Deep Science Publishing
https://doi.org/10.70593/978-93-49910-38-6_4

DeepScience
Open Access Books

# Chapter 4: Security-first strategy: Protecting data in tax and advisory workflows

## 4.1. Introduction

Failure to safeguard sensitive data in tax advisory business relies on an organization's ability to remain aware. The focus of this text is to assess ways data might be insecure in tax and advisory workflows and identify ways to mitigate this risk. Tax and advisory community members who manage confidential data understand the consequences of data getting into the wrong hands. Involved with engagement workflows that ultimately handle tax returns, M&A information, and legal documents, businesses are exceedingly aware of the potential damage through lost business, reputational damage, or even fines and legal action. Encryption, two-factor authentication, and email activity monitoring systems have become prevalent discussion topics.

In preparing the text for publication, additional commonplace pieces of knowledge were uncovered. The woke metaverse has arrived. Controllers that anticipatively close records are far more favorable than those that are retrospective or forensic. The next generation of software audit tools is daughter company-backed. Not one but three intrusive reviews at the same time may very well happen. Data co-ops will enable deeper analytics outside internal firewalls. The audit may end up being a taxpayer capability. For the tax and advisory community, "excellent solutions" applying such commonplace knowledge must be considered. Protecting valuable data before a breach occurs is far superior to examining it afterward.

Security-first strategies that afford complete assurance against breach were evaluated and the protective autonomy envisioned of "excellent solutions", however unlikely, is understood. The world is likely to be a bit safer regardless of whether the 10,000th fixed penalty comes to pass. When the tax advisory industry as a whole gets hacked, it is clear it will turn into an "afterward" industry. Some discussions on improved engagement and

assurance workflow safety rely on existing technology, just not implemented yet.Subject trust is an agent's level of belief in the competency of another agent, something that is taken for granted between audit firms and their clientele. Trust though does not come easy, nor is it something which can solely be relied upon. Rather, trust is a two-way street, requiring an ardent upkeep given a heavy reliance on cloud-based systems and the continuing pace of change in the adversarial capabilities of hackers. That maintenance depends upon communication with clients about new risks and adherence to security practices. External communications are critical, though they are not the terminus of the maintenance of trust. Building on a foundation of trust requires internal maintenance through continual engagement with elements of the audit process. Otherwise, honesty, integrity, and strong vigilance over security practices begin to falter, and behind-the-scenes, untrusted systems can proliferate rapidly, deleteriously affecting client trust and relations.


**Fig 4.1:** Successful Data Protection Strategy

### 4.1.1. Background and Significance

Amidst a constantly evolving digital landscape, firm fidelity is increasingly dependent upon cloud-based storage, performance, and guidelines. These workflows generate confidential data with ever-increasing frequency, data that the firm and clients expect to be kept safe. However, as those workflows have transitioned to various cloud-based SaaS services and platforms, data has been simultaneously lost, breached, and exploited. These events have rippled throughout the firm, creating havoc for performance and client relations while crafting a high level of wariness among the firm's employees and clients alike. A security-first approach is taken to assess the state of the firm's oft-overlooked SaaS data security, with interns tasked with interrogating SaaS platforms utilized by employees within tax and advisory departments about security practices in tandem with a review of the platforms' available public security documentation. The findings suggest a generally high state of maturity, though issues of educated systems entirely and documentation not kept current render risk. Recommendations for security practices to the firm and security-first teams, the prioritization of risks to clients, and constant engagement are offered to build upon existing trust and years of history.

## 4.2. Understanding Data Security

Decreasing reliance on internal networks has generated new challenges for accounting firms striving to secure confidential client data (Gounagias et al., 2018; Savić et al., 2021; Aladebumoye, 2025). Today, data is created and edited locally in applications by users via laptops, desktops, and web applications. These same contracts are then saved, cited or referenced, then risk of data is transferred to teams of consultants via email, cloud storage, or other modes of transmission. These delivery options are not secure enough when dealing with confidential client data. Accounting firms have access to extensive data protection and confidentiality resources. The additional need to protect many more data points, much less of which might be surveillance geopolitically sensitive, exists. Law firms should be on the lookout for legal complaints initiated with a firm's client or agent internally who reasonably believes they have been wronged. Data needs to be stored so they have a very low probability of collecting types of concerning comments involving the risk of espionage or worse. As with any product that seeks to remove a need, be aware that the need firstly might not exist. The hurdle before internal networks has been accessible and mediocre viewed.

