Augmentation of SECaaS model with eCISO in cloud-based security services: A Comprehensive study

Siddharth Saxena and T N Nisha*  
Symbiosis Centre for Information Technology  
Symbiosis International (Deemed University), Pune, Maharashtra, India  
Email: nisha@scit.edu8*

Abstract. In today’s competitive world and the time of business discontinuity and falling economies due to many reasons, enterprises worldwide are trying to process business data securely and minimize IT systems’ operational cost with technologies in cloud computing. With the benefit of cost-efficiency in cloud services, there are some concerns regarding IT security, IT governance, and compliance, which plays a vital role in the business as usual. Security as a service model is a cloud-based security service model to provide secure environments, mediums, and systems to enterprises. In this paper, we are attempting to introduce a new service model to cloud-based security platform and perform a comprehensive study with augmenting security as a service (SECaaS) model with eCISO services for better governance of risks and decision making related to IT security to optimize the service model to help out CEOs and CIOs to ensure the security of their IT systems and data.

Keywords: Security as a service, SECaaS, eCSIO, Cloud computing, compliance, controls, security resilient.

1. Introduction
From MNCs to SMEs and startups, Cloud computing from the past two decades played a critical role in the growth of businesses across the globe, outsourcing information systems and support to store, control, and to operate the business data on a remotely located place, not only provided a huge reduction in operational cost but also optimized the old-fashioned business systems [1]Since its inception; it has given astonishing results in, how global to local business compute the data for providing and creating products and services in the market [2]. The security of Internet-accessible digital services always has been a cross-cutting, non-functional necessity of the utmost prominence. In recent times of development of the Cloud Computing model and its prevalent have given the lead to unaware challenges in securing existing Cloud-based services, with due account being taken of problems related to their models of delivery and their consumption patterns, and has initiated the road to the brand new conceptualization of SECaaS (Security as a service)[3].

Security as a service model is a cloud-based security service model to provide secure environments, mediums, and systems to enterprises. SECaaS (Security as a service) is essentially a business model in which companies can procure on-demand security solutions to protect their data, systems, and applications while benefitting from what cloud storage provides m[4]. IT discusses the evolution of the SECaaS model from conventional on-premise and controlled security approaches and assesses opposing and supporting hypotheses for cloud-adopted security services to provide a secure
environment. Cloud computing providers incorporate several SECaaS components that constitute cloud computing security measures [5]. The right provider of SECaaS will help the company solve vulnerabilities without wasting its own IT resources and without charging an exorbitant amount for a server-based solution. Most would align their services with the customer’s existing infrastructure. Others will also operate in hybrid environments if a combination of cloud and technology is to be used. A CISO (Chief Information Security Officer) is an executive officer solely responsible for managing and governing the information security-related issues and decision making while maintaining the vision, strategy, and need of fundamentals of an enterprise. With the current scenario, the importance of CISO has been increased significantly because nowadays, even one serious security issue can crash the growth rate and profitability of the business and cause huge losses and reputation [6]. The current scenario has seen CISO are amongst the most critical jobs and play an important role in Business Continuity Planning and being cyber resilient. Chief Information Security Officer (CISO) usually reports to the CIO or CTO responsible for looking after its technology horizontally [7].

But from the past 5-6 years, CISOs have been promoted to the board of directors and C-suite meetings with CIO or CTO to plan and execute C-suite meeting agendas and help in the business’s growth. CISOs help businesses plan and execute IT security strategies and lead physical business securities with CSOs[8]. Research and development, learning programs, and technology introduction to the existing system for security. But to onboard an expert and experienced professional to the company could be financial and administratively perturbing for a HR head of the company who is not investing much in a project or have low budget deliveries or being a startup they do not have money to found and hire a person with that level of knowledge and skill[9]. In this paper, we will talk about some of the issues in the SECaaS model and how SECaaS providers can overcome that with the addition of eCISO services.

2. Literature Review

SECaaS (Security as a service). is a modern framework developed to address the various security aspects of a cloud system’s genres and models? The Cloud Security Alliance (CSA) is a non-profit organization, works in this area to advocate the use of best practices to provide security assurance within Cloud Computing (CC), as well as to provide knowledge on Cloud Computing(CC) applications to benefit all other types of computing [10][11]. According to Cloud Security Alliance(CSA), the formulation of the concept of SECaaS (Security as a service) leads to providing applications of data security and information security services through the cloud to either cloud-based infrastructure or software as well as from the cloud to customers. The Cloud Security Alliance, also known as CSA, is an organization focused on allowing enterprises and researchers to understand the concept of security prompted cloud computing and raise awareness programs to encourage secured cloud computing.

