Law Journals
A Treasure Trove of Legal Knowledge.

National Journal of Cyber Security Law
Volume 1, Issue 1
www.stmjournals.com

Cybersecurity Risk Compliance in India

Mukesh Saini*
Managing Director, Xitiz Cyber Security Solutions Pvt. Ltd., Noida, Uttar Pradesh, India

Abstract

The cyber risk to all companies is real and present. It impacts not only financially but also adversely to the company's reputation and its brand. The Companies Act 2013 has made the Board of Directors responsible for appropriately manage risk to the company (S. 134), while auditors are accountable for reporting any risk to the company (S.177). The Auditing standard AAS 29(SA 401) requires computer security auditing. Therefore, annual auditor's report will be incomplete without assessing cybersecurity risk management policy and its implementation. The auditors may seek experts' help to complete the effective audit. Therefore, cybersecurity risk management is statutory for compliance requirement.

Keywords*: Cybersecurity risk management, The Companies Act 2013, Auditing Standards, Compliance, Auditor's reports, Vulnerability Assessment and Penetration Testing (VAPT), Cyber Hygiene, Incident Management, Awareness*

**Author for Correspondence* E-mail: commandersaini@gmail.com

INTRODUCTION

No one can deny that cybersecurity risk to any corporate is real and present. According to the cost of Cybercrime study, 2017 by Ponemon Institute, the companies on average have lost $11.7 million to cybercrimes which have increased 27.4% over previous year. The total loss is estimated to be more than $600 billion in 2017.

In the minds of Boards of Directors, there is lots of fear, uncertainty and doubt about the state of technological risk their respective company is facing. The issue has become more complicated because till now the non-tech savvy Board of Directors were not too concern about this highly technical field and they trusted that the professional staff. With the extreme crunch of manpower CISO (Chief Information Security Officer) is limited to large companies. Medium and small companies lack the financial ability to have one on their payroll. But that apart, is there a statutory compliance requirement to manage the cybersecurity risk?

The Company Act 2013 and the Information Technology Act 2000 are the primary laws seeking compliance in relation to the technology matters. While Auditing standards are mandatory to comply with before a financial audit report is signed-off and submitted to the Government. But can any company registered with Ministry of Corporate Affairs afford to be non-compliant? It needs to be clearly established as to what are the exact compliance requirements if any and how can they be met?

CYBER INTRUSIONS AND E-FRAUDS POSE SIGNIFICANT FINANCIAL/SURVIVAL RISKS

According to the Kroll Annual Fraud and Risk Report released on 24 Jan 2018, in India, the percentage of respondent affected by fraud increased significantly by 21% in 2017 to 89% while the global average this year is 84%. It was also reported that 84% of respondent in India experienced cyber-attack in past 12 months. According to PwC 21st CEO Survey report, cybersecurity risk has moved up to 4th position to challenge the existence of the company. Ponemon Institute estimates the average cost of a data breach in 2017 as $3.6 million. With GST becoming the law of the land, all financial data across the country now are in digital form. Any company with more than 100 employees uses networked environment for its most of the functions. There is enhanced risk from the *General Data Protection Regulation* (*GDPR*) for companies operating in European countries. The failure to comply with GDPR can attract fine up to 2 million Euro or 4% of group turnover whichever is higher. Similar laws are expected

all over the world including India in the near future, impacting very existence of the company in case Cyber (privacy related) risks are not controlled. Therefore, cyber risk (technology related risk) is significant and can have a dramatic adverse impact on a victim company.

THE COMPANY ACT 2013

A company today maintains their financial records in digital form. Websites/ Net-Banking/ On-line payments are used for the financial transaction, financial data is kept on the cloud, transactions and approvals are granted through emails and other electronic means. These records are accessed over net either at the Local Area Network (LAN), the Wide Area Network (WAN) and Virtual Private Net (VPN). Access control mechanisms are all computerised. Authentication and Authorisation are undertaken by machines on behalf of humans. Audit trails and logs are voluminous and not-human-readable. All these and many more things are vulnerable to various risks which only proper methodological approach can evaluate and mitigate.

Section 134(3)(n) of the Company Act expects from the Board of Directors to approve the financial statement including indicating development and a risk management policy for the company including identification therein of elements of risk, if any, which in the opinion of the Board may threaten the existence of the company. As computer- based threats (such as ransomware encrypting all financial record) and e-frauds comprehensively called Cyber risk pose a clear and unambiguous threat, they should be included in such annual financial reports submitted to MCA. If God forbid, the company suffers significant financial loss or reputation loss, the company not having cyber risk management policy will be held non-compliant.