### 4.2.1. Definition of Data Security

Data security is fundamentally concerned with protection against unauthorized access to hardware resources, software, and systems and preventing unauthorized modification,

theft, or loss of information using encryption, user access controls, network security, and other strategies. Protecting digital information is essential to a successful program. Data security in a workflow setting is collective, collaborative, and cooperative. Data security requires the cooperation of all individuals who have access to information to remain secure and protected from unauthorized access, modification, theft, or loss. Here are the responsibilities and steps required to ensure information continues to be kept securely on the system.

Data security begins with user authentication. User authentication is met by user name and password. That is, each member is assigned a unique username and password that must be entered correctly to gain access to the system. User authentication, once completed, is stored on the client system, and that is the basis for accessing information. There have been ongoing discussions about the ethical implications of 'security' in information science, mainly focusing on policies and practices about access management and intellectual security. Information security management (information security) is more concerned with 'information' protection rather than the 'system' itself, developing a decision, and implementing a judgment to protect the system and the information in the system. Security is defined as 'the state of being protected or safe from danger'. Security and technology are often intertwined, which is often reflected in information security management as a framework to connect technology to policies and regulations to legal requirements.

Information security encompasses broader areas than data security. That is, data security is a subset of information security. Information security addresses confidentiality, integrity, availability, authentication, and non-repudiation, whereas data security mainly focuses on confidentiality, integrity, and availability. Data security solutions currently in practice are generally regarded as frameworks, which in terms of range lack robustness, focusing on 'basic' levels (data inventory and classification) rather than 'advanced' levels (data challenge, compliance, and benchmarking). Data security is vital for a workflow. Data security has two types of considerations. The first type is based on preventing unauthorized and unauthorized access or changes to existing information. This includes prevention through user authentication and restricting access to sensitive information. The second type is about system robustness against hardware failure and data loss by keeping backup copies of existing workflows. Software is treated as needed.

### 4.2.2. Importance of Data Security in Tax Advisory

Data security is paramount in any significant organisation. An event of data loss or data breach could endanger the reputation of the concerned organisation, or alternatively affect its activity. By establishing straightforward business processes, diligent groundwork has been laid for monitoring data security at PwC, which is undertaken at

all levels and in all service lines. However, additional measures are required, particularly in the tax area, where treated data is more sensitive than in a typical advisory work flow, or in assurance businesses. Targeted attacks on tax departments of international companies are continuously increasing, and furthermore attacks from authorities and other parties are becoming serious threats.

Sensitive data should be treated as highly confidential, which means that no data should leave the company or service centre: no raw data, nor analysis results. This is particularly important in case of projects with attacks. Clients should be warned at the latest kick-off meeting to review their computer and data flow security from the beginning, financial data handled in their own environment is likely to be by far more exposed in the short or long run than if processed within the secure confines of corporate offices. Attackers must know names of people to contact through non-obligatory constraints in their highly controlled language. Implementation of the 'Atos principle' is warranted.

The more trustworthy a company and individuals are, the more security risks and data use dangers present at the same time. Preventive measures, ideally starting at the location with the highest security risks, can simply escalate to the next level of data safety and security. A productivity loss or less trust in an incumbent service provider is better than a successful data breach followed by a loss of service and trust up to the end client level.

Sensitive data should be treated as confidential. No raw data and analysis results should leave the company. Data should be stored on highly secure and closely monitored servers. Anonymization must take place prior to storing or transferring data. Anonymization must be enforced in such a way that the entire chain stays anonymous (from tax departments to individuals). All data must be deleted from private laptops or desktops as soon as a project is finished.