Further in detail, CSA also defined the major categories of SECaaS resources. It also developed a collection of implementation procedures and technical properties and guidance to help enterprises integrate and evolve an understanding of SECaaS as a model concept [12]. These categories include:

- Security information and event management (SIEM)
- Web security
- DR (Recovery from disaster incidents)
- BCMS (Management system for Continuity of business)
- Continuous monitoring
- Cloud auditing
- Cloud governance and compliance
- Data loss prevention (DLP)
- Security assessment
- Network security
- Email security
Encryption
Identity and access management (IAM)
Intrusion management
Vulnerability scanning

[1] In a book, the authors proclaim the existence of the SECaaS (Security as a service). This gives the basic overview of why SECaaS (Security as a service) has been established and why it is needed due to its vital role in the CSP and Cloud users[13]. The author defines security as a Service (SECaaS) as a business model in which companies can procure and deploy on-demand security solutions to protect their data users and peripherals, end-user and CSP applications, and systems cloud computing. This chapter takes us on the journey of on-premises security solutions to the SECaaS (Security as a service). It covers governance and compliance issues, privacy considerations, interoperability, and technical and legal aspects, with the move from in-house processing to a CSP, i.e., it contributes to better trust and commitment to the CSP consideration security challenges that emerge through this conversion [14]. In a paper [2] published in 2019, describe security as a Service (SECaaS) as a framework to help security managers securely adopt cloud computing securely in their enterprise by considering and measuring various risk involved in moving to the cloud, they also concluded the various model of SECaaS (Security as a service) which can be taken into consideration while preparing the bouquets of security as a Service (SECaaS) services to the user. This paper also came up with benefits of cloud computing which establish this framework for easy adaptability, Cost-Cutting, Faster action planning, outsourcing of complex security tasks, Continuous compliance maintenance, as well as some of the core security benefits specialized 1 Tier service providers for Uniform and consistence protection, Auto updates of AVs, Pro-active approach on certificate expiration and virus definitions, Optimal Monitoring and Faster user provisioning [15]. This paper concludes why Security as a Service will be the most important framework to work horizontally with all the other different Cloud computing models. In a different paper [3]. The research paper starts with a holistic approach towards finding the various possible models of SECaaS. It also measures the security quotient required in different models of SECaaS according to the enterprise's demand and scale. It concludes in a way that SECaaS (Security as a service) is more beneficial for small and medium enterprises while migrating to the cloud and establishing a digital roadmap for their services at a very low price and with no on-premises security services from Antivirus to identity management or secured gateways to their system in the cloud. Whereas when it comes to Multinational big enterprises, the model can help them for proactive monitoring of huge mainframe systems and data centers with cost-cutting.

The scalability characteristic of cloud-related services, including the SECaaS (Security as a service), can help enterprises go for project-based subscriptions according to the models of SECaaS (Security as a service).

[4] While in another paper, the study has shown that even with continuously improving SECaaS (Security as a Service) model, Cloud computing is one of the most attractive fields of current day's technology due to its cost-effectiveness and versatility. Cloud computing is a major change in how computing is shifted to a 'stack' of computers from computers used for personnel work and even the individual business server for its applications. But cloud computing, together with its myriad powerful promises for storage, brings another layer of security problems that must be addressed before adopting the full potential model. The acceptance and growth of cloud computing are influenced by unresolved security issues that impact both cloud providers and cloud users alike. Inherently, cloud clusters are more vulnerable to cyber-attacks than conventional solutions, considering their scale and associated service-related ambiguity — which allows immense visibility of services and interfaces to third-party companies. Before a company or any other person migrates to the cloud, they must ensure that standard safety enforcement standards are properly followed. The secret to the cloud transformation is to protect confidential data and systems and provide access to those systems' protection.

[5] The founder &Chief Executive Officer of eCISO.io, cybersecurity services and consultancy company that offers electronic CISO services and management consultancy to startups and provide an
effective method to solve most cybersecurity problems. Professionals are deluged by alert, exhaustion & shifting priorities also with confusing signals and incoherent business support. To be more efficient, they don't need more tools – they need processes that function in their business context and relationships which allow those processes to be effective, and then tools can be aligned towards the common goal of C'suite and Subject matter experts, Mr. Kohrman in conversation with Security website. Security vendors should make an investment in client-driven projects and collaborate with them to make the protected environment they need and make it with better availability and less complexity for themselves to handle it. The ability to communicate risk without invoking fear, uncertainty, and doubt is a technique he's seen with tremendous success some vendors wield. It's awesome how impactful you can be for us when you're transparent, frank, and practical about your expectations and what we can do together. This method includes dedication and a commitment to prepare one's target audience, but the payoff is worth it: by establishing a business group that has learned how to handle the risks of their business efficiently, more consumers would, of course, trust those vendors with their business.

