SIMPLIFIED CYBER SECURITY FRAMEWORK

FOR EDUCATIONAL INSTITUTIONS

by

Nagaraja Seshadri

DISSERTATION

Presented to the Swiss School of Business and Management Geneva

In Partial Fulfilment of the Requirements

For the Degree

DOCTOR OF BUSINESS ADMINISTRATION

SWISS SCHOOL OF BUSINESS AND MANAGEMENT GENEVA

November, 2023

SIMPLIFIED CYBERSECURITY FRAMEWORK FOR EDUCATIONAL INSTITUTIONS

by

Nagaraja Seshadri, DBA Research Scholar

Supervised

by

Dr. Mario Silić

APPROVED BY

Dr. Milica Popovic Stijacic, Chair Person

RECEIVED/APPROVED BY:

SSBM Representative

DEDICATION

This dissertation is dedicated to all the temples of learning who want to improve their cybersecurity posture but are not able to find a suitable roadmap that are in accordance with their needs and is within their budget.

ACKNOWLEDGMENTS

My heartfelt gratitude to the dissertation chair of my research and supervisor, Professor Dr. Mario Silic, for the guidance, continuous support, and encouragement during the course of the research.

I sincerely thank Dr. Shinu Abi, Director RACE, REVA University, and Dr. Ramkumar, Mentor, for giving me with the platform to learn and upskill into the cybersecurity domain. I would like to thank Ehack academy and EC council for providing a platform to enhance my knowledge in cybersecurity. I thank my teammates, my clients, and my mentors for their continuous support and motivation in this journey.

I thank the SSBM management and staff for the opportunity to study at this prestigious business school and to all my co-students and colleagues for their support and help during the study.

I wish to thank all the institutions and their staff who contributed with their valuable inputs to this research study. Without their true input of crucial cybersecurity information, my research could not have been meaningful.

To my parents Smt. Nagamani and Late Sri. Seshadri S, who gave me freedom to choose my path very early on, let me deal with challenges and consequences, while still always having my back when I needed them. To my sister, Dr. Uma Seshu and brother-in-law, Dr. Seshu P who were there to guide me through out. Last but not least, I would also like to give special thanks to my wife Ramamani and my daughters Kruthi and Shruthi who have given great support and cheered me up while proceeding towards my research work.

Finally, I want to thank the almighty for giving me the strength to pass through all the difficulties and achieving my dreams. I want to extend my thanks to all others who have directly or indirectly helped me realize this vision.

ABSTRACT

SIMPLIFIED CYBERSECURITY FRAMEWORK FOR EDUCATIONAL INSTITUTIONS

Nagaraja Seshadri

2023

Dissertation Chair: Dr. Milica Popovic Stijacic

Co-Chair: Dr. Minja Bolesnikov

In a broad sense, education is the passing of or transmission of knowledge, skills, and character traits. The education sector can be described as the collection of organizations that provides products and services aimed at enhancing the quality of education in society and includes schools, colleges, and universities and various private institutions like vocational training institutes and coaching institutes. In its entirety, the sector is responsible for training individuals irrespective of their age on new skills, enabling them to obtain meaningful employment, and thus helping accelerate the economic growth.

The institutes face many challenges like containing costs, competition for students, differing views on standardized learning, and adapting to changing economic needs. Forming education partnerships, developing customized and personalized learning programs, and adapting to new technologies are some unique strategies institutions adopt to overcome these challenges.

With online education gaining ground, educational institutes are easy targets for hackers. In fact, reports of instances of breaches in schools and colleges are increasing year on year. These breaches are more worrying because student safety is compromised as educational institutions are entrusted with data of their students and are responsible for their safety and security. A weak cybersecurity infrastructure can make these people vulnerable and put them at risk. With

a proactive approach, it is the right time for them to prioritize security as a focal issue and find a solution for it.

Hence, it is important for the institutes to do everything they possibly can to ensure their IT infrastructure including the applications and systems are protected, and work to overcome any cybersecurity challenges. While various cybersecurity controls are adopted by the educational institutes, there is a need to establish a simple, cost-effective framework specific to this sector. This research is an attempt to shed light on the current state of cybersecurity in the higher education sector and study the problems and challenges they are facing in implementing an effective security system. Based on the inputs from the survey and interviews, EduSec framework is recommended as the probable solution to the cybersecurity needs of the educational institutions.