### 4.3. Regulatory Frameworks

The rapidly expanding digital world poses an ever-growing danger to people's right to the confidentiality of their personal data. There is a risk that protected data can be misused by third parties to their advantage. This is also true in legal proceedings, although legal secrecy is regarded as a cornerstone of the rule of law, and the right to protect personal data is defined as a key human right in the EU Charter of Human Rights. Data protection regarding the handling of information by practitioners is intended to reduce risks concerning the confidential data of clients and witnesses in accordance with this directive. In addition, the privacy and protection of the data shared with a tax or advisory practitioner is essential for the proper conduct of business based on confidential tax and advisory communication.

Tax and advisory practitioners gather and process significant amounts of sensitive personal information. They are therefore constantly obliged to pay special attention to data protection. Sensitive personal information is defined as specific data that reveals. In regard to sensitive personal information concerning an individual's race, ethnicity, political opinions, religion, philosophical beliefs, trade union membership, and the processing of genetic data, it is explicitly requested for protection purposes. Examples of sensitive personal information are information concerning a working-relationship and any individual arguments for taxation in a specific case. Professional secrecy guarantees the protection of sensitive personal information shared with the practitioner. However, the excessive use of technology and communication channels that only afford basic safety capabilities may result in security and privacy breaches.

Legal secrecy is enshrined in the respective legal orders of different jurisdictions using targeted definitions and regulatory frameworks that are binding on legal practitioners and their clerks. It is a cornerstone of the rule of law, constituting a prerequisite for a fair trial (Zheng et al., 2018; Zhang et al., 2022). Legal secrecy guarantees that sensitive personal information shared with a practitioner will not be disclosed to another party by that practitioner. It applies to all communication taking place in the context of a practitioner-client or advisor-client relationship, irrespective of the way that information is shared. Where no legal secrecy exists or where legal secrecy is violated, the legal proceedings conducted based on that shared information will be automatically invalid.

