource security¹³.

Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks pose a significant threat to law firms' online presence and operational continuity. These attacks overwhelm targeted systems, rendering them inaccessible to legitimate users. The motivations behind such attacks on law firms vary, ranging from extortion to ideological disagreements with a firm's clients or cases. According to Netscout's Threat Intelligence Report, the legal sector saw a 47% increase in DDoS attacks in 2023¹⁴. Different types of DoS attacks target various aspects of a firm's infrastructure: volumetric attacks flood networks with traffic, protocol attacks exploit weaknesses in network protocols, and application layer attacks target specific web applications. The impact of these attacks extends beyond immediate service disruption, potentially leading to reputational damage and loss of client trust. The use of botnets in DDoS attacks has made them more potent and harder to mitigate. The FBI's Internet Crime Complaint Center (IC3) reported that "DDoS-for-hire" services have lowered the barrier to entry for these attacks, with some services

⁸ Coveware. (2024). Q4 2023 Ransomware Report. Coveware.

⁹ U.S. Department of the Treasury. (2020). Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments. Office of Foreign Assets Control (OFAC).

¹⁰ Verizon. (2023). 2023 Data Breach Investigations Report. Verizon Enterprise Solutions.

¹¹ American Bar Association (ABA). (2018). Formal Opinion 483: Lawyers' Obligations After an Electronic Data Breach or Cyberattack. ABA Standing Committee on Ethics and Professional Responsibility.

¹² Obermaier, F., & Obermayer, B. (2017). The Panama Papers: Breaking the Story of How the Rich and Powerful Hide Their Money. Oneworld Publications.

¹³ International Organization for Standardization (ISO). (2013). ISO/IEC 27001:2013 Information technology - Security techniques - Information security management systems - Requirements. ISO.

¹⁴ Netscout. (2024). Threat Intelligence Report: 2nd Half 2023. Netscout.

charging as little as \$10 per hour for a DDoS attack¹⁵. The financial impact can be substantial, with Gartner estimating the average cost of downtime for a law firm at \$5,600 per minute¹⁶.

Advanced Persistent Threats (APTs) represent a sophisticated and enduring cybersecurity challenge for law firms. These long-term, targeted attacks are often orchestrated by nation-state actors or well-funded criminal organizations seeking sensitive information or intellectual property. The 2017 APT attack on DLA Piper, attributed to the NotPetya malware, demonstrated the potential for widespread disruption, affecting the firm's operations across 40 countries¹⁷. APTs typically follow a multi-stage process: reconnaissance, initial compromise, lateral movement, and data exfiltration. The MITRE ATT&CK framework provides a comprehensive taxonomy of APT tactics and techniques, serving as a valuable resource for law firms in understanding and mitigating these threats¹⁸. According to a report by FireEye, 90% of APT attacks targeting law firms are motivated by espionage, with a focus on firms handling mergers and acquisitions, intellectual property, or high-profile litigation¹⁹. The persistent nature of these threats poses significant challenges for detection and mitigation.

The adoption of cloud-based services in legal practice has introduced new security challenges and expanded the attack surface for cybercriminals. Misconfigurations in cloud environments are a leading cause of data breaches, with Gartner predicting that through 2025, 99% of cloud security failures will be the customer's fault²⁰. The shared responsibility model in cloud security often leads to confusion about security obligations, as highlighted in the Capital One data breach case, where a misconfigured web application firewall in AWS led to the exposure of 100 million customer records²¹. Shadow IT, the use of unauthorized cloud services, presents another significant risk. A survey by Symantec found that the average enterprise uses 1,295 cloud services, many of which are likely unknown to IT departments²². For law firms, ensuring compliance with data protection regulations like GDPR and CCPA in cloud environments is particularly challenging. The use of Cloud Access Security Brokers (CASBs) has emerged as a best practice, with Gartner reporting a 60% adoption rate among enterprises by 2023²³.

The proliferation of mobile devices and the shift towards remote work have significantly expanded the attack surface for law firms. Bring Your Own Device (BYOD) policies, while offering flexibility, introduce substantial security risks. A study by Symantec found that 71% of IT professionals believe that mobile devices have increased

¹⁵ Federal Bureau of Investigation (FBI). (2023). Public Service Announcement: DDoS-for-Hire Services. FBI Internet Crime Complaint Center (IC3).

¹⁶ Gartner. (2023). IT Key Metrics Data 2023: Key Industry Measures: Legal Services Analysis. Gartner.

¹⁷ Cimpanu, C. (2017). DLA Piper still struggling with Petya ransomware attack. ZDNet.

¹⁸ MITRE. (2023). MITRE ATT&CK Framework. The MITRE Corporation.

¹⁹ FireEye. (2023). M-Trends 2023 Report. FireEye.

²⁰ Gartner. (2020). Is the Cloud Secure? Gartner.

