The Attorney's Role in Cyber Security Compliance

Alejandro VILLEGAS
Seattle University School of Law
Seattle, WA, 98122, USA
villega3@seattleu.edu

ABSTRACT

Cyber Security has become a predominant challenge for organizations responsible for protecting and safeguarding customer data. Attorneys serve a critical function ensuring that companies adhere to the cyber security requirements mandated by local, national, international and industry information security frameworks. The purpose of this article is to provide an overview of the attorney's role in cyber security compliance; emphasizing the focus areas where legal counsel serves an imperative part. Attorneys can reference this journal paper to better understand how to perform cyber security compliance due diligence for their clients. While cyber security attacks continue to evolve into sophisticated threats, the attorneys must zealously advice their clients to prevent inadvertent negligent behavior regarding cyber security compliance which could cause long term adverse repercussions.

Keywords: Attorney, Audit, Cloud Service Providers, Compliance, Counsel, Cyber Security, Information Security.

1. INTRODUCTION

Cloud Service Providers[1] (CSPs) provide software and storage services to their customers available for access via the Internet. CSPs generally offer three types of cloud computing services: Infrastructure as a Service (IaaS), Software as a Service (SaaS) and Platform as a Service (PaaS). CSPs that store customer information are under compliance and legislative scrutiny to provide adequate cyber security controls in order to facilitate effective safeguard measures.

The goal of cyber security compliance is to enforce a baseline framework that aims to protect nonpublic customer information. Cyber security compliance is supported by a plethora of frameworks at both the federal and international levels. Furthermore, there are also industry specific compliance frameworks available. CSPs frequently have to determine which compliance certifications are applicable to their business model and that satisfy customer demands.

Attorneys must be well versed in compliance certifications to efficiently advise their clients. Pursuing a compliance certification requires substantial financial and operational resources, therefore it is imperative that the decision to pursue a given certification is well thought out. In addition, compliance certifications require continuous monitoring and surveillance to maintain the certification; the obligations do not end once a certificate is granted. Attorneys must be able to advise their clients during the entire compliance lifecycle. Depending on the size of the organization, attorneys might be able to partner with the cyber security compliance department; however, some Small and Medium Businesses (SMBs) seldom have formal compliance teams and entrust their legal department to assist them pursing and managing compliance certifications.

Cyber Security compliance requirements also expand beyond certifications; governments often define legal requirements around the security controls that protect customer nonpublic information.

National Cyber Security Compliance

The United States Government is well involved in the regulation of CSPs from a cyber security compliance perspective. The overarching legislative and regulatory effort to safeguard government information is The Federal Information Security Management Act (FISMA):

"The Federal Information Security Management Act[2] (FISMA) is United States legislation that defines a comprehensive framework to protect government information, operations and assets against natural or man-made threats. FISMA was signed into law part of the Electronic Government Act of 2002[3]"

FISMA relies on The Federal Risk and Authorization Management Program[4] (FedRAMP) to manage and oversee its operational enforcement. FedRAMP is the federal compliance framework that ensures CSPs meet the necessary controls to protect government's information stored in the cloud. FedRAMP leverages the National Institute of Standards and Technology (NIST 800-53 Revision 4[5]) to evaluate CSPs security controls. Albeit NIST is used by FedRAMP, it is also leveraged by CSPs to define their overall cybersecurity compliance baseline that encompasses protection of customer data not limited to government data.

The FBI also has an interest on protecting Criminal Justice Information (CJI). The FBI created the Criminal Justice Information Services[6] (CJIS). CJIS is used to monitor CSPs' cyber security controls where Criminal Justice Information is stored. The policy that describes the cyber

[1] Definition of a Cloud Service Provider: http://www.webopedia.com/TERM/C/cloud_provider.html
[2] FISMA: http://csrc.nist.gov/groups/SMA/fisma/index.html
[3] Electronic Government Act of 2002: http://www.gpo.gov/fdsys/pkg/PLAW-107publ347/pdf/PLAW-107publ347.pdf
[4] FedRAMP: https://www.fedramp.gov/
[5] NIST 800-53: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf
[6] CJIS: https://www.fbi.gov/about-us/cjis/cjis-security-policy-resource-center/view

security controls is CJIS Security Policy version 5.4[7]. NIST cyber security controls are also referenced in the CJIS Security Policy.

"While the NIST Framework is voluntary and principally directed at critical infrastructure, security experts expect it to be widely implemented and to provide a standard of care of sorts with respect to cybersecurity. Accordingly, companies should refer to the NIST Framework when developing or assessing their security programs" [3][4].