The terms of reference for the Audit Committee constituted under Section 177(4)(vii) requires relevant financial controls & risk management system. It has been argued by some that law expects only financial risk management system and cyber security has no role. This is an incorrect view. As stated earlier, today no accounting system is manual. The financial controls are executed through information technology. The process of execution is not visible to humans. For example, there is a control of maker-checker where person entering data has to be different from person validating the data. It has been observed that in many small company same person holds both the username & passwords and process from the same computer. Without Technical support it will not be possible for the auditors to validate this control. It is also possible to do "salami" from financial accounting. With huge database it is impracticable to validate entries & controls correct execution. Software integrity, insiders or hackers manipulating financial records requires that the appropriate cyber security controls are also implemented. The sub-section 177(6) empowers the audit committee to seek professional advice from external sources. Though law allows them to have full access to the information contained in the records but only IT Security professional can actually see using appropriate tools.

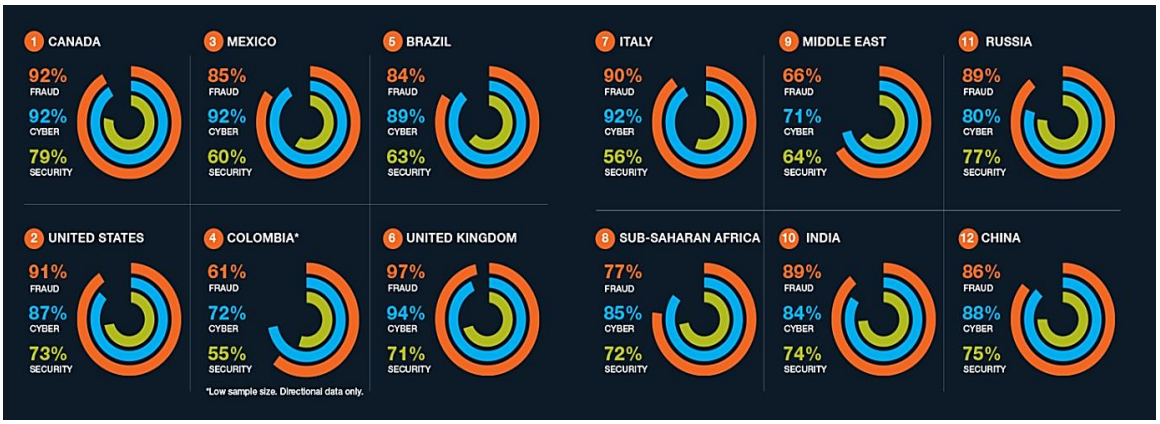

Fig. 1: Global Fraud &Risk Report-2018

Source: https://www.kroll.com/en-us/global-fraud-and-risk-report-2018.[1]