3. Proposed Methodology

3.1 Need of augmenting SECaaS model with eCISO/vCSIO Services
Before introducing this new model of augmented security, let's take a tour of the cause of this development. One of the world's top analysis firms, Gartner's report, predicted in 2017 that security as a Service (SECaaS) technology could be a boom to the IT industry with its win-win deal with IT firms and related enterprises. According to their sources, they forecast that perhaps the growth of cloud-based security services worldwide will remain high. The market for worldwide cloud-based security services was USD $5800 Million in 2017, and it is predicted to be $9000 Million USD by the end of 2020. This shows that worldwide cloud-based security services provide frameworks that are beneficial for users and CSPs and their peripherals. Email security, identity and access management, and web security remain organizations' top-3 cloud priorities, said the R&D director at Gartner [13]. Mainstream services like identity and access management (IAM) and Security information and event management (SIEM) will always be the priority of enterprises. They will grow in accordance with the cloud migration of IT giants and will show subsequent growth in the coming years till 2020. The SECaaS platform based on the CSP provides a different level of security and security solutions and monitoring system. In an enterprise where cloud has been indulged in business as usual (BAU) tasks, the security level is required for security in-depth and no-compromise policy in terms of business application deployed on the cloud through various DevOps tools and served through ITIL practices, in compliance of the regularity standards and bodies for avoiding discontinuity in business and services. Achieving the highest and latest security level and patching in the system is a continuous process for businesses and CSPs providing service on a 24/7 X 365 basis.

3.2 Components of Security as a Service Model
i) Security access management:
Access management is a major part of SECaaS modules as multiple parties are involved in a contemporary IT system. Securing IAM takes out the major part of the complexity and operations of a business.

ii) Business Continuity Planning:
In a tough time like CoVID, businesses worldwide struggle for business continuity, whereas the IT companies are not much impacted due to a proper Business continuity management system.

iii) Disaster Recovery:
Disaster recovery is a set of critical activities, which are performed after a disaster impact on business. To recover the business to its existing shape again.

iv) Centralized security of web APIs:
A central body is responsible for security in web APIs to neglect the system from outsider listeners and monitors.
v) **Real-Time Monitoring System:**
The real-time monitoring system is the control system of the SECaaS model. Where monitoring is done with real-time highly computable data through cloud services, building an in-house system with such computation power can be highly expensive.

vi) **DE for MIS and security events:**
A decision engine is used to provide decisive data to take action and provide high-rated MIS reports and events happening in the system.

Security information and event management:
Security information and event management systems are tools and services that give the accessibility to have real-time information of security events and IS.

vii) **Antivirus**:
SECaaS provides antivirus systems to secure the system, network, and peripherals from malicious files and injections.

viii) **Network security**:
Network security is one of the major concerns of businesses working with IT, where the network is highly vulnerable.

Figure 1 shows the Common services of the SECaaS platform and its features. It is quietly around seven features mentioned below.

![Figure 1: Common services of SECaaS platform](image)

3.3 **Challenges in the SECaaS model**
However, the developing and demanding SECaaS model still needs to be focused on some of the out-of-scope security measures lost by SECaaS customers. In a market with a player like Amazon Web services, Azure cloud, and Google cloud security services, issues related to compliance, governance, executing regulatory programs are still not solved. Below are some of the major challenges in the SECaaS model:

- **Data loss**:
  Loss, unethical monitoring, using, or change of critical nor sensitive data and business data due to manual activities or archiving.
• *Regulatory compliance violations:* 
  Violation of state compliance under which business is used to be run can impact business closure and loss of trust in case it's compromised. For example, ISO standards compliance for business clients, HIPPA, PCI DSS, and GDPR.

• *Compromised credentials:* 
  Disclosure or impact on the integrity of critical know credentials to use business application and data. On-compliant or avoidance of security guidelines leads to this type of attack. It occurs mostly by brute force attacks with password dictionaries.

• *Hacked APIs:* 
  Hacked APIs while using third-party applications or medieval applications connected through web APIs for smooth transactions of data queries and data processing in applications for the scheduled or nonscheduled tasks, often used by the network listeners.

• *Advanced persistent threats (APTs):* 
  Threats of data mining by illicit users or outsiders through advanced persistent attacks for long-term monitoring or sensitive data of business applications and its users.