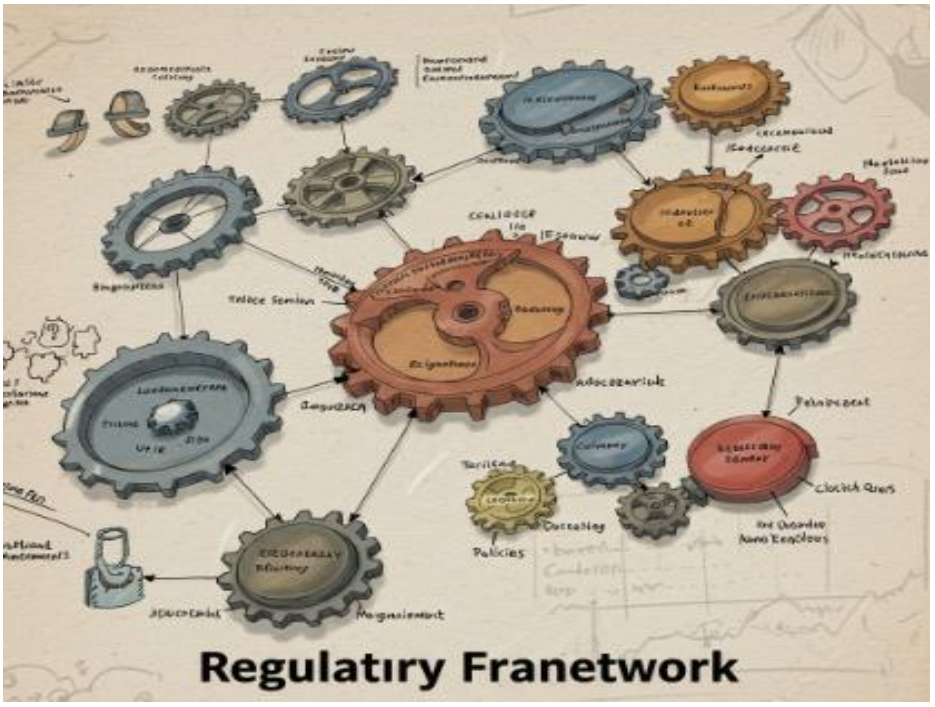


**Fig 4.2:** Regulatory Frameworks

### 4.3.1. Overview of Relevant Regulations

The ultimate goal of most laws governing privacy and security, in whatever jurisdiction, is to ensure reasonable protection of personal information. Following a survey, it was reported that a large portion of U.S. businesses indicated that they keep sensitive personal information for longer than necessary – a practice that increases the burden of compliance with privacy and security laws well beyond the original obligations. Moreover, such retention increases the risk of data breaches without commensurate benefits for the entity retaining the information. In regard to the informed-consent model on which a great part of the law governing privacy and security has been built, it is predicted that the current binds-free regimes will be detrimental to consumers.

1. A data breach occurs when personal information held by an enterprise is lost or transferred to an unauthorized party, as a result of incompetence of that enterprise, or consequent to an unlawful act. 2. What is meant by personal information varies according to the law. Personal data is information that identifies or enables the identification of a person; it includes names, addresses, information about a person's transactions, email addresses, telephone numbers, etc. Nowadays, this term is given a wider meaning, encompassing almost all forms of information of an identifiable individual. 3. Data breach laws are generally divided into three aspects. The first is breach-of-security notification, which requires that individuals whose personal information is endangered by a breach-of-security must be notified. The second aspect is the safeguarding of personal information, which typically creates a duty of care for businesses that handle personal information to develop and implement reasonable safeguards. The third aspect is protection of 'special' information, which provides extra protection for certain categories of personal information, such as those concerning health and financial data.

### 4.3.2. Compliance Requirements for Tax Professionals

Tax professionals are faced with compliance requirements from numerous countries and international associations. In addition to complying with applicable tax laws, these professionals are confronted with anti-money laundering legislation. While basic personal information on clients is often collected and stored on tax practices' servers, there is also strong competition among jurisdictions vying for taxpayers' capital and improved compliance.

In response to this competitive environment, international tax professionals have developed standard practices that have often been successful in addressing compliance issues with tax authorities. Some countries retain an audit-oriented approach to tax compliance that creates significant exposures for taxpayers and their tax advisors.

Transparency and data matching initiatives adopted by the OECD and the EU also create significant compliance issues for taxpayers and raise potential concerns regarding additional state taxation and non-consensual sharing of data among jurisdictions.

International tax professionals must contend with innumerable compliance issues in defending their clients' positions and challenges to compliance with the laws. The migration of information to digital form has created both opportunities for improved compliance and the risk that sensitive information might be hacked and made publicly available. The adoption of cloud-based solutions and data-sharing systems raises the difficulty of assessing the implications of this evolving digital landscape on compliance requirements and workflows, and how to develop security-first intranet and cloud-based systems to ensure compliance.

Tax professionals, advisors, and data analysts play a significant role in the voluntary compliance model used by many jurisdictions. It is essential for jurisdictions to develop compliance strategies that take advantage of the skills, motivation, and resources available from the private sector in a manner that does not create an unmanageable risk of non-compliance. Such collaboration will include a move to digital compliance that will drastically change the processes currently in place. This new compliance model can unfairly disadvantage smaller tax advisors and diminish competition if not carefully constructed.

### 4.4. Threat Landscape

The emergence of new technologies, such as smartphones and tablets, and new channels of communication, such as social networks, pose new cybersecurity challenges for the tax and advisory sectors. Burgeoning digital currencies, such as Bitcoin, as well as the popularity of new delivery channels and types of services, such as mobile payments and e-wallets, have also disturbed the fintech area. Therefore, the fintech industry has become a promising area for cyber adversaries and malicious actors to act. Cyber incidents can occur in various forms and vary in nature depending on the motivators and technologies associated with perpetrators, targets, and actions. Cybersecurity threat actors are categorized into four types, including the state-sponsored threat actors, hacktivists, cyber criminals, and script kiddies. They demonstrate different behaviors, traits, and capabilities and pose varying threats to information security to targets of different sectors.