KEYWORDS

Cybersecurity, Educational Institutions, Framework, Security Breaches, Cyber-attacks, Digital Education, Cyber Threats, Online education, Security Standards, Security Controls.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

LIST OF ABBREVIATIONS

IoT	Internet of Things
IT	Information Technology
CPR	Check Point Research
YoY	Year on Year
CIA	Confidentiality, Integrity, and Availability
ISO	International Organization for Standardization
ICT	Information and Communication Technology
DoS	Denial-of-Service
ICA	Integrity, Confidentiality, and Availability
CEO	Chief Executive Officer
JISC	Joint Information Systems Committee
DDoS	Distributed Denial of Service
BYOD	bring-your-own-device
NIST	National Institute of Standards and Technology
CISO	Chief Information Security Officer
CTI	Cyber threat intelligence
CIS	Center for Internet Security
ISMS	Information Security Management System
ISM	Information Security Management
PII	Personally Identifiable Information
ISMF	Information Security Management Framework
ITIL	Information Technology Infrastructure Library
SANS	SysAdmin, Audit, Network, and Security

PCI DSS	Payment Card Industry Data Security Standard
HIPAA	Health Insurance Portability and Accountability Act
FINRA	Financial Industry Regulatory Authority
GDPR	General Data Protection Regulation
CCTV	Closed Circuit Television
ACL	Access control lists
NA	Not Applicable
WiFi	Wireless Fidelity
MITM	Man-in-the-middle
NOC	Network Operations Center
SOC	Security Operations Center
ID	Identity Document
SIEM	Security Information and Event Management
IR	Incident Response
IIoT	Industrial Internet of Things
SCADA	Supervisory Control and Data Acquisition
HMI	Human-Machine Interface
PLC	Programmable Logic Controller
RTU	Remote Terminal Unit
OT	Operational Technology
SLA	Service Level Agreement
NERC CIP	North American Electric Reliability Corporation Critical Infrastructure Protection
SOC2	Service Organization Control Type 2

CMMI	Capability Maturity Model Integration
CMMI CSF	Capability Maturity Model Integration CyberSecurity Framework
VPN	Virtual private network
AWS	Amazon Web Services
SaaS	Software as a Service
IaaS	Infrastructure as a Service
PaaS	Platform as a Service
EASM	External Attack Surface Management
SSL	Secure Sockets Layer
IP	Internet Protocol/Intellectual Property
CVE	Common Vulnerabilities and Exposures
CVSS	Common Vulnerability Scoring System
SCM	Security Configuration Management
SDPI	Sensitive personal data or information
IAM	Identity and access management
MRA	Mutual Recognition Arrangement
CSM	Continuous security monitoring
NDA	Non-Disclosure Agreement
CMDB	Central Management Database
KPI	Key Performance Indicators

CHAPTER 1

CONCEPTUAL FRAMEWORK

1.1 Introduction

Cyber environments are becoming highly integrated systems, and the need for multi-layered and adaptive security systems is growing. With the expanded reliance on computer systems, the Internet, and wireless network standards such as Bluetooth and Wi-Fi, and because of the growth of smart devices, including smartphones, televisions, and the various devices that constitute the Internet of things (IoT), this field has become significant. Cybersecurity is the protection of computer networks and systems from information theft or unauthorized disclosure, damage to electronic data, hardware, or software, and also protection from the disruption or misdirection of the services they provide (Sharma, 2022). Cybersecurity is a significant challenge because of its complexity, both due to the technology usage and political implications. The goal of cybersecurity is to reduce the risk of cyber-attacks and to protect IT systems, networks, and technologies against unauthorised exploitation. It therefore becomes important to have an excellent cyber security strategy that will help safeguard sensitive information from high-profile security breaches.

