EVOLUTION OF CYBERSECURITY STANDARDS IN FINANCIAL SECTORS

Dr. Sanjay Shinde, IPS, Research Scholar, VAMNICOM, Pune, deosanjay64@gmail.com
Dr.Yashwant Patil Research Guide, VAMNICOM, Pune yspatil@vamnicom.gov.in
Prashant Wadkar Assistant Professor, IIMS, Pune pnwadkar@gmail.com

Abstract:
Cyber Security standards are the set of rules that an organization has to comply with in order to gain security which has to be provided to their customers and financial institute itself to protect from fraudulent cases, e.g. while accepting or doing online payment. The standards consist of basic rules that the organization is supposed to obey in order to maintain compliance with any of the cybersecurity standards. Various Financial Institutions/Banks have several different standards that they can opt for to bring special capabilities and extension of security. The cyber security standards used in many of the countries are to protect themselves and their customers from hackers/fraudsters. The standards used are different in different Financial Institutions/Banks. In India there are different Banking Sectors like Public, Private, Co-operative etc. The research paper is focussed also on these three sectors wherein all these sectors are monitored by Reserve Bank of India(RBI). There is no central foolproof solution provided by the RBI. All three sectors of Banking are utilizing different standards or mix standards which are namely International Organization for Standardization (ISO), National Institute of Standards and Technology (NIST), Payment Card Industry Data Security Standard (PCI DSS) which specifies the security standards for handling credit card information, Health Insurance Portability and Accountability (HIPAA) is used for formation of national standards to protect patient health information, British Standards etc.The Research paper titled "***Evolution of Cybersecurity Standards in Financial Sectors***" throws a light on how the evolution in rules and regulations has happened in India and what is the current scenario of protection against cyber security.

Key Words:
Cyber Security Standards, Hackers, Banking Frauds. Reserve Bank of India. Information Technology

I. INTRODUCTION

Cyber Frauds is the main challenging topic to the entire Financial Institutions/Banks which is increasing fast and difficult to control, because the fraudsters are using different new techniques to do the fraud. Many of the Financial Institutions/Banks are Investing more money to protect them. The three sectors of Banking like Public, Private, Co-operative are utilizing different standards or mix standards which are namely International Organization for Standardization (ISO), National Institute of Standards and Technology (NIST), Payment Card Industry Data Security Standard (PCI DSS), Health Insurance Portability and Accountability (HIPAA), Reserve Bank of India Framework, Center for Internet Security (CIS), COBIT (Control Objectives for Information and Related Technology), British Standards etc .In India the CERT-In is the national nodal agency for responding to computer security incidents as and when they occur as specified in IT Act notifications on 16th Jan 2014. The Research paper titled "***Evolution of Cybersecurity Standards in Financial Sectors***" studies how the changes in the rules, guidelines, technologies and hackers mindset has evolved and what is the current scenario. The loss in cyber cases is more that is why this research is more significant which might give a solution to the problem of Financial Institutions/Banks and to their customers.

II. OBJECTIVE OF THE STUDY

1. To study various Cyber Security Standards.
2. To study the Evolution of Cybersecurity Standards.

III. RESEARCH METHODOLOGY ADOPTED

The Secondary data has been used for doing the research and it has been taken from the genuine and renowned websites, Books, Journals, RBI portal, Banks portals, Cyber Crime cell of Police Department in PCMC area etc.

IV. DATA ANALYSIS AND INTERPRETATION

The entire study is on secondary data and is based on literature review, so evolution is a qualitative type of research rather than quantitative.

V. EVOLUTION OF CYBERSECURITY STANDARDS

The cybersecurity standard is a set of guidelines/best practices that organizations can use to improve their cybersecurity.Organizations can use cybersecurity standards to help them identify and implement appropriate measures to protect their systems and data from cyber threats. A cyber security standard defines both functional and assurance requirements within a product, system, process, or technology environment. Well-developed cyber security standards enable consistency among product developers and serve as a reliable metric for purchasing security products. The principal objective of Cybersecurity standards is to reduce the risks, including preventing or mitigating cyber-attacks, which includes tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies.The cybersecurity market size is expected to grow to $345.4 billion by 2026 according to Statista. It is necessary to study the importance of Cyber Security standards too to know how and to what extent it is facilitating the bank customers and Financial Institutes/Banks to protect them from financial loss happening in the current digital world. Cybersecurity standards have existed over several decades and it emerged from work at the Stanford Consortium for Research on Information Security and Policy in the 1990s.The research has focused on which are the different cyber security standards and how and on what basis the evolution has happened in these standards. There are different standards used worldwide, each country as well as Financial Institutes/Banks of these countries are using some of these or mixed standards, or utilizing it at full extent. The goal of cyber security standards is to improve the security of information technology (IT) systems, networks, and critical infrastructures.