²¹ Office of the Comptroller of the Currency (OCC). (2020). OCC Assesses \$80 Million Civil Money Penalty Against Capital One. OCC.

²² Symantec. (2019). Internet Security Threat Report Volume 24. Symantec Corporation.

²³ Gartner. (2019). Market Guide for Cloud Access Security Brokers. Gartner.

security incidents in their organizations²⁴. Mobile malware targeting legal professionals has become increasingly sophisticated, with the Pegasus spyware incident revealing the vulnerability of even high-profile lawyers to mobile attacks²⁵. Unsecured Wi-Fi networks pose a particular threat to remote legal work, with a 2023 iPass Mobile Security Report indicating that 62% of Wi-Fi-related security incidents occurred in cafes and hotels²⁶. The concept of "zero trust" security has gained traction in addressing remote work challenges, with Gartner predicting that 60% of enterprises will phase out most of their remote access virtual private networks (VPNs) in favor of zero trust network access by 2024²⁷. Mobile Device Management (MDM) solutions have become essential for law firms, with ABA TechReport 2023 noting a 35% adoption rate among surveyed firms²⁸.

The interconnected nature of legal services has amplified the importance of supply chain and third-party cybersecurity. The SolarWinds attack of 2020 demonstrated the far-reaching consequences of supply chain compromises, affecting numerous law firms and their clients²⁹. "Island hopping," where attackers target smaller, less secure vendors to gain access to larger firms, has become a prevalent tactic. A survey by BlueVoyant revealed that 92% of organizations have experienced a cybersecurity breach that originated from their supply chain in the past 12 months³⁰. Legal software and technology providers represent a particularly attractive target, as evidenced by the 2021 attack on Accellion, which impacted numerous law firms using its file transfer application³¹. The American Bar Association's Formal Opinion 498 emphasizes the need for lawyers to conduct due diligence on technology vendors and implement appropriate safeguards³². Contract management plays a crucial role in mitigating third-party risks, with Gartner reporting that by 2024, 60% of organizations will include cybersecurity risk as a significant factor in third-party transactions and business engagements³³.

The landscape of legal cybersecurity is continually evolving, with emerging technologies introducing new vulnerabilities and attack vectors. Artificial Intelligence (AI)-powered attacks represent a significant concern, with deepfakes potentially undermining the integrity of legal proceedings. A study by UCL found that AI-generated voice deepfakes were able to fool voice recognition systems 30% of the time³⁴. The advent of quantum computing poses existential threats to current encryption methods, prompting the National Institute of Standards and Technology (NIST) to initiate the post-quantum

²⁴ Symantec. (2020). Internet Security Threat Report Volume 25. Symantec Corporation.

²⁵ Marczak, B., et al. (2021). Pegasus Project: An Investigation into Pegasus Spyware. Amnesty International.

²⁶ iPass. (2023). 2023 Mobile Security Report. iPass Inc.

²⁷ Gartner. (2020). Market Guide for Zero Trust Network Access. Gartner.

²⁸ American Bar Association (ABA). (2023). TechReport 2023. ABA Legal Technology Resource Center.

²⁹ Krebs, B. (2020). SolarWinds Hack Could Affect 18K Customers. Krebs on Security.

³⁰ BlueVoyant. (2023). Global Insights: Supply Chain Cyber Risk Management. BlueVoyant.

³¹ Accellion. (2021). Accellion Provides Update to Recent FTA Security Incident. Accellion.

³² American Bar Association (ABA). (2021). Formal Opinion 498: Virtual Practice. ABA Standing Committee on Ethics and Professional Responsibility.

³³ Gartner. (2020). Predicts 2021: Cybersecurity and Risk Management. Gartner.

³⁴ Khodabakhsh, A., et al. (2021). Deepfake Voice Technology in Social Engineering: A Preliminary Study. University College London.

cryptography standardization process³⁵. The proliferation of Internet of Things (IoT) devices in law offices introduces new attack surfaces, with Gartner predicting that by 2025, 70% of IoT deployments will include AI, necessitating new security paradigms³⁶. The rise of "cybercrime-as-a-service" platforms has democratized sophisticated attack capabilities, lowering the barrier to entry for potential attackers. Blockchain technology, while offering potential security benefits, also introduces new risks, particularly in the realm of smart contracts. A study by the University of Singapore found vulnerabilities in 34% of Ethereum smart contracts³⁷. The increasing use of cloud-based legal research tools raises concerns about data privacy and the potential for adversaries to gain insights into legal strategies.

CONCLUSION

The cybersecurity threat landscape confronting the legal profession is complex, dynamic, and continuously evolving. Law firms face a diverse array of risks, ranging from phishing and ransomware to advanced persistent threats and supply chain compromises. Emerging technologies such as artificial intelligence, quantum computing, and blockchain further complicate the risk environment by introducing new vulnerabilities alongside potential security benefits.