These days, it is not just the governing bodies and huge corporations that are usual targets of cyber-attacks, ordinary people, especially children and young adults, are targets as well. This demography is a very vulnerable link in the person technology network (Yan *et al.,* 2018) because of the extended usage of group work (project-oriented activity). In this regard, it is reasonable to exploit the operators' experience of preventing against cyber threats in the field of education (Lavrov *et al.,* 2017). With teaching and learning in the contemporary digital environment, achieving security and safety of the educational process is possible by adapting to the students' activity depending on their cognitive state in digital education and by designing

intelligent individual-oriented systems and services that alleviate human – E-technology interaction (Bykov *et al.*, 2019).

According to CPR, the Education/Research sector endured the highest volumes of cyber-attacks every month in 2022 and in 2021 worldwide. (Check Point Research Team, 2022). The Education/Research sector has seen more than twice the number of weekly cyber-attacks compared to the other industries' average in July 2022. With a 6% increase compared to July last year and 114% increase compared to July two years ago, this sector had an average of almost 2,000 attacks per organization every week. Such attacks have had devastating consequences as in the case of Lincoln College, which shut down on May 13 2022 after it suffered a ransomware attack. The attack was the final straw that contributed to their decision to shut down after 157 years in the field.

India is among the top 5 countries to have seen very high cyber-attacks in the education sector (Check Point Research Team, 2022). As per the report, digitisation of education, and prevalence of online learning platforms along with wide adoption of remote learning are key triggers that enlarged the attack surface. The trend shows that developing countries are seeing higher YoY increase in cyber-attacks. Expanding education technology market, population growth and increasing digital penetration in developing countries seems to be contributing to this trend. To combat the disruption caused by the ongoing Covid-19 pandemic, schools, universities, and related entities adopted remote learning. There was also large-scale digitisation of educational content, student data and documents. Since then, online learning platforms are increasingly being used to cater to the needs of everybody ranging from preschool children to retired professionals. These are among the major reasons listed behind the increase in cyber-attacks as per the report.

There are not many standard indicators to measure the economic effect of a cyber-threat; nevertheless, evidence exists that for educational institutions, a cyber-attack could be disastrous. Companies and governmental agencies are equipped to act with standard countermeasures. But educational institutions need a more specialized approach due to their peculiar nature and organization. Therefore, instead of using general frameworks, we suggest a cyber-security paradigm specifically created for this sector. Our goals are to identify the priorities, minimize the controls, simplify the language, and keep the attack surface as small as possible. In brief, we propose a customized cyber security framework for educational institutions that, we think, will have a direct effect on the protection of the institution's data and on the safeguards of institutions and students' privacy: two essential pillars for the competitiveness and success of the institution.

1.2 Problem Statement and Justification

While it is evident that there are numerous standards and guidelines for business organizations and governmental agencies to implement cybersecurity, they are very expensive for a budget strapped educational institute. Also, because of the unique nature of the organization and the IT setup of the educational institutes, this sector requires a specialized approach.

Educational institutes are very vulnerable to cyber threats because of the limited or lack of security controls adopted by them. Due to the sensitive data they hold, any successful cyber-attacks they may face is a serious risk. It is necessary to understand the challenges these institutes are facing especially in the implementation of cybersecurity controls. Using a well formulated research survey conducted by the authors, this research thesis throws light on the current cybersecurity controls implementation posture in the education sector, along with the challenges they are facing that are hindering them in deciding, planning and implementing cybersecurity controls. The research uses the analysis of the survey data and the core concepts

of cybersecurity to propose a recommended framework as a possible solution for educational institutes.

1.3 Objectives

The main objective of this study is to determine what challenges educational institutes face while implementing cybersecurity program and recommend the best possible cybersecurity controls.

To achieve the main objective, these specific objectives are considered:

1. To identify the challenges and gaps in the existing cybersecurity practices that the educational institutes face in implementing an effective cybersecurity program.
2. To study the existing cybersecurity standards or frameworks and understand their usefulness and limitations with reference to educational institutes.
3. To come up with a cyber security paradigm specifically created for the educational sector. This will involve identifying the priorities, minimizing the controls, simplifying the language, and keeping the attack surface as small as possible.
4. To propose a customized cyber security framework for educational institutions.