International Cyber Security Compliance

Cyber Security compliance is a global matter that affects any nation or organization involved in any online transaction that utilizes a cloud software component. Therefore, it is vital that entities can rely on international cyber security compliance certifications that simplify contractual agreements. One of the most common cyber security compliance frameworks used at the international level is ISO *27001:2013 Information Security Management*[8]. CSPs widely use ISO 27001 on contractual agreements, parties will typically seek mutual compliance with ISO 27001 within the cyber security compliance provisions.

Certain nations and regions have unique compliance requirements that must be met regardless of ISO 27001 compliance. For example, the European Union Model Clauses (EUMC[9]) that oversee the protection of European Community members' customer data.

A plethora of different countries have their peculiar cyber security requirements; some provide the ability to comply with specific compliance certifications while others dictate the obligations via legislation. For instance, Argentina has its own Personal Data Protection Act[10].

List of countries that require certifications (not an exhaustive list):

- G-Cloud[11]: UK Government Security Standard.
- MTCS[12]: Multi-Tier Cloud Security (MTCS) Singapore Standard.
- IRAP[13]: Australia InfoSec Registered Assessors Program.

Industry Cyber Security Compliance

Highly regulated industries such as the Health Industry and the Payment Card Industry have narrowly tailored compliance frameworks that articulate more stringent cyber security requirements applicable to their business models.

Examples of Industry based Cyber Security compliance requirements:

- HIPPA[14]: Health Insurance Portability and Accountability Act.
- PCI DSS[15]: Payment Card Industry Data Security Standard.

While this cyber security compliance summary intends to provide a high level overview of the compliance certifications and obligations available, it is important to reiterate that this document does not contain a comprehensive list of every compliance framework available from a national, international or industry perspective. Attorneys must work closely with their clients to identify what compliance certifications and laws are applicable to their business operations and jurisdictions where they conduct business.

2. ATTORNEY ADVISORY ROLE

"Cyber-attacks and the resulting security breaches are part of a rapidly expanding international cyber threat that costs companies and taxpayers billions of dollars each year in lost information and response costs. Company executives are under increasing pressure to prevent these attacks and must act immediately to contain any damage once an attack occurs. Counsel's advice can be critical in guiding companies to develop legally compliant response plans to prevent and respond to cyber-attacks and identify the civil and criminal actions their clients can pursue against cyber attackers" [1].

Chief Compliance Officers (CCOs) are responsible for: deterring cyber-attacks, containing any attacks and minimizing any financial or reputational harm [1]. Attorneys can play a crucial role assisting companies and stakeholders to prevent and remedy cybersecurity breaches by complying with cyber security compliance and related legal requirements [1].

Given the plethora of available cyber security compliance frameworks, it is imperative that attorneys are able to provide zealous guidance regarding what compliance certifications and obligations to comply with. CSPs must be cautious when deciding what compliance frameworks to pursue in order to achieve their goals and meet the customers' expectations. Deciding to pursue a compliance certification should not be taken lightly as it might require several engineering and operational investments.

Attorneys must be able to articulate the rationale to justify pursuing or passing on a particular certification. Business leaders make decisions based on risk, lawyers must adhere to such approach and present the legal risks on a manner that is easily digested by senior leadership. An attorney should be able to advise the client whether is it feasible or suggested to pursue a certification from a recommendation angle. The role of the attorney is not to provide the definitive answer, but to ensure that client is making an educated decision with all the elements and factors necessary to make a sustainable choice.

[7] CJIS Policy: https://www.fbi.gov/about-us/cjis/cjis-security-policy-resource-center
[8] ISO 27001: http://www.iso.org/iso/home/standards/management-standards/iso27001.htm
[9] EUMC: http://ec.europa.eu/justice/data-protection/international-transfers/transfer/index_en.htm
[10] Argentina Personal Data Protection Act: http://www.protecciondedatos.com.ar/law25326.htm
[11] UK G-Cloud: https://www.digitalmarketplace.service.gov.uk/
[12] MTCS: https://www.ida.gov.sg/Tech-Scene-News/ICT-Standards-and-Framework/MTCS-Certification-Scheme
[13] IRAP: http://www.asd.gov.au/infosec/irap.htm
[14] HIPPA: http://www.hippa.com/
[15] PCI DSS: https://www.pcisecuritystandards.org/security_standards/

Furthermore, the attorney's role goes beyond obtaining a compliance certification. The goal is to envision the compliance obligations end to end inclusive of the preparatory phase, compliance phase and continuous monitoring phase. Additionally, determine what contractual obligations are at risk, and how does the compliance certification ties into the contract provisions. For example, what would be the implication of deciding to incorporate a provision that requires the client to meet a high scrutiny level of compliance requirements and any minor non-compliant incident might cause the client to be on breach of contract. Henceforth, it is worth taking the time to diligently analyze holistically what the implications are of pursuing and maintaining a compliance certification or regulation. Generating a matrix that outlines the risk and decision factors customized for each client's needs could be a useful tool. Determinative elements should be included such as cost, breach of contract implications, potential penalties, or opportunity costs.