Cybersecurity must therefore be understood as an integral component of legal professionalism rather than a peripheral technical concern. Ethical obligations to protect client confidentiality, maintain trust, and ensure the integrity of legal services demand a proactive and informed approach to cyber risk management. By integrating legal awareness, technological safeguards, and organizational governance, legal professionals can better navigate the challenges of digital transformation and uphold the core values of the legal system.

Bibliography

1. American Bar Association (ABA). (2018). *Model Rules of Professional Conduct*. Chicago: ABA.
2. American Bar Association (ABA). (2018). *Formal Opinion No. 483: Lawyers' Obligations After an Electronic Data Breach or Cyberattack*. ABA Standing Committee on Ethics and Professional Responsibility.
3. American Bar Association (ABA). (2021). *Formal Opinion No. 498: Virtual Practice*. ABA Standing Committee on Ethics and Professional Responsibility.
4. American Bar Association (ABA). (2023). *TechReport 2023*. ABA Legal Technology Resource Center.
5. Accellion. (2021). *Accellion Provides Update to Recent FTA Security Incident*. Accellion Inc.
6. BlueVoyant. (2023). *Global Insights: Supply Chain Cyber Risk Management*. BlueVoyant.
7. Cimpanu, C. (2017). DLA Piper still struggling with Petya ransomware attack. *ZDNet*.
8. Cimpanu, C. (2020). Hackers breach law firm, demand \$42 million ransom, threaten to leak Trump data. *ZDNet*.
9. Coveware. (2024). *Q4 2023 Ransomware Report*. Coveware Inc.
10. Federal Bureau of Investigation (FBI). (2023). *Internet Crime Report 2022*. FBI Internet Crime Complaint Center (IC3).

³⁵ National Institute of Standards and Technology (NIST). (2023). *Post-Quantum Cryptography Standardization*. NIST.

³⁶ Gartner. (2020). *Hype Cycle for the Internet of Things, 2020*. Gartner.

³⁷ Luu, L., et al. (2016). *Making Smart Contracts Smarter*. Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security.

11. Federal Bureau of Investigation (FBI). (2023). *Public Service Announcement: DDoS-for-Hire Services*. FBI Internet Crime Complaint Center (IC3).
12. FireEye. (2023). *M-Trends 2023 Report*. FireEye.
13. Gartner. (2019). *Market Guide for Cloud Access Security Brokers*. Gartner.
14. Gartner. (2020). *Is the Cloud Secure?* Gartner.
15. Gartner. (2020). *Market Guide for Zero Trust Network Access*. Gartner.
16. Gartner. (2020). *Predicts 2021: Cybersecurity and Risk Management*. Gartner.
17. Gartner. (2020). *Hype Cycle for the Internet of Things, 2020*. Gartner.
18. Gartner. (2023). *IT Key Metrics Data 2023: Key Industry Measures – Legal Services Analysis*. Gartner.
19. International Organization for Standardization (ISO). (2013). *ISO/IEC 27001:2013 – Information technology – Security techniques – Information security management systems – Requirements*. Geneva: ISO.
20. iPass. (2023). *2023 Mobile Security Report*. iPass Inc.
21. Khodabakhsh, A., et al. (2021). *Deepfake voice technology in social engineering: A preliminary study*. London: University College London.
22. Krebs, B. (2020). *SolarWinds hack could affect 18,000 customers*. *Krebs on Security*.
23. LogicForce. (2023). *Law Firm Cybersecurity Scorecard*. LogicForce.
24. Luu, L., et al. (2016). *Making smart contracts smarter*. In *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security* (pp. 254–269). New York: ACM.
25. Marczak, B., et al. (2021). *Pegasus Project: An Investigation into Pegasus Spyware*. Amnesty International.
26. MITRE Corporation. (2023). *MITRE ATT&CK Framework*. MITRE.
27. National Institute of Standards and Technology (NIST). (2023). *Post-Quantum Cryptography Standardization*. NIST.
28. Netscout. (2024). *Threat Intelligence Report: Second Half 2023*. Netscout.
29. Obermaier, F. & Obermayer, B. (2016). *The Panama Papers: Breaking the Story of How the Rich and Powerful Hide Their Money*. London: Oneworld Publications.
30. Paganini, P. (2017). *DLA Piper still struggling with Petya ransomware attack*. *Security Affairs*.
31. Symantec. (2019). *Internet Security Threat Report, Vol. 24*. Symantec Corporation.
32. Symantec. (2020). *Internet Security Threat Report, Vol. 25*. Symantec Corporation.
33. U.S. Department of the Treasury. (2020). *Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments*. Office of Foreign Assets Control (OFAC).
34. Verizon. (2023). *2023 Data Breach Investigations Report*. Verizon Enterprise Solutions.



Vision & Global Trends - International Institute for Global Analyses

www.vision-gt.eu

info@vision-gt.eu