This research should lead to a better understanding of the challenges faced by educational institutions in implementing cybersecurity controls and recommend a simplified and budget friendly framework customized to this sector and thereby help them secure their data.

1.4 Scope of the Study

This research considers higher education institutes in India. Though there is a vast difference in the way the institutes in urban and rural areas look at cybersecurity, the research has not differentiated between these. Schools, coaching institutes, and vocational training institutes are currently out of scope of the study. The research establishes the current cybersecurity position

of the participating institutes. This information is internal to the organization and confidential, hence it is difficult for the management to share.

1.5 Significance of the Study

The term Cybersecurity, according to the ISO definition, means maintaining the Confidentially, Integrity and Availability of information in cyberspace which is made up of entities that connected to the internet. The term information security means the protection of data as an asset from cyber threats and vulnerabilities. Cybersecurity is the protection of cyberspace, along with all assets contained within the cyberspace (Bay, 2016). It is also important to understand that cyberspace is made up of not just entities linked to the internet, but also those that communicate with each other using the internet. Which essentially means cyberspace is a subgroup within Internet. Cyber assets also known as ICT can be both tangible and intangible. Information, data, intellectual property (IP), reputation, service, software programs and applications are all intangible assets. Hardware like the storage media, equipment, machines, and users' are examples of tangible assets (Ozier, 2010). Asset value is determined based on the importance of the asset to the organization and may change over a period of time. CIA triad is a common method to determine asset value based on the cost, sensitivity, and criticality of the asset. Sometimes the amount of maintenance required and the effort for the same is also additionally considered during asset valuation (Fisch, 2000). Some of the security concerns that affect cyberspace are viruses, unauthorized access, data theft, DoS attack, financial fraud, abuse of wireless network and systems, sabotage, and website defacement (Fenz, 7 2005). Relationships between physical entities, applications, systems, people, and processes determine the character of the cyberspace. Hence it is clear that cyberspace is nothing but the people, processes and underlying technology and their interaction with each other and the internet (Daras, 2018). This study is aimed at understanding the ground-level difficulties that educational institutes face in protecting their cyberspace. The survey is used to determine the

cybersecurity implementation statistics in the education sector and try to comprehend the gaps. Inputs are also taken from various existing research literature available to date. The objective of this study is to find any hidden indicators that will help the institutes articulate their problems and offer simplified and relevant solutions.

1.6 Structure of the Thesis

This thesis is divided into nine major chapters.

Chapter One involves introduction to the research, which delves into the scope, background, and nature of the study. This chapter further defines the research problem, its purpose, objectives, significance and aims.

Chapter Two is a summary of the literature review that the author studied as part of the research process. This section identifies major works that are relevant, highlights significant research and most importantly identifies the gap in existing literature. This research will try to reduce or close that gap.

Chapter Three deals with the approach taken for this research. It covers the qualitative research approach and data gathering method used in this research. The section will also provide insights into how the semi-structured interview questions were formed along with the nature of these questions.

Chapter Four lays out the high-level findings of the research and analysis of the data collected along with the inferences. It also documents the exploratory data analysis done and the results.

Chapter Five discusses the results of the analysis in detail to arrive at an interpretation.

Chapter Six gives comparative study of a few important cybersecurity frameworks in use.

Chapter Seven deals with the recommended Cyber Security Framework for the Educational sector. It also highlights the advantages of this framework against the existing standards.

Chapter Eight deals with the step-by-step implementation methodology recommended for the framework.

Chapter Nine provides the conclusion of this research. It contains the final findings, the caveats of the study, its limitations, practical applications, and recommendations for further research.

CHAPTER II

LITERATURE REVIEW

2.1 Introduction

While referring to existing literature, we have gained considerable understanding on the cybersecurity-related problems faced by educational institutions. We have also tried to summarise few common cyber-threats faced by the educational institutes. Further, we have reviewed some of the existing cybersecurity standards, frameworks, and concepts, followed by few concerns about the same which might be impacting decisions for implementation of those by educational institutions.

