Yes, Governance Matters.

December 26, 2024

LEVERAGING CYBER SECURITY GOVERNANCE AS A STRATEGIC TOOL FOR STARTUPS

In this digital age, where a single data breach can shatter years of hard work, cyber governance has become the cornerstone of business stability and consumer confidence. For startups navigating uncharted waters of the digital world, cyber governance is more than just a safety net. New businesses often face unique challenges when it comes to cybersecurity threats and data privacy. Cyber governance goes beyond merely installing antivirus security software; but is a strategic approach that integrates cybersecurity measures into a company's overall business goals.

In December 2023, data associated with around 200 million profiles on a leading social media platform was compromised,[1] leading to a massive backlash and impact on the stakeholder's trust in the organisation. Similarly, in March 2024, an Indian financial services platform suffered a data compromise,[2] in May 2024, a leading technology solution provider's corporate network was breached,[3] and in June 2024, an Indian telecom giant suffered a breach wherein data such as phone numbers and internal server information was compromised.[4] While only the cyberattacks on larger organizations make headlines, startups cannot afford to overlook cyber governance, as a single breach could be catastrophic, jeopardizing their growth, reputation, and very survival in a competitive landscape. As per reports, 50% of smaller organisations or startups do not have a cybersecurity plan or governance structure in place, while 33% of these entities rely on free cybersecurity solutions rather than professional-level solutions.[5]

IMPORTANCE OF CYBER GOVERNANCE

Startups are particularly vulnerable to cyberattacks, facing significant risks such as financial losses, reputational damage, and statutory liabilities. For startups with limited resources and expertise, prioritizing cyber governance is vital to protecting their digital assets and maintaining stakeholder trust. Strong cyber governance not only keeps sensitive information safe but also ensures compliance with regulations and promotes a culture of security awareness throughout the organization. Further, adopting robust cybersecurity practices can be a key differentiator for startups, enhancing customer trust and setting them apart in competitive markets. Such security measures, like encryption and advanced controls, not only address critical risks but also appeal to investors by demonstrating resilience and foresight. The board of directors ("**Board**") can play a crucial role in driving a strong cybersecurity culture within the organization by providing strategic guidance and oversight. Implementing cyber governance at an early stage is crucial, as it helps establish clear policies, roles, and accountability frameworks.

Further, "privacy by design" is an essential approach for integrating privacy protection into every stage of system and product development. By embedding privacy measures from the start, startups ensure bare minimum and necessary collection, processing, storage and retention of personal data. Implementing good data and cyber security practices are also paramount and involve adopting "privacy first" measures at an organizational level, maintaining an adequate level of security for the data and systems, documenting comprehensive security measures, appointing a data protection officer, conducting regular risk assessments, and enforcing privacy controls to comply with privacy regulations such as privacy notices and consents.

CYBERSECURITY COMPLIANCE IN INDIA

India has progressively strengthened its focus on cybersecurity and governance, refining its legal framework to ensure protection against cyber threats. Organizations must ensure that their cyber governance framework complies with several key regulations. One of the most important is the *Information Technology Act, 2000* ("**IT Act**"), which provides the legal framework for electronic governance in India. The IT Act criminalizes various cybercrimes, including unauthorized system access, data theft, system disruption denial of access, while also mandating compliance with reasonable security practices and policies if an entity collects or deals with sensitive personal data. The Board should be actively involved in reviewing and approving the organization's cybersecurity policies and procedures, as well as overseeing the implementation of these measures. The board should also ensure that the organization has adequate resources and expertise to address cybersecurity risks.

In addition to the IT Act, there exist several other critical frameworks in India aimed at reporting, investigating, and combating cybersecurity incidents. One such framework is the *National Cyber Security Policy*,[6] which serves as a comprehensive guide for businesses and government entities in developing customized security measures. The policy emphasizes collaboration between the public and private sectors to enhance the protection of information technology systems and networks. Another significant regulation is the *CERT-In Directions, 2022*[7] read with the FAQs, which require service providers, intermediaries, data centers, and body corporates to report any cyber incidents within 6 (six) hours, provided certain severity thresholds are met such as the impact on public information infrastructure, data breaches, data leaks, large scale or frequent incidents or incidents which impact the safety of

Research Papers

FAQs on Setting Up of Offices in India
December 13, 2024

FAQs on Downstream Investment
December 13, 2024

Gaming Law 2024
December 12, 2024

Research Articles

The Revolution Realized: Bitcoin's Triumph
December 05, 2024

The Bitcoin Effect
November 14, 2024

Acquirers Beware: Indian Merger Control Regime Revamped!
September 15, 2024

Audio

Securities Market Regulator's Continued Quest Against "Unfiltered" Financial Advice
December 18, 2024

Digital Lending - Part 1 - What's New with NBFC P2Ps
November 19, 2024

Renewable Roadmap: Budget 2024 and Beyond - Part I
August 26, 2024

NDA Connect

Connect with us at events, conferences and seminars.

NDA Hotline

Click here to view Hotline archives.