The advice provided to the client should be able to address the fundamentals questions with a compliance lens: Who? What?, When?, Where?, Why?, and How? The advice must be dynamic in nature and adapt to the disruptive and evolving compliance world. The portfolio of compliance certifications and obligations must be revised periodically to validate that it is appropriately addressing the customers' needs. An attorney should consider asking the following questions: Is it worth maintaining certification A?, Would it make sense to stop renewing certification B?, Should certification C supersede certification A?, Could I use certification D in lieu of A and B? In a nutshell, the goal is to be able to clearly understand the portfolio of certifications from a Return of Investment (ROI) and legal risk perspective.

Attorneys can also assist the client with the following cyber security compliance related tasks as stated by PLC [1]:

- *Developing a cyber incident response plan.*
- *Planning and implementing cyber-attack recovery, mitigation and remediation.*
- *Considering and preparing post-attack public disclosures and announcements and handling public relations.*
- *Reporting cybercrimes.*
- *Cooperating in law enforcement investigations.*
- *Pursuing civil and criminal remedies.*
- *Obtaining appropriate cyber liability insurance coverage.*

Attorneys should also be able to address cyber-attack scenarios from a preventive, responsive, and mitigation perspective in order to comply with legal and regulatory cybersecurity requirements [1].

3. ATTORNEY COMPLIANCE ROLE

"Recognizing the need to ensure that privacy and data security protections remain effective as data collection capabilities evolve, lawmakers in the US and abroad have been active on both the regulatory and enforcement fronts. This trend is likely to continue as technology and consumer behavior combine to enable the collection and analysis of increasing amounts of detailed information about individuals. Companies must understand how the dynamic legal framework governing this area applies to their businesses and ensure their policies and procedures are compliant" [2].

Complying with cyber security compliance controls is a constant responsibility. Majority of the compliance certifications require continuous monitoring strategies and yearly surveillance audits. Attorneys need to have an ongoing and frequent communication with their clients to determine where they stand from a compliance perspective at any given time: real time compliance monitoring.

Compliance frameworks usually have controls that provide guidance on how a cyber security risk should be managed or mitigated. CSPs are responsible for translating the control guidance into an operational control that meets the spirit of the compliance control to mitigate the risk defined on the control language. Attorneys must take the time to understand how the CSP engineering groups are incorporating the compliance requirements into their operational business processes. Attorneys should feel comfortable with the compliance strategy and tactical approach that goes beyond the client stating that the compliance requirements are met. Proactively working with the engineering groups and dissecting their processes to better understand the implementation of the cyber security controls can have great payoffs in the long term. Attorneys that have an end to end understanding of how compliance is managed by the business and engineering groups have the ability to provide better cyber security compliance advice by becoming knowledgeable and well informed of the granular specificity involved in meeting the compliance requirements.

Compliance with cyber security controls is a combined effort that involves several departments, groups and teams within an organization. The attorney has the ability to view cyber security compliance from a holistic view and provide advice that is unbiased and originated from a neutral position by analyzing compliance across the organization.

Compliance needs to be monitored frequently and each compliance control might have a different cadence based on risk. Controls are generally monitored on a monthly, quarterly, or yearly basis. While the attorney might not necessarily have the bandwidth to closely work with the engineering teams to monitor each control, it would be wise to get visibility on the overall compliance status on a monthly or quarterly basis to understand where the company stands. If a cyber security control is not being met, the attorney should be able to investigate the potential legal repercussions and be able to vet that the proposed control improvements are adequate to mitigate the cyber security risk and compliance with the corresponding requirements.

Certain cyber security controls might require high scrutiny, for instance if a breach occurs, the client might be in obligation to notify the customers either because of a contractual obligation or a compliance requirement. Attorneys that are proactively monitoring compliance can

create value by either preventing litigation or lessening the risk of litigation by addressing non-compliance on a prompt and reasonable manner.

4. ATTORNEY DRAFTING ROLE

Attorneys have grown accustomed to draft and review contracts for their clients. Attorneys representing CSPs have seen an increase of cyber security provisions and addendums when dealing with contractual obligations. It is vital that attorneys become comfortable with the technological intricacies of cyber security controls. Attorneys need to make sure that their client's interests are well protected from a cyber security perspective. Conversely, attorneys need to make sure that their client can comply with the cyber security provisions prior to agreeing to sign a contract, clause or addendum.