2.2 Cyber Threats in Current Times

The world, at present is experiencing an exponential growth in cyberspace (Bykov, Burov and Dementievska, 2019). This extraordinary growth in information access provides ample opportunities to those with malicious intentions. Protecting the data and making the cyber world safe is the need of the hour (Arora, 2016). Cyber security is the act of protecting the systems and technologies from unusual activities. Cyber security essentially means maintaining the 3 important factors - Integrity, Confidentiality, and Availability (ICA) of computing assets of an organization. These assets may be within the organization or connecting to another organization's network. It is not just the rising rate of cybercrime, but also its varied and diverse characteristic features that is the source of concern. Cyber-crime is a term that covers a wide scope of criminal activities performed using computers. Performing criminal act using cyberspace as the medium of communication is referred as Cybercrime (Harpreet, 2013). As a result of rapid globalization, easy access to Internet and low cost of mobile phones, there is a huge increase in cyber-crimes. Cyber bullying and cyber defamation are some of the common cyber-crimes that are rapidly increasing.

Study by The Identity Theft Resource Center found that the number of data breaches in 2022 are hitting a new high and that is after a record-setting 2021. And more than 90% of data breaches are cyberattack-related. Data breaches in quarter 1 increased when compared to that of the previous year for the third consecutive year (www.securitymagazine.com, n.d.).

President and CEO of the Identity Theft Resource Center, Eva Velasquez, said "Quarter 1 generally sees the minimum number of data compromises reported each year. But the fact that the number of breaches in quarter 1 has seen a double-digit increase over the same period last year is an indicator that data compromises will continue to rise in 2022. And this is over and above the all-time high that was seen in 2021. As mentioned in 2021 Annual Data Breach Report of the Identity Theft Resource Center, there has been an alarming number of data breaches in 2020-21 due to highly complex and sophisticated cyberattacks that are fuelling the dramatic rise in identity fraud. Thus, it is imperative that everyone continues or starts to practice good cyber-hygiene. This applies to both businesses and consumers and will help reduce the amount of personal information from flowing into the hands of cyberthieves."

Among the Internet-based technologies, cyber security threats are the most negative outcomes, and they have become the major challenge of recent years (Mantha and de Soto, 2019). Covid-19 pandemic has increased use of technology many times over and has intensified this negative outcome, forcing many companies around the world, both public and private (i.e., unregulated), to examine the strength of their cyber security vis-à-vis their risk exposure (Carr, 2016). These threats are broad and diverse. They include, for example, phishing attacks, which are threats aimed at fooling people into clicking on links or opening attachments that may cause a malicious software to be installed on their computers, thus exposing them to leaks of sensitive data from their devices (Pienta, Thatcher and Johnston, 2018). Ransomware attacks is another prevalent threat. These are characterized by the installation of ransomware viruses. The

malware is often installed on endpoint computers of the organisation, where it tries to exploit an application's vulnerabilities to leak critical or sensitive data to the attackers through the Internet. The malware employs an encryption method that renders the company's data unavailable or inaccessible until the ransom money is paid to the attackers (Anghel and Racautanu, 2019). In addition, IoT devices like smart manufacturing equipment and web cameras, security systems, networking devices like switches and routers, that are operated by the company are also exposed to cyber-attacks. These attacks are usually executed by "black-hat hackers" (Kwon and Shakarian, 2018) According to Kaspersky, these black-hat hackers are "criminals with malicious intent breaking into computer networks. They also tend to release malware that destroys files, steals passwords, credit card numbers, and other personal information, or holds computers hostage" (www.kaspersky.com, 2023). The stolen data may lead to further penetration of the company's databases in order to steal additional sensitive information which can then be used to extort money.

2.3 Importance of Cyber Security in Education Sector

Cyber-attacks increased 50% Y-o-Y on corporate networks in 2022. The Education and research sector experienced the highest volume of attacks in 2021, according to Check Point Research, with an average of 1,605 attacks per organisation every week. This shows a staggering 75% increase from 2020.