Video

"Investment return is not enough" Nishith Desai with Nikunj Dalmia (ET Now) at FII8 event in Riyadh
October 31, 2024

Analysing SEBI's Consultation Paper on Simplification of registration for FPIs

individuals. In other cases, cyber incidents affecting or involving computer infrastructure within Inda are required to be reported as soon as possible to leave scope for timely action *(pursuant to the CERT-In Rules, 2013)*. Organizations are required to designate a point of contact (PoC) to liaise with CERT-In on cyber incident reporting and response efforts, as well as store system logs on an ongoing basis for 180 days.

Once the personal data protection law in India, i.e. *The Digital Personal Data Protection Act, 2023* comes into force, 'personal data breaches' are required to be reported to the Data Protection Board and affected data subject.

Furthermore, organizations must comply with various sectoral regulations if they are regulated or licensed entities in the respective sector. Industry-specific regulations issued for instance by the Securities and Exchange Board of India, the Reserve Bank of India, and the Insurance Regulatory and Development Authority prescribe cybersecurity practices to be implemented and data breach reporting to the respective regulator.

A HOLISTIC APPROACH TO EFFECTIVE CYBER GOVERNANCE

A holistic approach to cyber governance is essential for building resilient organizations that can withstand evolving cyber threats. By addressing technical, legal, and operational risks collectively, startups can create a robust framework for secure and sustainable growth. Methods that may be adopted by startups in order to improve cyber governance are discussed below, offering actionable insights to enhance resilience and readiness against cyber risks.

1. *Board* – The Board plays a key role in steering a startup's cyber governance strategy, overseeing risk management framework, and prioritizing cybersecurity as a core foundation. By fostering a strong cybersecurity culture, the Board ensures alignment with industry best practices and regulatory requirements, actively monitoring threats, and driving the integration of cybersecurity into the organization's overall strategy. This includes allocating sufficient resources to address emerging risks, enabling efficient risk assessments, and ensuring swift incident responses that help prevent costly data breaches and operational downtime. The chief information security officer ("**CISO**") plays a crucial role in executing this strategy, providing specialized expertise, leading the development of cybersecurity policies, and managing day-to-day security operations. The CISO also works closely with the Board to ensure the organization is prepared to tackle evolving cyber threats, offering critical insights into risk management and incident response planning.

2. *Cyber insurance* – Beyond governance, cyber insurance is a critical tool for startups to manage the financial impact of cyber incidents. The Board can evaluate the organization's risk profile and collaborate with insurance providers to secure appropriate coverage. Such policies not only mitigate the costs associated with cyberattacks but also provide access to cybersecurity experts and legal advisors to guide effective incident response and remediation. This comprehensive support helps startups recover quickly with minimal disruption, reinforcing their ability to navigate and manage the growing threat of cyber risks.

3. *Risk Assessments* – Conducting regular risk assessments is essential to effective cyber governance, enabling organizations to identify gaps and vulnerabilities in their cybersecurity frameworks. The Board should play an active role in overseeing these assessments, ensuring that risks are evaluated comprehensively and mitigation strategies are implemented promptly and effectively. A well-structured risk assessment not only highlights areas of concern but also aligns the organization's cybersecurity priorities with its operational goals and regulatory obligations.

   For instance, a startup operating in the healthcare industry must prioritize a thorough evaluation of the sensitive patient data it collects and whether all of it is necessary to collect in order to develop and offer its service to consumers. This includes understanding what types of data are gathered (e.g., medical histories, payment details), how and where the data is stored (e.g., on-premises servers or cloud solutions), and with whom it is shared (e.g., insurance companies, third-party service providers). Risk assessments in this context would involve analysing the security measures protecting this data, identifying potential vulnerabilities such as insufficient encryption or unauthorized access points, and addressing them through targeted interventions.

4. *Employee Training* – Employee training is a critical component of improving cyber governance, as human error can prove to be a reason behind security breaches. The Board plays a key role in allocating sufficient resources to ensure that employees are consistently trained and equipped with the knowledge necessary to mitigate cybersecurity threats. This training should not only cover basic security protocols but also focus on practical skills employees must inculcate in their day-to-day tasks.

   Training programs should include key topics such as recognizing phishing emails, avoiding suspicious links, and maintaining strong password hygiene. Employees should be taught to identify red flags in emails, such as unfamiliar senders, urgent language, or mismatched URLs, and how to report such incidents. Additionally, employees should be educated on the importance of using multi-factor authentication, ensuring that sensitive data is only accessed through secure networks, and safeguarding personal devices used for work purposes. By fostering a culture of awareness, employees become the first line of defence against cyber threats, reducing the likelihood of breaches and minimizing potential damage to the organization.

5. *Incident Response*– An incident response plan is a structured approach that outlines the steps an organization will take in the event of a cybersecurity breach or attack. It provides clear guidelines for detecting, escalating, responding to, and recovering from security incidents, to minimize damage, protect sensitive data, and restore normal operations as quickly as possible. A well-defined response plan, supported by expert personnel, is a critical component of effective cyber governance and can significantly mitigate the impact of a cyberattack.

