Information Security Compliance Management considerations and challenges posed by evolving landscape of cyber threats

Ashish Ukidve
Principal, Vidyalankar Polytechnic,
Mumbai, India
email- ashish.ukidve@vpt.edu.in

Dr S S Mantha
Ex-Chairman, AICTE
Chancellor-KL University
e-mail-ssmantha@gmail.com

Dr D N Reddy
Professor, Osmania University
Former VC , JNTUH
e-mail-reddydn @gmail.com

Abstract – The cyber threat landscape is constantly evolving. Different types of cyberattacks continue to contest the minds of cybersecurity professionals around the globe. Phishing ,malware , man-in-the-middle and Denial of service attacks, have become common jargon in a world battling with the cyberattack challenges. In present evolving threat landscape, it's logical that organizations want to take a proactive approach against threats, create an environment of continuous compliance, and have responsive IT operations processes. Organizations want to reduce risk exposure and the attack surface, detect and respond to advanced threats, and drive down security operations costs. This paper analyses security practices at various commercial and public institutions and provide approach to optimize future security and compliance programs.

Index Terms- compliance management , risk mitigation, operational risk security threats, security breaches, compliance framework, end point devices

1. INTRODUCTION

The diffusion of technology & commoditization of the information has transformed the role of information into a resource equal to any other major resource such as land, labour & capital. The exponential growth of information exchange & information availability after the internet boom has resulted into a situation where fortunes of most organizations are tied to the information they possess and the sophistication with which they are able to manage it. .

The cyber threat landscape is constantly evolving. Different types of cyberattacks continue to contest the minds of cybersecurity professionals around the globe. Phishing ,malware , man-in-the-middle and Denial of service attacks, have become common jargon in a world battling with the cyberattack challenges. The analysis done here provides AS-IS scenario of information security compliance management and the considerations that will drive future course of security compliances for organisatons. For this analysis, purposive sampling technique was used to select interview respondents across the hierarchy in organizations to capture multiple viewpoints and interviews were conducted, face-to-face in the real-life setting of the respondents**.** Also the findings of surveys conducted by global leaders in information security were taken into account. After detailed analysis , the major parameters which will have to be taken into consideration for information security compliance in future are presented below -

2. COMPLIANCE REQUIREMENTS OF INFORMATION SECURITY

Compliance is multifaceted and involves analyzing a company's security processes. It details their security at a single snapshot in time and compares it to a specific set of regulatory requirements. These requirements come in the form of legislation, industry regulations, or standards created from best practices.It was observed that companies may have to comply with multiple frameworks ,either as statutory requirement or to adopt industry best practice or as a business need . The main goal is to manage risk which include overseeing policies, regulations, and laws and also cover physical, financial, legal, or other types of risk. Organizations face an ever-increasing list of statutory, regulatory, contractual, and legal compliance obligations. Multiplicity of Security frameworks, practices and standards can overwhelm organizations and introduce substantial unexpected costs and cause unforeseen consequences.

3. EFFECT OF SECURITY BREACHES

Global Information Security Survey (Oct 2020) conducted by EY , revealed that about 6 in 10 organizations (59%) have faced a material or significant incident in the past 12 months. Global Board Risk Survey also conducted by EY reveals, 48% of the governing boards believe that cyber attacks and data breaches will more than moderately impact their business in the next 12 months. About 21 % of these attacks came from "hacktivists" who are tech-enabled, political and social activists. This is alarming when compared with cybeattckes carried out by professional hackers i.e 23%

As per PWC cyber threats 2020 survey , due to COVID-19 pandemic bringing an unprecedented change to the business world and also to the cyber threat landscape. The dependency on remote working infrastructure has brought existing threats into prominence, such as the exploitation of vulnerabilities in VPNs, enterprise remote access.

4. RAPID EVOLUTION IN SECURITY AND TECHNOLOGY

As a result of digital-physical convergence , security threats are not uniform and theore security dimensions differ from one business to another. Hence" Single Security Solution " may not be available for keeping systems and data safe.