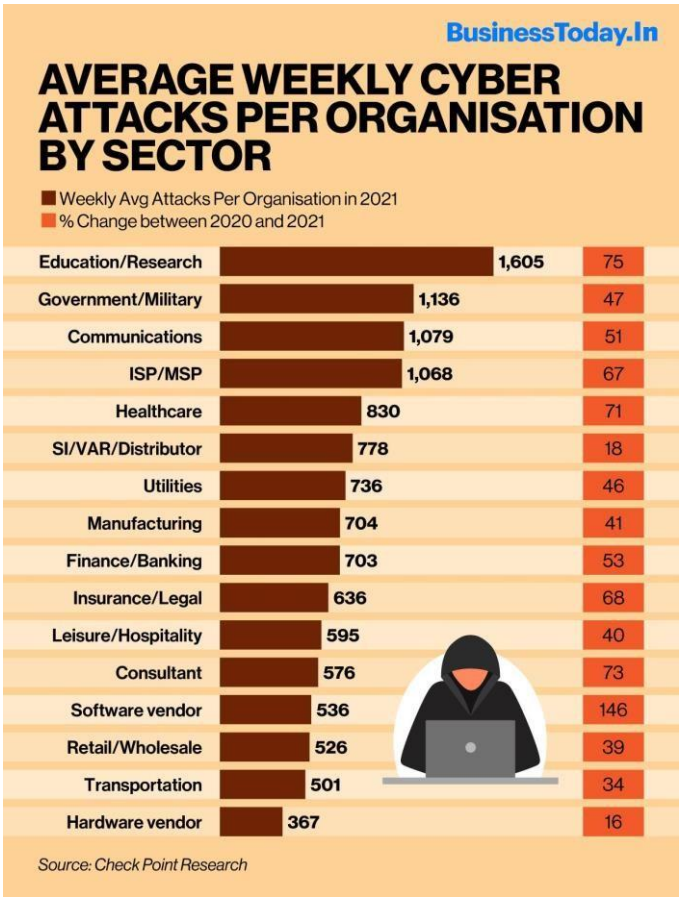

Figure 2.1: Checkpoint Research – Average Weekly Cyber-attacks per organization by sector

(Check Point Research Team, 2022)

Why Hackers choose educational institutions for cybercrime:

The motives for attack vary with the size, purpose, and stature of the educational institutions. Hence it is important for these institutions to evaluate the risk and understand which data is vulnerable to unauthorized access. They should be very concerned about Cyber Security in their systems that house data on students/staff and their research.

- **Data theft** – One of the major types of cyber-attack affecting all levels of educational institutions is Data theft. In this type of cybercrime, the hacker usually hacks the system that houses the student and staff data, including sensitive details like names and addresses that the institutions hold, and uses them for their advantage.

- **Financial gain** – Financial gain is another major motive for hackers. It is done by targeting the fees paid via an online portal, often large sums of money that covers a whole term or year of tuition which are transferred without proper protection.
- **Espionage** – Higher education institutes like Universities and College often possess valuable intellectual properties and these are a big lure for hackers. Universities/Colleges need to be suitably protected to keep these safe.
- **Lack of awareness** – Lack of awareness is among the major reasons for cybercrimes. It may be because, the staff or students are not aware of cyber security or due to lack of knowledge on the use of security systems.

How is the Education sector targeted?

A survey by JISC's 2018 on the cyber security posture questioned IT professionals in the education sector to name the top cyber threats facing their institutions. Below are the top three answers that were given:

- **Phishing** – Phishing is a scam that takes the form of an email or instant message which was designed to trick the user to trust the source in a fraudulent attempt. After gathering the access details, like sensitive student data or confidential research, they tear the poor security patch. These days, this is the most common technique of cybercrime.
- **Ransomware/Malware** – Ransomware and malware attacks can prevent authorised users from accessing the network or files. In brief, Ransomware or malware normally infects devices using a file or attachment disguised as a standard program called a Trojan.