• *Hijacked accounts or traffic:* 
  Compromised accounts of users and internal clients or administrators of applications. This occurs due to low-level login security.

• *DOS and DDOS attacks:* 
  Denial of services attack for shutting down or collapsing business service applications and peripherals to impact business and trust in business or service consumers. It is among the most common attack.

• *Network Penetration:* 
  Penetrating network among various or standalone application(s) to impact or catch the data flow for implanting code injections or monitoring tools.

• *Business discontinuity:* 
  Risk of business discontinuity due to natural disasters or loss of physical assets due to criminal activities. To avoid this, CSPs and ITS firms provide DR and backup services by replicating databases, servers, and monitoring systems.

• *Maintenance of Compliance:* 
  Maintain compliance through annual or periodic checkups or expiration of certificates or credentials within or outside the application system.

• *CEO Strategy execution:* 
  Deviation or failure in the execution of top-level strategy for business scope and tactics to perform penetration in existing or implementation of market or products in the business market.

To overcome the above challenges, enterprises need dedicated resources and planning. Electronic /Virtual CISO can do the same for enterprises at low cost with no hassle to HR services. eCISO will first review the enterprise's systems and then provide a suggestion report to the enterprise and then put up a contractual service proposal to the enterprise. Appointing an eCISO will ensure the compliances will meet on time and get reviewed and audited. To combine with it, eCISO can also suggest Business continuity planning and suggest VAPT practices as and when needed according to business scope. eCISO services can be added to any model of SECaaS below:

- Pay as you go, model.
- Subscription Model
- Freeware Model
- Open-source model
4. Challenges in SECaaS model
Most of the major SECaaS models are based on service models that were introduced to fulfill the customer's subscription needs because of its convenience to the consumer and long-run business plans for CSPs and SECaaS providers. One of the drawbacks of such models is the incapability to cover the scope of business of an enterprise using SECaaS services, to overcome this company hires experts as CISO who can provide the best-fit bouquet of models and service from CSPs, allowing negotiations and include on-premises services or cloud-based security services like AWS guard which secure the cores of business workflows. Through eCISO services, Enterprises can select the best fit SECaaS and security services with added benefits for financial savings. The need-based financial models are not much available in the market, which sometimes results in overprotection or under the protection of security to products and projects telecasted to consumers. In some models, services are designed to be consumed and paid as broadcasted mode, whether there were consumed or not by enterprises.

4.1 IT Levels: Impact on Security
There are multiple layers on security as a Service model to cope up with eCISO services; the following are the layers and their peripherals, which can be enhanced with eCISO services.
- IT Governance
- Identity and access management
- Decision engine and board meetings
- Business Continuity Planning
- Disaster Recovery
- Media and PR
- IT Compliance Audit
- Security consultancy
- Strategy Management
- Research and Development
- Critical Incident Management
- IoT application management

4.2 Tools Impacting in Augmenting SECaaS with eCISO.
Tools play an important role in the current IT security scenario. Below are some external tools that eCISO services can use along with SECaaS service provider for executing security strategies and business activities:
- **CyberArk:**
  A tool to provide access security solutions to protect workstations against credential theft in a public cloud environment.
- **Evident.io:**
  Security, compliance, and threat defense platform for public cloud infrastructure
- **Immune.io:**
  A tool to protect web apps against application-layer attacks
- **Force point DLP:**
  A tool to enhance data loss prevention.
- **Chef Automate:**
  An analytical tool that enables cross-team collaboration aiding compliances and auditable history.
- **IBM QRadar:**
  Security information and event management tools help the security teams reduce the incidents and prioritize the detected threats by analyzing the events.
- **ServiceNow:**
  Security information and event management tools help the security teams reduce the incidents and prioritize the detected threats by analyzing the events.
- **AWS Cloud security monitoring (AWSGuard):**
Tools for monitoring security firewalls and networks.

Based on the configuration and scope of business and service provider, many other tools for governance and security compliance can be used by eCISO. There is no suggestion for compulsion of tools or services in this paper.

4.3 Impact of cost-efficiency

Based on a payscale survey \(^{[14]}\) and bitsight \(^{[15]}\), the annual remuneration for CISO will cost between $50,000 to $500,000 to the company. In contrast, the eCISO services, for example, from eCISO.io, will cost $500 to $1500 monthly, based on a subscription model for any SME/MSME.

This plays important reasoning for adapting eCISO services and the SECaaS model by service providers for a cheaper and better bouquet of services to the consumer and businesses.