The evolution of cybersecurity standards is more significant due to complexity and risk of cyber threats. Due to the tremendous use of technology in recent decades, there is a need for cybersecurity standards to protect against cyberattacks.

The first cybersecurity standards emerged in the 1980s with the development of the Trusted Computer System Evaluation Criteria (TCSEC), also named as Orange Book. The TCSEC established a set of criteria for evaluating the security of computer systems and became the basis for later standards such as the Common Criteria.

In the 1990s, the International Organization for Standardization (ISO) developed the ISO 17799 standard, which provided guidelines for information security management. This standard was later revised and expanded into the ISO/IEC 27001 standard, which remains one of the most widely recognized cybersecurity standards today.

In the 2000s, new cybersecurity standards were developed to address the unique challenges of online security. For example, the Payment Card Industry Data Security Standard (PCI DSS) was developed to protect against credit card fraud, while the Health Insurance Portability and Accountability Act (HIPAA) established standards for protecting the privacy and security of medical information.

The recent development of new technologies like cloud computing, artificial intelligence, and the Internet of Things (IoT) has led to the development of new cybersecurity standards to address the unique security challenges of these technologies. e.g the National Institute of Standards and Technology (NIST) developed the NIST Cybersecurity Framework in 2014 to provide a framework for improving cybersecurity risk management across various sectors.

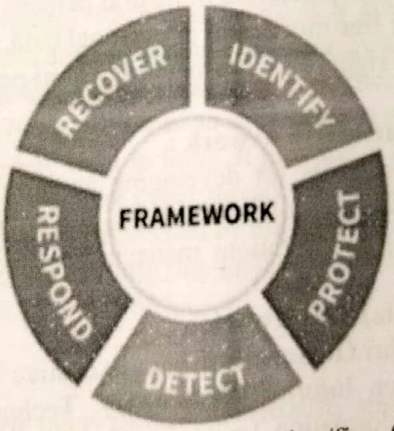
Overall, the evolution of cybersecurity standards has been driven by the need of the time and due to tremendous use of the Internet. So to stay ahead of emerging cyber threats and to provide a framework

for organizations to manage their cybersecurity risks effectively, the financial Institutes use one of the Cyber Security Standards or Mixed Standards to protect their organisation and customers.
The some of the cyber security standards/Frameworks are :

1. NIST Cybersecurity Framework (2013 by US): This is a framework developed by the National Institute of Standards and Technology (NIST) that provides a set of guidelines, best practices, and standards for improving cybersecurity risk management.
2. PCI DSS (2004): The Payment Card Industry Data Security Standard (PCI DSS) is a set of security standards that apply to organizations that handle credit card information.
3. HIPAA: The Health Insurance Portability and Accountability Act (HIPAA) is a set of regulations that govern the security and privacy of patient health information.
4. GDPR: The General Data Protection Regulation (GDPR) is a regulation implemented by the European Union that governs data protection and privacy for individuals within the EU.
5. HIPAA : Health Insurance Portability and Accountability Act dictates how patient data and protected health information.
6. RBI (Reserve Bank of India) Framework (2011) formed Under the Chairmanship of Shri G. Gopalakrishna committee in 2011. (In India)
7. COBIT (Control Objectives for Information and Related Technologies)(1996), created by ISACA (Information Systems Audit and Control Association-a nonprofit organization)
8. Center for Internet Security (CIS) Framework (2008), a nonprofit organization which controls 20 Critical Securities.
9. BSI (British Standards Institution) (1986 in UK) Standards, a standard on IT and Cyber Security.

a) NIST Cybersecurity Framework : is a set of guidelines for mitigating organizational cybersecurity risks, which is published by the US National Institute of Standards and Technology (NIST).
In 2016 US security framework adoption study report says that 70% of the organizations assumes that the NIST Cybersecurity Framework as the most popular best practice for Information Technology.

Functions and categories of cybersecurity activities of NIST :
The NIST Cybersecurity Framework organizes its core part into five functions which are subdivided into 23 categories. For each category, it defines a number of subcategories of cybersecurity outcomes and security controls, with 108 total subcategories. The main five functions are as below



source: https://www.nist.gov/cyberframework/online-learning/five-functions

1. **Identify :**"Develop the organizational understanding to manage cybersecurity risk to systems, assets, data, and capabilities."
2. **Protect :** "Develop and implement the appropriate safeguards to ensure delivery of critical infrastructure services."
3. **Detect** : "Develop and implement the appropriate activities to identify the occurrence of a cybersecurity event."

4. **Respond** : "Develop and implement the appropriate activities to take action regarding a detected cybersecurity incident."
5. **Recover** : "Develop and implement the appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity incident."