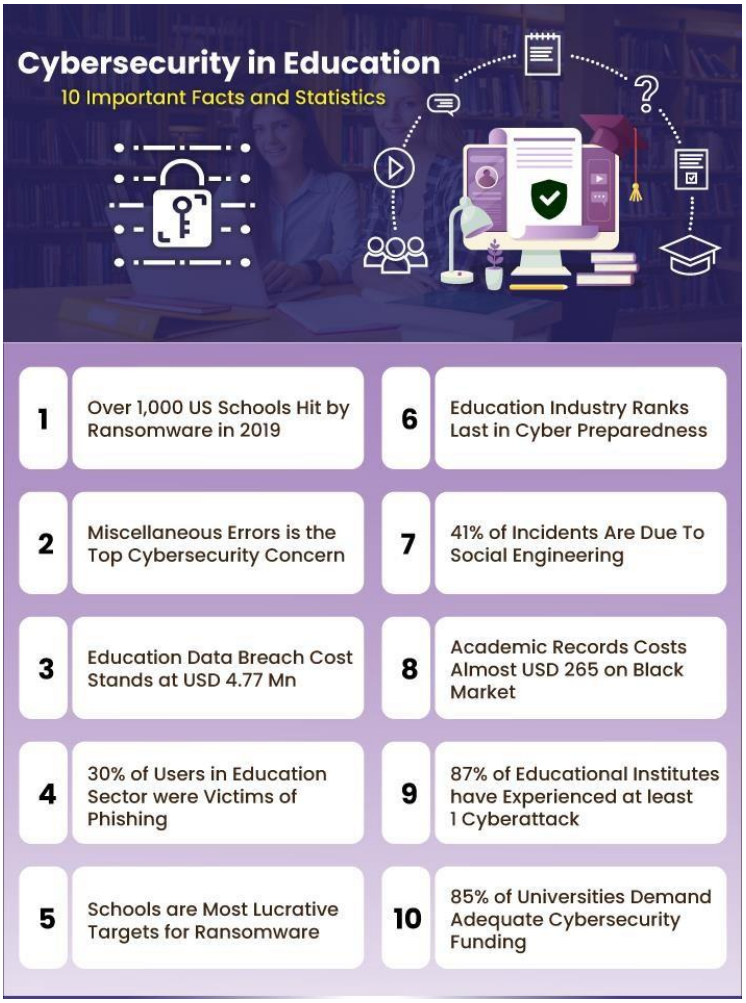

Figure 2.2: Cybersecurity in Education – Important facts (Stealth Lab, 2021)

- **DDoS attacks** –Distributed Denial of Service or DDoS attacks are among the common kind of attacks in Education venues. This is generally an easy attack even for an amateur cybercriminal to carry out, specifically if the target network is not properly protected. The motive may be as simple as wanting a day off to protesting the way a complaint was handled.

The most targeted section of the population is the young children and the youth, who are affected by the perilous consequences of electronic media. Broadly, the cybercrimes are classified as Type I and Type II. A single event from the viewpoint of the victim is generally a Type I cybercrime. In contrast, Type II cybercrimes refer to on-going series of events,

involving frequent interactions with the target (Harpreet, 2013). Some such activities are computer related frauds like cyber defamation, child predation, cyber harassment, travel scam, fake escrow scams, blackmail, stock market manipulation, identity theft, extortion, credit card frauds, email spoofing, software piracy, complex corporate espionage, newsgroup scams, health care, insurance/bonds frauds, auction frauds, non-delivery of merchandize, salami attacks, data didling, sabotage, web jacking, spamming, DoS, forgery etc. It also includes major international threats like planning or carrying out terrorist activities. We are currently living in a tech-savvy world and that world is rapidly evolving because of the advancement in digitization. Today, no sector is immune from the threat of a cyber-attack, and this includes schools and universities. This sector has become a vulnerable platform for cyber-hacking because of the extent of data that is available in the educational institutions as well as the increasing number of interconnected devices that are used. Because of the complexity of networks today, and the threats to their security, traditional anti-virus solutions are definitely not enough anymore. Cyber security is hence no longer considered as just an IT issue, it should be approached holistically throughout all the sectors and treated as a collaborative effort to diminish the threat.

Educational and healthcare records are among the most sought-after information by cybercriminals. For the hackers, these sectors provide extremely high levels of financial gain. Due to this reason, many educational organizations have been victims of cyberattacks. Research IPs are extremely valuable to higher educational organizations, and it is very much essential to protect them by adopting the correct technology. The rapid rise of attacks in the last year serves as a warning to the administrators of these institutes. The institutions should recognize the necessity for investing in and implementing proactive strategies for cybersecurity. Many organizations are unprepared for cyberattacks today, many of who remain

unprepared even after an attack. Hence it is importance for the organizations to implement the necessary technology to avoid future attacks before a breach can occur.