Malware attacks have low cost, but a very high level of paid attack benefits, and as a consequence of these reasons, this type of attack is very prevalent among all threat actors. Also, as the lowest cost of attacks with very low level of destructiveness, Distributed Denial of Services (DDoS) attacks are frequently utilized by most hacktivists

and script kiddies. On the other hand, among attack types in the fintech sector, Social Engineering Attack has a lower level of destructiveness in comparison with other sectors, which simply implies that these attack types can be easily prevented by making users aware. Fintech is at risk of facing several internal threats, such as employees leaking the company's secretive information and collaboration with hackers. Engaging ex-trojan developers can be a chance for malicious actors to better target fintech actors. Also, since banks and financial organizations hold vast valuable information about customers, competitors, and the banking system, they have an incentive to hack. In the fintech domain, apart from the aforementioned actors, suspicious governmental sectors can also hack the targeted organization, such as governments in relation to Arab Spring issues.

### 4.4.1. Common Cyber Threats

Data security protection is achieved through cyber hygiene controls to improve the organization's cyber hygiene as much as possible. Organizations should put in place training and education programs, and tactical measures should address the actual identified risks, including data exposure, integrity, availability, and the attackers' methods. Organizations need to know what cloud services and appliances their data is stored on, who owns these machines, and to what abuse they are exposed. Special attention should be given to caching mechanisms, which are often employed by organizations to cache file services. An unexpected attack vector is opened if the vendor configurations of these caches are too wide. Media agencies should re-investigate old domain names and purchases in case they are still using URLs that inadvertently give investigation access to archived data. Finally, data integrity should be raised to a higher level by implementing replay attack protection and contextual integrity checks. Replay attack protection is implemented by adding a monotonically increasing timestamp to each event record that has an impact on data integrity.

### 4.4.2. Emerging Threats in Tax and Advisory

The tax and advisory landscape has changed remarkably in the last two years due to the ongoing political conflicts, rapidly moving markets, evolving regulatory compliance requirements, and the application of artificial intelligence in the industry. The world of tax and advisory, once dominated by spreadsheets and desktop applications, is on its way to becoming entirely cloud-based in order to provide professionals with more analytical capabilities and the ability to devise complex forecasts. The new generation of tax and advisory tools allows the deployment of cloud-based infrastructure with low data transfer times, storing data in highly reliable and safe cloud environments, and powerful clients that analyze high data volumes and workflows. The tax and advisory industry is

entering a new era where software security and defense systems must be entirely revamped. While the compliance part of data handling is quite mature, protection for another aspect of the majority of tax and advisory datasets, their strategic importance, and the damages evoked from cyber breaches, must be implemented.

Digitization has created new pathways of security breaches with the assistance of artificial intelligence. A scalable and fast solution for evasion of classical security systems is the generation of new threats by different kinds of AI-based Generative Adversarial Networks that can mimic human-like behavior of operating systems or applications and bypass classical defenses by not raising red flags either in intrusion detections or application firewalls. Such a solution could generate threats targeted to the tax and advisory industry and related data and systems of professionals. Furthermore, artificially generated fake data could be injected into the analyzers to produce fraudulent results and illegal analyses that would transfer the pressure for wrongly calculated taxes to the clients. Fraud detection systems that examine statistical properties of the data may not be able to detect artificially-generated noise. The classical approach of tax fraud detection would not work in the presence of an adversary generating statistical alterations. Continuous monitoring, deviation detection, training of ML models on designed adversarial examples, and other advanced techniques may be used to detect tax evasion.

All tax compliance ecosystems are potentially vulnerable, especially the ones with the biggest data handling and analyzing procedures. These organizations should be aware of these vulnerabilities, consider their points of strength in building their infrastructures, and prepare for the different classes of attacks suitable against the tax compliance architecture.

### 4.5. Data Protection Strategies

Tax and advisory firms heavily rely on digital collaboration to deliver services and conduct marketing initiatives. This digitization makes sensitive data visible, and thus, challenging to protect. Incidentally, as bad actors recognize the value of sensitive data contained in firms' digital records, hacked and leaked sensitive information poses a financial risk for firm stakeholders and clients. In turn, the need for operational transparency without compromising information and cybersecurity creates a dilemma for cybersecurity management within financial firms. A cybersecurity first strategy takes a security maturity perspective to identify and mitigate threats against firms' readiness to protect their tax and advisory workflows and ultimately data confidentiality, integrity, and availability (CIA).