For each subcategory, it provides "Informative Resources" referencing specific sections of a variety of other information security standards, which consists of ISO 27001, COBIT, NIST SP 800-53, ANSI/ISA-62443, and the Council on CyberSecurity Critical Security Controls (CCS CSC, now managed by the Center for Internet Security).The cost and complexity of the framework has resulted in bills from both houses of Congress that direct NIST to create Cybersecurity Framework guides that are more accessible to small and medium businesses.

But its requires significant investment for this. Cross-border, cyber-exfiltration operations by law enforcement agencies to counter international criminal activities on the dark web raise complex jurisdictional questions that remain, to some extent, unanswered. The Tensions between domestic law enforcement efforts to conduct cross-border cyber-exfiltration operations and international jurisdiction are likely to continue to provide improved cybersecurity norms.

b) PCI DSS Cybersecurity Framework :

The Payment Card Industry Data Security Standard (PCI DSS) is a widely accepted set of policies and procedures intended to optimize the security of credit, debit and cash card transactions and protect cardholders against misuse of their personal information. PCI DSS standard was released firstly in 2001 with Version 1.0. It came in 2004 by Visa, MasterCard, Discover Financial Services, JCB International and American Express. And with regular updates PCI DSS 4.0 was released in March of 2022.

c) HIPAA Cybersecurity Framework:

The Health Insurance Portability and Accountability Act (HIPAA) dictates how patient data and protected health information (PHI) is protected and to ensure health information is kept secure and patients are notified of breaches of their health data. It was formed in 1996.

d) GDPR Cybersecurity Framework :

The main objectives of General Data Protection Regulation (GDPR) are

1. lays down rules relating to the protection of natural persons with regard to the processing of personal data and rules for free movement of personal data.
2. Protection of fundamental rights and freedoms of natural persons and right to the protection of personal data.

e) ISO/IEC 27001 Cybersecurity Framework :

This Standard includes requirements for developing an information security management system (ISMS), implementing security controls, as well as conducting risk assessments. The Standard's framework is designed to help organizations manage their security practices consistently and cost-effectively.

f) RBI (Reserve Bank of India) Framework :

Under the Chairmanship of Shri G. Gopalakrishna, Executive Director, RBI ,the Reserve Bank, had provided guidelines (2011) on Information Security, Technology Risk Management, Electronic Banking and Cyber Frauds. Information Technology in banks has given recommendations in 9 areas namely Information Security, IT Governance, IT Operations, IS Audit, Cyber Fraud, IT Services Outsourcing, Business Continuity Planning, Legal aspects and Customer Awareness programmes. As per RBI, the Banks were expected to implement guidelines specified in the RBI Framework. The quarterly discussions with banks were planed to get a review of the compliance. Later some of the refinements has been done in RBI Framework in 2016 that the measures suggested in 2011 for implementation cannot be static and banks need to proactively create/fine-tune/modify their policies, procedures and technologies based on new developments and emerging technologies.

g) COBIT (Control Objectives for Information and Related Technology) Framework: It helps organisations meet business challenges in regulatory compliance, risk management and aligning IT

strategy with organisational goals.COBIT (Control Objectives for Information and Related Technologies), was created by ISACA. (Information Systems Audit and Control Association-a nonprofit organization). The latest version of COBIT 2019 was published in 2018.

h) Center for Internet Security (CIS) Framework : a nonprofit organization which controls 20 Critical Securities. (CIS was formerly known as the SANS 20). The CIS focus was to stop the most common attacks. On May 18, 2021, CIS has launched a new version 8.

i) BSI (British Standards Institution) Standards, a standard on IT and Cyber Security

The some of the BSI Standards on IT and Cyber Security are

- BS 10012:2009, Specification for a personal information management system,
- BS ISO/IEC 18043:2006, Selection, deployment and operation of intrusion detection systems,
- BS ISO 22301:2012, Business continuity management systems requirements,
- BS ISO 22313:2012, Business continuity management systems guidance,
- BS ISO/IEC 27000:2014, Information security management systems – Overview and vocabulary,
- BS ISO/IEC 27001:2013, Information security management systems – Requirements,
- BS ISO/IEC 27002:2013, Code of practice for information security controls
- BS ISO/IEC 27037:2012, Guidelines for identification, collection, acquisition, and preservation of digital evidence
- BS ISO 28000:2007, Specification for security management systems for the supply chain
- BS ISO/IEC 27033-5:2013, Information technology. Security techniques. Network security. Securing communications across networks using Virtual Private Networks (VPNs)
- BS ISO/IEC 27033-4:2014, Information technology. Security techniques. Network security. Securing communications between networks using security gateways
- BS ISO/IEC 27033-3:2010, Network security - Part 3: Reference networking scenarios. Threats, design techniques and control issues.

It seems that the BSI has a comprehensive solution to handle cyber threats.