5. Results with Future Scope and Development

This is an attempt to introduce a new conceptual model to overcome the challenges faced in the SECaaS model by business and services providers through augmenting it with eCISO services for IT Security cost reduction and better compliance management. To practically implement the same needs keen supervision by business owners and understanding the complex scope of a business, which can impact such a model's sub-modeling. We can implement this augmented security model and find out the hidden flaws and complexity in the practical world in the near future.

6. Conclusion

In today's digitalization of business to support its core activities requires a keen vision, and execution of IT security strategy customized for their business scope is very important. Security in the IT world is an area where continuous development is required to help out business enhance IT security. Security as a service model is a cloud-based security service model to provide secure environments, mediums, and systems to enterprises. SECaaS (Security as a service) is essentially a business model in which companies can procure on-demand security solutions to protect their data, systems, and applications while benefitting from what cloud storage provides.

Implementation and execution of activities through this model can be introduced for cost reduction without compromising the security wall of the business applications, at a better rate of consumption with better accuracy and allowing owners to focus on planning, targeting, strategizing, and execution of core activities for IT governance, it will be a revolution in IT security services world.

Acknowledgment

The authors wish to acknowledge the Symbiosis Centre of Information Technology for providing the laboratory facilities.

Conflict of Interest: There is no conflict of interest among the authors

Funding: Self-funded

Ethical approval: Not applicable

References

[1]. Delamore, Baden & Ko, Ryan. (2015). Security as a service (SecaaS)—an overview.10.1016/B978-0-12801595-7.00009-4.
[2]. TaghaviZargar, Saman & Takabi, Hassan & Iyer, Jay. (2019). Security-as-a-Service (SECaaS) in the Cloud. 10.1002/9781119053385.ch9.
[3]. Furfaro, Angelo & Garro, Alfredo & Tundis, Andrea. (2014). Towards security as a Service (SecaaS): On the modeling of Security Services for Cloud Computing. Proceedings -
International Carnahan Conference on Security Technology. 2014. 1-6. 10.1109/CCST.2014.6986995.

[4]. N. Chakraborty and R. Singh Patel. (2014) "Security Challenges in Cloud Computing: A Comprehensive Study," International Journal of Computer Science Engineering and Technology (IJCSET), vol. 4, no. 1, 1-4.

[5]. J. Kehrmann. (2019) "Cybersecurity issues can’t be solved by simply buying a product". Available at https://www.helpnetsecurity.com/2019/09/09/cybersecurity-issues/

[6]. Fang Liu, Jin Tong, Jian Mao, Robert Bohn, John Messina, Lee Badger, Dawn Leaf. (2011); NIST Cloud Computing Reference Architecture; NIST Special Publication 500-292.

[7]. Thomas Winans and J S Brown. (2009). Cloud Computing: A Collection of Working Papers, May.

[8]. Bouayad, A.; Bilat, A.; ElHoudaMejhed, N.; El Ghazi, M. (2012),“Cloud computing: Security challenges,” Information Science and Technology (CIST), Colloquium in, vol., no., pp.26,31, 22-24 Oct. 2012 doi: 10.1109/CIST.2012.6388058

[9]. N Jenefa, N Jayalaxmi. (2013). A Cloud Storage System with Data Confidentiality and Data Forwarding, International Journal of Soft Computing and Engineering, ISSN: 22312307, Vol X Issue X, March

[10]. DS Bhilare and Nilotpal(2013) Chakraborty Enhanced Security in Cloud Computing Environment, International Journal of Advanced Research in Computer Science and Software Engineering, Vol 3Issue 9, September

[11]. Cloud Security Alliance (2013). “The Notorious Nine: Cloud Computing Top Threats in 2013”, To Threats Working Group, Cloud Security Alliance February.

[12]. C. Gentry (2009). Fully homomorphic encryption using ideal lattices. In STOC '09, pages 169-178, ACM, Cloud Security Alliance: Security Guidance for Critical Areas of Focus in Cloud Computing: http://www.cloudsecurityalliance.org/csaguide.pdf.

[13]. A Forni. (2017). "Gartner Forecasts Worldwide Cloud-Based Security Services to Grow 21 Percent in 2017", Gartner. [Online].Available: https://www.gartner.com/en/newsroom/press-releases/2017-06-13-gartner-forecasts-worldwide-cloud-based-security-services-to-grow-21-percent-in-2017

[14]. PayScale (2020).Average CISO salary in India Available: https://www.payscale.com/research/IN/Job=Chief_Information_Security_Officer/Salary

[15]. Bitsight. (2020).CISO Salaries 2020: ‘Does a Changing Role Demand a Change in Pay?’ Available: https://www.bitsight.com/blog/ciso-salaries-2020-does-a-changing-role-demand-a-change-in-pay