Security management has to evolve to meet today's sophisticated threats. The solutions that were used last year, or the year before, need to be re-assessed, relative to their current value proposition. Only those technologies and vendor partnerships who will rise to meet the change will go into the future. Already big shifts in the vendor community are apparent; vendors long considered leaders in the space have lost their standing, and new vendors are taking their place. In any case, solutions need to consider current and future needs of an organization. On the other hand security solutions need to commonly share threat intelligence with each other and other industry members.

These changes can make it difficult for organizations to invest in security. As a result, organizations need to decide as to what is their risk appetite and what they want in terms of security. They should identify the critical assets that need the most protection along with the technologies, people, and other resources that are necessary to get the job done.

Most organizations should adopt appropriate security framework . The publically available security frameworks such as ISO27001 , NIST, CIAS ,Gartner's PPDR etc. can be adopted and implemented. After selection of framework, it will need to be calibrated and tuned to the specific requirements and ecosystem of the organization. Implementation of the selected framework will require a elaborate plan, strong investment, expert partners.

5. NON AVAILABILITY SKILLED RESOURCES

One of the contributing and elevating factors to rising breach costs is the ongoing InfoSec skills gap, as per the joint study conducted by ISACA and RSA.

In the joint study by ISACA/RSA study, 52.44% of respondents felt that less than a quarter of their organizations' employees are qualified for their positions. They also identified the largest skills gap in security practitioners' ability to understand the business.

This problem is indeed a serious risk to an organization. If security practioners are not able to fully understand the nature of their business, others in the organization will not be able to appreciate how each asset is relevant to the support of an organization's mission. That means they won't comprehend the relative business importance of protecting each asset, which will hinder their ability to reduce threats and mitigate risks.

A study estimated that there a huge gap between the global need for security professionals and the practitioners which were currently engaged in the field. This skills gap poses a double-risk to organizations as information security practitioners as well as skilled personnel both are rarely available . Each 880rganization needs to address this challenge in order ramp up their data security.

6. THE VOLUMINOUS GROWTH OF ENDPOINT DEVICES

Continuous evolution in technology has now demonstrated that just about everything is now, or shortly will be, connected, accessible, serviced and controlled from the network.(Fig 2)

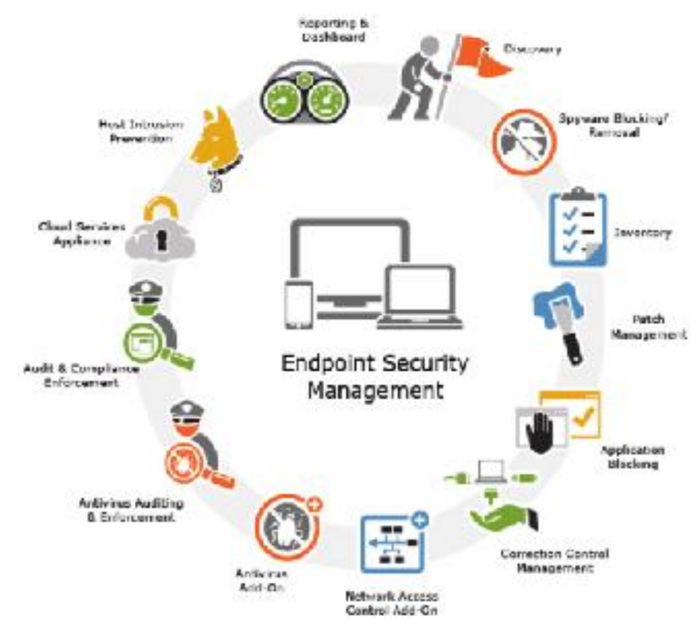
Reporting & Dashboard
Discovery
Spyware Blocking/ Removal
Inventory
Patch Management
Application Blocking
Connection Control Management
Network Access Control Add-On
Antivirus Add-On
Antivirus Auditing & Enforcement
Audit & Compliance Enforcement
Cloud Services Appliance
Host Intrusion Prevention
Endpoint Security Management

Fig-2 Endpoint Security management

As per CISCO , now some 22.9 billion endpoints are up and running on organizations' networks. This explosion of connected devices and assets introduces an incremental scaling problem for most of our earlier security and compliance models and predictions. Companies should have educated, skilled security personnel to protect the diverse array of endpoints in the modern IT environments.

This emphasis to protect so many diverse endpoints will ability of the organization to make sure each device is compliant with industry standards and will therefore drastically increase security operations costs.