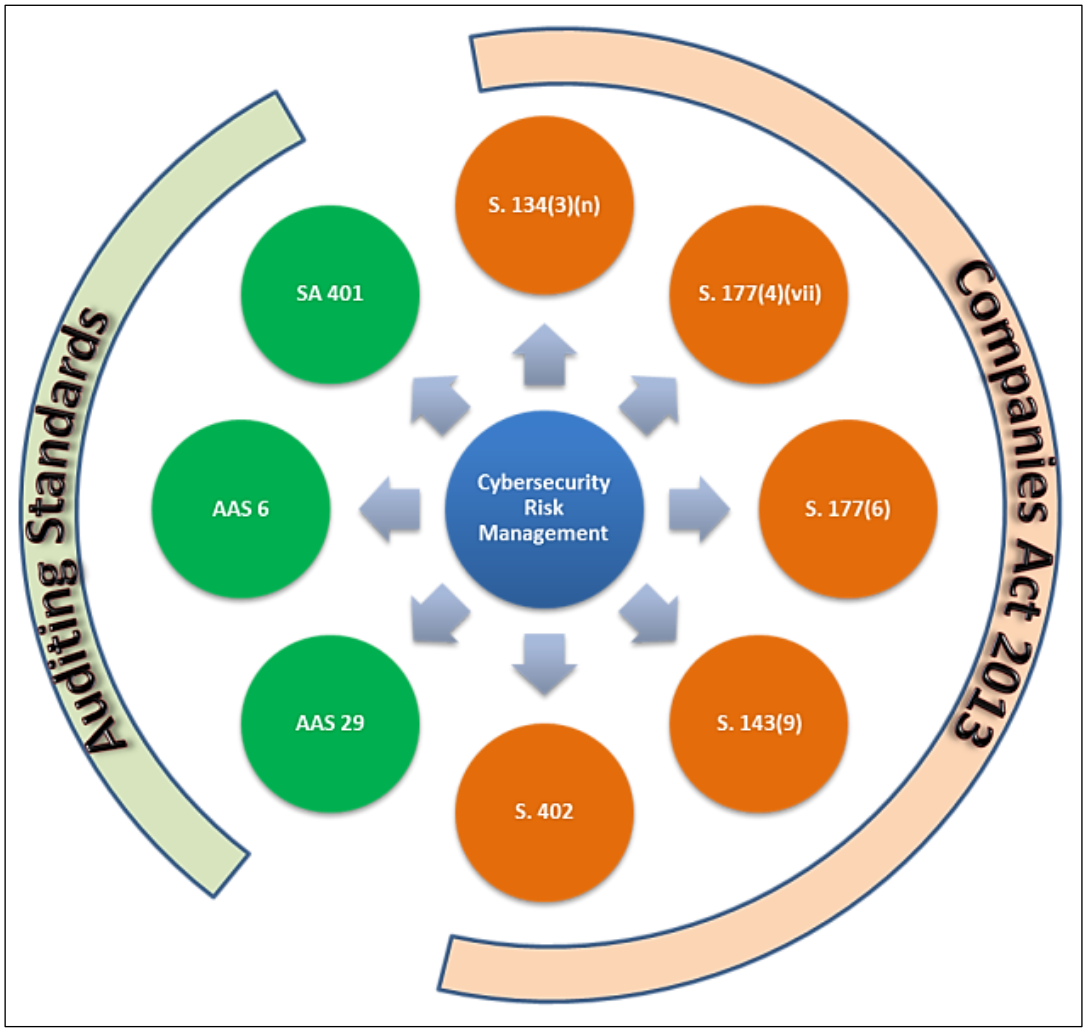

Fig. 2: Cybersecurity Risk Management

The auditors have absolute rights all the time access to the company's financial records and controls kept at head office or anywhere else. It is possible to have VPN access to these records from anywhere in the world. If a company gives such rights it must be adequately instituted after a due Cyber risk assessment, else hackers may exploit such functionalities.

Section 143(9) of the Companies Act requires all auditors to comply with the auditing standards. This includes Auditing and Assurance Standard (AAS) 29, "Auditing in a Computer Information Systems Environment" read with Auditing and Assurance Standard (AAS) 6, "Risk Assessments and Internal Control". To undertake such task in today's sophisticated cyber environment with basic knowledge of computers is insufficient. The standard expects to join of experts for it. Non-compliance with AAS 29 and AAS6 can put the auditors as well as the Board in trouble.

The Section 402 Companies Act extends all provisions of the Information Technology Act on the Companies Act related to electronic documents and records. This also means that relevant provisions in the Evidence Act and Indian Penal Code are also applicable. The new privacy laws will also impact companies and its data security issues. These issues can have a vital impact on the very survival of a company.

CYBER SECURITY RISK MANAGEMENT

Therefore, to achieve compliance, it is preferable that company meet the ISO/IEC 27001 standard. In case due the size or scope of the company or due to financial constraints it is not possible then every company

registered with Ministry of Corporate Affairs undertake at least following measures [2]. In their own interest auditors must ensure the same. Support for Cybersecurity professionals should be taken as this is a deeper technical issue.

Vulnerability Assessment and Penetration
Therefore, it is a compliance requirement for a company to undertake Vulnerability Assessment and Penetration (VAPT) testing to gather evidence-based risk estimate. The VAPT form the basis of risk assessments related to CIS, without which all other actions are arbitrary and unfocused.

Cyber Security Policies
A company must adopt any framework for designing Cyber Security policies. According to rules made under Section 43 of the Information Technology Act ISO/IEC 27001:2013 is recommended by the regulatory ministry. The compliance with these policies correct must be routinely audited by qualified auditors.

Cyber Hygiene
All networks must maintain at the very least appropriate cyber hygiene. Unstructured and ad-hoc approach to technology procurement, software/application development and non-compliance with fundamental tenets of Cybersecurity can put only the company in a harm's way but with various statutory provisions can cause fine as well as penal action against those who are responsible for corporate affairs. [3]

Incident Management
Most critical component of cybersecurity is incident management policies, processes and procedures. It should be defined appropriately with the help of experts and implemented meticulously. An annual Incident management report is one of the critical reports to the Board. [4]

Awareness
Humans are the first shield against any cyber threat. They must be kept aware of the challenges of a cyber threat as well as various attempts made by hackers to extract information including social engineering.

CONCLUSION
The Company Act was passed in 2013 has several provisions for control or risk & auditing mechanism for the well-being of a company. Those provisions are presently being overlooked by most in respect of Cybersecurity Risks, as if they do not have a financial impact, which is not true. Most financial auditors do not have necessary technical knowledge to handle complex and highly technical cybersecurity issues; therefore, they should seek expert help. It can thus be concluded that the Cybersecurity risk management is a statutory compliance requirement.

REFERENCES
1. https://www.kroll.com/en-us/global-fraud-and-risk-report-2018
2. https://www.pwc.com/gx/en/ceo-agenda/ceosurvey/2018/gx.html
3. https://www.accenture.com/t20170926T072837Z__w__/us-en/_acnmedia/PDF-61/Accenture-2017-CostCyberCrimeStudy.pdf
4. https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&uact=8&ved=0ahUKEwifqamqrMnbAhWDV30KHbURCuYQFggoMAA&url=https%3A%2F%2Fwww.kroll.com%2Fen-us%2Fglobal-fraud-and-risk-report-2018&usg=AOvVaw3AomBK7jSWO0lwWrwlsEFB

Cite this Article
Mukesh Saini. Cybersecurity Risk Compliance in India. *National Journal of Cyber Security Law.* 2018; 1(1): 65-68p