Whether the attorney is revising a new cyber security provision, drafting a new addendum, or redlining an existing contract; it is vital that the attorney understands the technical details included on the language. If the attorney is not well versed in technology, is best to seek advice from a cyber security expert within the organization if feasible. The core advice should be from a legal perspective, however understanding the underlying technologies and intricacies can be critical. The attorney should be comfortable explaining the risks to the client inclusive of the technological and operational requirements at least at a high level.

Attorneys must be extremely careful when referring to compliance frameworks within contractual agreements. Agreeing to comply with ISO 27001:2013 might or might not be feasible for the client. If a compliance certification is going to be used explicitly on the contract, ensuring that the client is comfortable and capable of meeting the requirements is preponderant. If the attorney has been proactively involved monitoring compliance, she might be able to comfortably assess whether the client would be most likely able to comply with the requirements.

Like in any other contractual due diligence, language is key, attorneys shall revise the obligations to better understand whether the client must comply with all cyber security controls or a subset of controls for a specific compliance certification. Also, whether the client must have controls in place, must provide the certificate, or what specifically is the client agreeing to comply with. Another important aspect is the implications of not meeting the requirement, is the client comfortable with the consequences for non-compliance.

Attorneys must also advice the client regarding other provisions that might have an association with the cyber security compliance provisions. For instance, whether the warranty and indemnification provisions are reasonable regarding the potential cyber security implications. The attorney can also advise if cyber security insurance might be a viable risk mitigation.

"Coverage for data breach-related expenses under traditional commercial insurance policies has become increasingly uncertain. Cyber insurance addresses gaps in coverage that may arise under traditional commercial policies. Their primary purpose is to protect against data loss and exposure of personally identifiable information (PII)" [5].

The best way to analyze a cyber security provision, clause or addendum is to understand the language and how it is tied into the rest of the contract. Attention to detail is crucial to avoid overlooking implied or intertwined obligations. Due diligence is imperative: 1) Are other provisions or sections of the contract making references to the cyber security addendum? 2) Do other provisions include cyber security language or obligations? 3) Do the cyber security controls address the risk adequately? 4) Are both parties equally agreeing to manage the cyber security risks? 5) Is the language properly addressing the cyber security risks?; Is it best to use broad language? Is staying silent on a specific provision the best approach?

5. ATTORNEY AUDIT ROLE

The right to audit clause has become very popular in cyber security contract provisions and addendums. The right to audit gives a customer or business partner the ability to audit the CSP at least once a year. The party executing the right to audit can opt for conducting the audit or hire a third party audit company. The frequency and scope of the audit are items that need to be carefully reviewed when drafting, revising or redlining a contractual cyber security obligation.

Attorneys must become familiarized with the logistics of the audit. The attorney should be able to engage and oversee the pre-audit preparation, participate doing the audit on a supervising capacity if applicable, and lastly, work with the CSP to review and mitigate any potential findings discovered during the audit. The attorney must be aware at all times of the potential consequences correlated to executing an audit. Certain CSPs might conduct internal audits or assessments to monitor the overall cyber security compliance, other CSPs might not have a robust internal assessment program. Therefore, it becomes vital that the attorney understands the risks of executing an audit. Additionally, CSPs engage with a myriad of different customers, it is relevant to envision and limit the amount of audits that can be conducted. Some CSPs might have a specific timeframe where they prefer to conduct audits, perhaps during non-peak hours or season. The contract language should account for potential scenarios when multiple customers might want to audit the CSP. The attorney must look beyond one contract and understand the holistic obligations across all contracts, agreements and any other cyber security contractual obligations.

Another important consideration relates to funding the audit. Attorneys must advice the client on whether it is reasonable to fund the audit or shift that responsibility to the customer requesting the audit. Also, decide whether the audit execution should be restricted to the customer or to a third party audit company.

Right to audit could be triggered based on the what the contract stipulates. However, there might be other triggers such as a security breach. The attorney needs to envision caveats related to special triggers. A CSP might have

several concerns to address when there is a breach, having to deal with audits might not be necessarily wise during such critical times. The attorney must try to anticipate such circumstances and tailor the contract to address that type of concerns. Perhaps, the CSP can agree to notify the customers under certain reasonable agreeable terms but delay the audit until timing is more feasible.

6. ATTORNEY LITIGATION ROLE

"Most companies understand the consequences of security breaches. But how well do they recognize their potential security gaps that could lead to breaches?" [3][4].