7. THE CONJUNCTION OF PHYSICAL INFRA CONTROL BY DIGITAL TECHNIQUES

Across all sectors of the economy, including financial services, retail, food and beverage, industrial, energy, oil/gas, automotive, transportation and utilities companies, the number of endpoints are thriving.

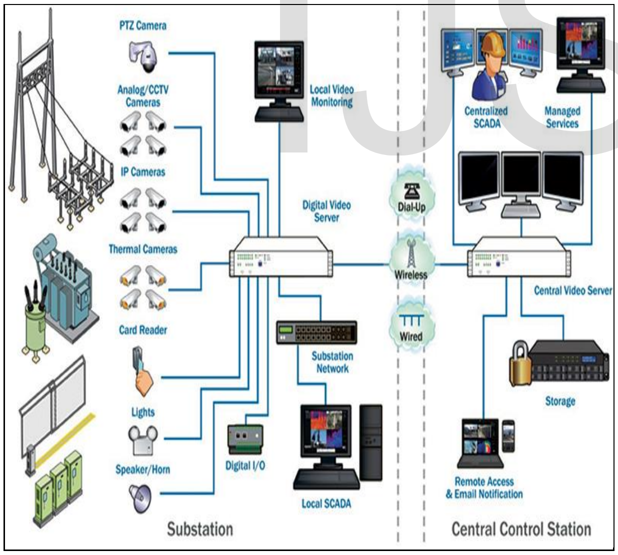

Fig.1 Digitally controlled video monitored power distribution

Many of these organizations maintain critical national infrastructure such as power generation and transmission systems (Fig 1), durable goods and food manufacturing , processing and distribution facilities. Security compromise and threat to their endpoints could lead to harmful consequences or disrupt economy.

In the event that an industrial organization becomes aware of a vulnerability in Industrial Control Systems (ICS), they will apply countermeasures, perform necessary repairs and make sure there are no software conflicts before taking any further action. This is because critical issues in industrial control systems can cause power outages, reduced industrial output, and other adverse downstream effects in a production system.

Many enterprises dedicate much of their information security programs to information confidentiality in order to protect against a breach. However, are hardly concerned with data privacy and ensuring a set of rules limiting unprivileged users' access to information.

Similar to alignment of IT and OT priorities, convergence of the Internet of Things (IoT) and the Industrial Internet of Things (Industrial – IoT), where enterprise and industrial teams must align and work together to streamline their services is need of the time.

Going forward, companies will need to consider systems and all endpoints in IT, IoT/IioT as they decide on a common-ground objective in order to have productive partnerships.

8. CONCLUSION

Organizations need to adopt a forward looking plan that takes the above factors into account. They need to prepare to manage and mitigate the escalating security compliance and operational risks. This process should include:

- To take a pragmatic, proactive approach to cyber security and compliance
- Recognize the scale and complexity of the mission at hand given these trends.
- Use a risk-based orientation for Accurate assessment of the business's needs relative to IT and IoT/IioT,
- Appropriate standards-based framework identification and implementation
- Create security and compliance architecture relevant to organization needs
- Select strategic vendors/partners whose technical abilities, strategic vision, and commercial strength and viability, will support your architecture and whose core capabilities address the challenges these trends present to your organization.
- Development and phased implementation and deployment of your security and compliance plan, based on by business risk analysis.
- Implementation or expansion of continuous monitoring, response and calibration programs.

9. REFERENCES

1. Information Security Management Handbook, Sixth Edition, Volume 5
   edited by Micki Krause Nozaki, Harold F. Tipton
2. Roadmap to Information Security: For IT and Infosec Manager By Michael Whitman
3. Strategies for Information Technology Governance ,Van Grembergen
4. The Strategy-Focused Organization: How Balanced Scorecard Companies Thrive By Robert Kaplan, David P. Norton
5. https://www.pwc.co.uk/cyber-security/pdf/pwc-cyber-threats-2020-a-year-in-retrospect.pdf
6. https://www.isaca.org/Template.cfm?SectionSecurity&Template
7. https://www.iso27001.com
8. https://csrc.nist.gov/publiations/pubssps.html/800-27/sp800-27.pdf