   The Board must play an active role in reviewing, approving, and ensuring the incident response plan is robust, comprehensive, and regularly updated. The CISO is integral to the designing and implementation of this step, providing the necessary expertise to lead the response efforts, coordinate technical resources, and communicate effectively with stakeholders. The CISO ensures that the organization is prepared for any cyber threat, taking charge of incident management, and ensuring a swift, organized, and effective response to minimize business disruption and safeguard valuable assets.

6. *Vendors*– Vendor management plays a critical role in enhancing cybersecurity and reducing external vulnerabilities. Conducting thorough vendor diligence is essential to identify potential risks associated with third-

September 26, 2024

Scope of judicial interference and inquiry in an application for appointment of arbitrator under the (Indian) Arbitration and Conciliation Act, 1996

September 22, 2024

party service providers, ensuring that only vendors with strong security practices are engaged. Vendor contracts must include stringent security obligations and compliance requirements, such as adherence to industry standards, regular audits, breach notification protocols, and oversight. The company should seek back-to-back indemnities against the vendor for any liabilities that it may be exposed to against the customer or if subject to statutory fines in case of a non-compliance with cyber security laws and a cyber security breach.

The choice between a cloud-based provider and a physical server-based provider also has significant implications for cybersecurity. Cloud providers often offer advanced security features, such as automated updates, scalable encryption, and real-time threat monitoring, which are difficult to achieve with on-premises servers. However, selecting a reliable cloud provider requires evaluating their security certifications, data residency policies, and disaster recovery mechanisms. On the other hand, physical server-based solutions may offer greater control but can expose organizations to risks if internal security measures, such as physical access controls and regular patching, are not robust.

7. *Leveraging New Technologies*– Adopting cutting-edge security solutions is essential to curb cyber threats and ensure a resilient organizational framework. Technologies such as AI-based threat detection, encryption, and multi-factor authentication provide advanced safeguards against evolving risks. AI-powered systems, for example, can analyse vast amounts of data in real-time to identify signs of potential cyber breaches, such as multiple login attempts from different locations or transactions that deviate from normal behavior.

   These tools can also flag phishing emails by identifying inconsistencies in language, links, or sender addresses, effectively preventing scams before they escalate. Additionally, encryption protects sensitive data by converting it into unreadable formats accessible only with proper authorization, while multi-factor authentication adds an extra layer of security by requiring multiple verification steps. The Board must ensure adequate budgeting for these investments, replacing outdated technologies and prioritizing continuous upgrades.

8. *Data Residency and Control* – Effective data management is a strategic defence against cyberattacks, and can enable startups to protect their most critical assets. Data localization, which involves storing personal data (including sensitive data) within specific geographic boundaries, reduces exposure to foreign threats, foreign Government access and ensures compliance with local regulations. By keeping data within secure jurisdictions, startups can better control access and mitigate the risks associated with international cyberattacks. Similarly, implementing a policy wherein data is shared with employees on a "need-to-know" basis restricts access to sensitive information, limiting the potential for internal breaches or inadvertent leaks.

   In addition, robust infosec policies, "bring your own device" (BYOD) policies as well as the use of company-issued devices play a vital role in endpoint security. Clear guidelines on device usage, mandatory encryption, and regular security updates help prevent unauthorized access, data loss and reduce vulnerabilities. Complementing these measures, a comprehensive information security policy acts as a blueprint for safeguarding data. It should encompass key data management practices, including access controls, encryption standards, and incident response protocols.

DIFFERENTIATING FROM COMPETITION

As the digital landscape continues to evolve, startups and small businesses, which are particularly vulnerable to cyberattacks, must adopt a proactive rather than reactive approach to cybersecurity governance. By staying informed about emerging threats and regulatory frameworks, Board members can offer valuable insights and challenge management's assumptions, while organizations navigate national and international cybersecurity laws with legal counsel to mitigate risks. Establishing centralized governance frameworks ensures global compliance, allocates resources effectively, and strengthens defences across jurisdictions. Cyber governance can no longer be viewed as an after-thought; it must be an integral part of an organization's governance and cultural set-up, which can often be a differentiator against market competitors.

Authors:

– Divyansh Bhardwaj, Rhythm Vijayvargiya, Maulin Salvi and Aaron Kamath

You can direct your queries or comments to the relevant member.

[1] https://purplesec.us/breach-report/twitter-data-leak-200-million-users/

[2] https://www.business-standard.com/companies/startups/financial-services-firm-werize-becomes-the-victim-of-a-data-breach-124031501231_1.html

[3] https://purplesec.us/breach-report/cisco-cyber-attack/

[4] https://www.business-standard.com/companies/news/bsnl-data-breach-exposes-278-gb-of-sensitive-telecom-info-twice-in-6-mts-124062600314_1.html

[5] https://upcity.com/experts/small-business-cybersecurity-survey/

[6] https://www.meity.gov.in/writereaddata/files/National_cyber_security_policy-2013_0.pdf

[7] https://www.cert-in.org.in/PDF/CERT-In_Directions_70B_28.04.2022.pdf