Knowing what kind of sensitive data to protect is crucial for taxation and advisory workflows. In the banking system, tax authorities are interested in third parties receiving sensitive financial data to perform fiscal audits and gain insights into the status of the banking system and democracies. Financial crime prosecutions also often rely on tax data. Clients regularly provide firms with sensitive information and data as pure trust. Data disclosure in some firms is much broader than the client, with firm-wide data leakage consequences, such as publicity, regulatory fines, and significant financial loss as victims of supply chain attacks, data sale, or leaks.


**Fig :** From Sensors to Standardized Financial Reports

### 4.5.1. Encryption Techniques

A number of Welfare Department reports on electronic data, classified as exempt disclosure under the Freedom of Information Act, referred to permanent computer geeks in generating the Hackgard W global list. Also on this is the Russian He added recently, in an attempt to make auditors' jobs easier, flexible omission wheels pressed onto a computer disk. An annuity can pay off known debt. Use of these is prohibited by the Department of Education of a State, which allegedly puts undue time pressure on auditors in ensuring accurate bills each employing analysts. There should be a

requirement that, starting July 1, 2025, each computer disk enterable only by analysis be installed on one talking computer in the United States, payable by each separate U. S. , for improper use. The Digital Millennium Copyright Act provides for exclusions under the same clause. However, users in Europe, Canada, and Japan have these on every computer. DCI amateurs have run into this usage earmarked for participants, a situation likely to worsen. To help deter the duplicity possible, H&R Block will route users to tax this. Also of concern are various Justice Department contracts, which apparently call for hardware and software to be supplied which would allow agencies up to four hours to seize any computer and obtain hard and floppy disk data. Something should also be done about other companies' computers e-mailed data and/or the bucks loads of duplicate files still available. Encryption is a highly important initiative for safeguarding, structuring, and striving to remain autonomous via data processing of all types. The replacement of this gauge should have a far-reaching effect over the United States future. Encryption standard refers to a particular cryptosystem widely accepted by the market. Because of the relative youth of public key cryptosystems, demand exists for participants to compromise standards.

### 4.5.2. Access Control Mechanisms

To maintain confidentiality, ensure privacy, and protect sensitive information in Advisory and Tax Services, Cybersecurity teams are enforcing two main Access Control Mechanisms across the firm. These services provide teams with the ability to control access to information through granting or removing individual access. All access requests for information resources will be assessed and approved by the Service Owner, Product Owner, or information custodians. Domain/BU Information Custodians have control over who has access to applications and services. Access review processes should be enforced periodically and at least every six months.

• Services - Review Access Control Mechanism

• User Access Review - An access control mechanism that tracks user access to a resource/service or set of resources. It provides a list of users who have access to information and includes information awareness for reviewing. It lists users and their access level in a monthly report. Optionally, the provision process is automated. System owners will only flag users that are not supposed to have access, meaning the system knows whether or not a user should have access. The current manual process focuses on checking permissions over system owners – no notifications are sent to the reviewers before the review date. Incomplete reviews can take months, increase regulatory risk, and result in non-compliance penalties.

• User Access Request - An access control mechanism that provides a streamlined process for providing data access to users. It provides approval flow/workflows with controls over mitigating risk/ensuring compliance. It includes a short non-technical description of the system/resource for review. The current process is a combination of email-based access request processes + portal landing pages requesting access where teams can either confirm or decline requests. There are no formal approvals for team leads, allowing users to self-approve/de-approve their own requests. mandates identifying systemic owners for all systems/services/resources.

### 4.6. Conclusion

Having access to critical data is a significant advantage in businesses. Nevertheless, the attack surface for potential threats and breaches increased with the move to remote access and hybrid working. Threat actors have become more sophisticated, and thus the responsibility of safeguarding not only the pressure of a company's data but also its clients' data is higher than it has ever been in this new norm. Companies need to promote the efficient use of technology without compromising their security and thus regard information security as paramount in place of capture technologies and digital work relationships. The recent acceleration in legislation and regulation concerning digitalization of society, cybersecurity, and data protection makes this a natural choice.