India has implemented several cybersecurity standards and regulations to protect against cyber threats. Some of them are the Information Technology Act, 2000 which is a comprehensive law that governs electronic transactions and cybersecurity in India. It provides legal recognition to electronic documents and digital signatures and includes provisions for cybersecurity, with punishment for cybercrime. The CERT-In (Indian Computer Emergency Response Team) is a government agency responsible for responding to cybersecurity incidents and promoting cybersecurity awareness in India. The guidelines and best practices for organizations have been given to protect their information systems from cyber threats. The third one ISO/IEC 27001: which is an international standard for information security management systems which is widely used in India. It provides a systematic approach to managing sensitive information and protecting against cyber threats. The PCI DSS which is a set of security standards for credit card information. It is mandated by the Reserve Bank of India (RBI) and enforced by payment card networks in India.Along with this Indian government has given the Guidelines for securing IT systems.

VI. FINDINGS

It has been observed that worldwide many of the Cybersecurity standards have been used like NIST-National Institute of Standards and Technology PCI DSS: The Payment Card Industry Data Security Standard, PCI DSS -set of security standards that apply to organizations that handle credit card information. Also the HIPAA-The Health Insurance Portability and Accountability is used. The GDPR: The General Data Protection Regulation which is a regulation implemented by the European Union that governs data protection and privacy for individuals within the European Union. The COBIT get utilized by 7.3% (in 2018). The CIS focus was to stop the most common attacks.BSI (British Standards Institution) seems to be more comprehensive to handle the cyber threats. In India the RBI Framework is doing well to control the Cyber Frauds. India is using or getting help from the

IT Act too for the protection against Cyber threat. The planning and activities of CERT-In in India seems to be satisfactory.

VII. CONCLUSION

It has been seen in this study that worldwide many of the Cybersecurity standards have been used like NIST, PCI DSS, HIPAA, GDPR, RBI Framework, CIS, COBIT, BSI and how the evolution of these has happened as per the necessity. whose ultimate aim is to protect personal information, securing transactions/ credit cards, IT security, and protecting against Cyber Frauds. Many of the organization's/Financial Institutions/Banks are using these or mixed types of standards. The more stringent utilization/compliance of these will secure the organisation and hence their customers too and will protect them from financial loss. To ruin the fraudsters in India the IT Act 2000 is additionally helping along with compliance of RBI Framework. The Cert-In the national nodal agency, is responding to computer security incidents as and when they occur.The function of Cert-In is collection, analysis and dissemination of information on cyber incidents and to forecast, to alert Cyber Security incidents happening and to handle the same. But due to the recent news "CERT-in may be exempted from giving information under RTI Act" in The Hindu dt. March 31, 2023, all planning and activities of CERT-In may get stuck and again Cyber frauds might increase. Here we suggest that RBI and CERT-In have to do frequent amendments in their guidelines, implementations due to use of emerging technologies by fraudsters.

REFERENCES

Book reviews

A. Journals, Articles and News.

1. Cyber Security Standards, Karen Scarfone, Dan Benigni and Tim Grance,National Institute of Standards and Technology (NIST), Gaithersburg, Maryland
2.Deutscher, Stefan & Yin, William & Antonucci, Domenic. (2017). Standards and Frameworks for Cybersecurity. 10.1002/9781119309741.ch6.
3. Tofan, Dan. (2011). Information Security Standards. Journal of Mobile, Embedded and Distributed Systems. 3.

C. Web References:

1. https://www.educba.com/cyber-security-standards/
2. https://cybermagazine.com/cyber-security/history-cybersecurity
3. https://en.wikipedia.org/wiki/IT_security_standards#:~:text=BS%207799%20part%201%20provides,high%2Dlevel%20guide%20to%20cybersecurity.
4. https://en.wikipedia.org/wiki/NIST_Cybersecurity_Framework
5. https://en.wikipedia.org/wiki/IT_security_standards
6. https://www.nist.gov/cyberframework/online-learning/five-functions
7. https://gdpr-info.eu/
8. https://www.rbi.org.in/Scripts/NotificationUser.aspx?Id=6366&Mode=0
9. https://www.iso.org/standard/27001
10. https://www.thehindu.com/news/national/cert-in-may-be-exempted-from-rti-actgovt/article66683021.ece#:~:text=CERT%2Din%20coordinates%20with%20public,vulnerabilities%20as%20guidance%20for%20organisations.
11. https://listings.pcisecuritystandards.org/documents/pci_ssc_quick_guide.pdf
12. https://www.statista.com/statistics/1012729/india-number-of-bank-fraud-cases
13. https://economictimes.indiatimes.com/industry/banking/finance/banking/rbi-brings-in-central-fraud-registry-a-likely-major-gamechanger-for-banking/articleshow/70567463.cms
14. https://www.calyptix.com/hipaa/top-5-cyber-security-frameworks-in-healthcare/
15. https://www.bsigroup.com/en-GB/Cyber-Security/Standards-for-IT-and-cyber-security/