"The FTC is the primary federal regulator of consumer privacy and data security" [5].

Attorneys must become proficient with the NIST framework as the Federal Trade Commission (FTC) and other government entities leverage it to assess whether a CSP was compliant with the cyber security controls framework. Generally speaking, CSPs that were attacked and subsequently a victim of a clever malicious attacker using sophisticated techniques are not subject to penalties and punitive damages. However, if a CSP is found to be negligent with the NIST standards and cyber security controls in general, there is a likely possibility that a court would fine the company.

While it would be ideal to live in a cyber security world where following all the recommended controls to protect customer information will guarantee no security breaches; reality is that any CSP might be faced with an advanced or clever attack that will bypass and circumvent the applicable security controls in place. The goal of cyber security compliance is not necessarily to prevent every single attack, the objective is to define a set of cyber security controls that can provide a robust framework and assurance that the CSP has adequate protections to mitigate the risks. Malicious attackers are also investing time and effort developing new clever ways on how to reverse engineering technologies and find security vulnerabilities. The paramount FTC cases rarely seem to penalize CSPs for advanced malicious security breaches. The FTC rulings seem to analyze whether a CSP was providing an adequate cyber security compliance framework. If the CSP was knowingly or negligently not meeting the compliance requirements, that could be an area of concern. Attorneys must be able to monitor compliance in conjunction with the business to avoid negligent scenarios if possible.

Paramount Cyber Security Cases

- SONY: *Sony Gaming Networks & Customer Data Sec. Breach Litig*., 996 F.Supp.2d 942, 962 (S.D.Cal.2014)
- TJMAXX: *TJX Co. Retail Sec. Breach Litig*., 524 F. Supp. 2d 83 (D. Mass. 2007)
- TARGET: *Target Corp. Customer Data Sec. Breach Litig*., 66 F.Supp.3d 1154, 1177–78 (D.Minn.2014)

Ultimately, the question that must be answered is whether the CSP was diligent regarding the implementation and monitoring of cyber security controls. The attorney should keep that in mind throughout the entire compliance lifecycle inclusive of all phases. Even though an attorney might not be a cyber security expert, becoming well versed or relying on Subject Matter Experts (SMEs) is highly recommended. Attorneys should not try to understand how a cyber security control is performed at the last minute in preparation for litigation.

7. CONCLUSION

There is no doubt that attorneys' serve an instrumental role regarding cyber security compliance. Clients rely on their lawyers to provide legal advice that helps them manage cyber security risks. Attorneys not only have an opportunity to provide cyber security compliance advice but also a responsibility to participate in all aspects of compliance from an end to end perspective. Lawyers should not limit their contribution to the drafting of contractual agreements around cyber security compliance. Becoming proactively involved with all phases it is not a recommendation but a necessity.

Attorneys must work closely with their clients throughout the cyber security compliance lifecycle: 1) before pursuing cyber security compliance; 2) when pursuing cyber security compliance; 3) maintaining cyber security compliance; 4) drafting contractual language that involves cyber security compliance, and 5) during litigation related to cyber security compliance.

Attorneys may serve different roles such as inside counsel, outside counsel or transactional. The relationship with the client could be short or long term. Attorneys might be on the plaintiff or defendant side. Regardless of the specific role and position of the attorney, it is equally important to become familiar with cyber security compliance in depth from an end to end perspective; in order to better serve the client throughout the entire cyber security compliance lifecycle. Attorneys must confirm that the guidance provided aligns with NIST, ISO and any other applicable standards. Additionally, it is essential that lawyers partner with the cyber security leaders in the organization to evangelize security policies via training inclusive but not limited to using complex passwords, prevent phishing attacks, and mobile security best practices.

8. REFERENCES

[1] PLC Intellectual Property & Technology (2013). "Advising Clients on Cybersecurity". Retrieved from http://www.westlaw.com (Practical Law)

[2] Neuburger, J., Mollod J.P., et al., (2014). "Trends in Privacy and Data Security". Retrieved from http://www.westlaw.com (Practical Law)

[3] Rosenfeld, D.B., Zeltzer Hutnik, A., Drye, K. et al. (2014). "Security Contract Clauses for Service Provider Arrangements (Pro-customer)". Retrieved from http://www.westlaw.com (Practical Law)

[4] Rosenfeld, D.B., Zeltzer Hutnik, A., Drye, K. et al. (2014). "Common Gaps in Information Security Compliance Checklist". Retrieved from http://www.westlaw.com (Practical Law)

[5] Selby, J., Rosenberg, C.Z., "Cyber Insurance: Insuring for Data Breach Risk". Retrieved from http://www.westlaw.com (Practical Law)