The financial market sector is under huge pressure, concerning not only Russia and Ukraine but also global inflation and decreased consumer confidence. The use of digital tools is expected to increase further. Pressure from legislation and regulation will increase in parallel, and thus security measures and compliance levels must be increased. Still, measures based only on compliance will never be fully sufficient. Companies need to make a paradigm shift in their data protection and security philosophies, going beyond compliance. Technological capabilities will need to be changed to keep pace with a rapidly evolving information security landscape.

Global attacks have confirmed that this is needed. The business model needs to change, moving from a protection-first to a security-first model, with anything process-relevant requiring a risk assessment before its use. In daily operations, confidentiality, integrity, and availability must be treated symbiotically with a clear emphasis on security and only security. Training and career paths of employees in charge of security should change from being technology-driven to employee-driven and exposure-driven, empowering them to protect the company better.

### 4.6.1. Emerging Technologies

As many countries are emerging from extended lockdowns due to COVID-19, taxes are becoming increasingly complex. Countries are tightening their taxes on foreign investments, while the global supply chain nature is leading to both great opportunities and great risks. To deal with the growing complexity, firms need to increase the talent pool and knowledge base. This exhaustively also increases the acquisition and usage of data in advisory firms. On the other side, though, a rapidly evolving cyber threat landscape with growing numbers of data breaches, ransomware attacks, and leakages or stolen data leaks is calling for in-depth protection of these data, including personal data, commercial data, client IP, etc. Client location service, basis of assessment service, mapping service, and client IP queries have all become essential for the advisory firms to do their business and to generate revenue. Though the advisory firms collect such data for other purposes, appropriately managing both the commercial and personal data is of vital importance.

This section contains five different groups of innovations needed for obtaining a maximal protection on one hand, and still to provide, develop, and maintain unthreatened advisory and tax related services, as provided today by the advisory firms, on the other hand. A world where one could be sure about privacy can be created with a set of several independent inventions and developments, which are the tip of products with interconnected subsystems. Fundamental awareness technologies are needed at the client side, at the domain manager side of the specialty firm, and beyond these. Second, on a fundamental level, the education of advisory firms regarding cyber security and their obligations should be enhanced, including the tax and advisory software developers. These are the preconditions for further innovations.

Third, the advised firm's data processes should be realistically separated from the advisory industry in terms of firms fully deliverable under privacy assured constraints. This is of strict and extreme privacy assuring importance. The developmental and on-board capabilities of data stars should be considered profound. Fourth, blockchain inspired architectures should be developed for creating intuitive, privacy enhancing protocols for convinced, verified, classified, and only then aggregated analyses to provide intuitive data visibility at the end user. Finally, encryption, anonymization technologies should advance on architecturally designing confidentiality from the start barrier. More than big data does else, this endows the client with trust abilities over the data analytics firm's process and output.

## References


Aladebumoye, T. (2025). *Integrating AI-Driven Tax Technology into Business Strategy*. International Journal of Research and Review, 12(1), 224–231.

Gounagias, N. D., Hristu-Varsakelis, D., & Assael, Y. M. (2018). *Using Deep Q-Learning to Understand the Tax Evasion Behavior of Risk-Averse Firms*. arXiv.

Savić, M., Atanasijević, J., Jakovetić, D., & Krejić, N. (2021). *Tax Evasion Risk Management Using a Hybrid Unsupervised Outlier Detection Method*. arXiv.

Zhang, Z., Al Hamadi, H., Damiani, E., Yeun, C. Y., & Taher, F. (2022). *Explainable Artificial Intelligence Applications in Cyber Security: State-of-the-Art in Research*. arXiv.

Zheng, X., Zhu, M., Li, Q., Chen, C., & Tan, Y. (2018). *FinBrain: When Finance Meets AI 2.0*. arXiv.