A sizable number of total data breaches across different industries come from this one sector which is an indication of the seriousness of cybersecurity in education. The education sector is lagging in terms of technology adoption, at the same time has a user base of people who are very much susceptible to attack. This makes educational institutes an easy target for cybercriminals, who continue to attack schools and colleges to gain valuable information and data to sell to their advantage.

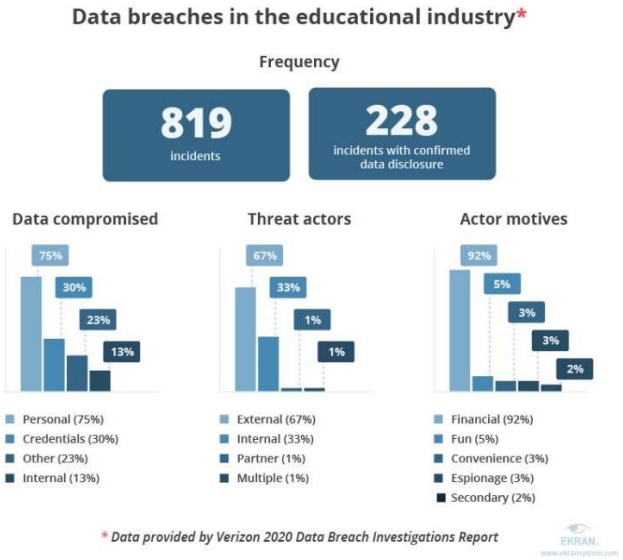

Figure 2.3: Data breaches in Education sector 2020 (www.verizon.com, 2020)

The increasing number of security breaches experienced in recent years by educational institutions epitomises the importance of confidentiality, integrity, and availability of information in universities. Insufficient protection often leads to incidents of data breaches, putting students' sensitive information at risk along with an institution's reputation. According to the Verizon 2020 Data Breach Investigations Report (Figure 2.3), the educational services industry suffers from phishing attacks, malware via websites, and miscellaneous errors (Ekran, 2020).

According to research by Check Point Software Technologies (Check Point Software, 2022), in 2022, the education and research sector was one of the top targets for cyber attackers. It has seen an average of 1605 attacks per organization per week, and this is a 75% increase from 2020 (Sharma, 2022). The educational sector has seen a major shift to distance learning. Online educational also means a large number of students, staff, and external one-time users access the systems from remote locations, which broadens the exposure, raising cybersecurity risks. Diverse learners who demand more than just traditional classroom-based experiences and this has pushed the educational sector to explore information systems and technology like never before. Course delivery models are now a blend of face-to-face elements with Webinars, e-Learning, and other online digital content (Johnson, 2007). According to Liz Miller, a Constellation Research analyst, the education sector is a very easy target for cyber-attacks since educational institutions do not prioritized cybersecurity. Pandemic forced educators into being accidental CIOs. Institutions suddenly had to upgrade to new technologies, and this had to be done both on-prim and remotely too. Attackers released that institutions do not get as much attention for their IT system updates as other critical sector like financial or medical institutions (Sharma, 2022).

In 2004, Foster wrote that '…related to computers, universities are among the least secure places in the universe' (Foster, 2004). Fifteen years later, Joint Information Systems Committee (JISC) in the UK conducted penetration testing which highlighted that there is a 100% chance of gaining access to the most valuable data in an institution within a couple of hours through spear phishing (Chapman, 2019). Universities operate with multi-stakeholder, open-by-design (Chapman, 2019), transient and decentralised platforms that are generally associated with technology, research, and innovation. Students, academics, staff, and visitors regularly access universities' IT infrastructure to consume and produce data, in a multi-modal fashion: from personal mobile phones and smartwatches (bring-your-own-device, BYOD), through corporate

laptops and tablets, to laboratory sensors and swipe access card systems, the data exchange among universities as organisations and their different categories of end users is continuous.

With their expanded digital footprint in the universities, there is an increase in their vulnerability to security breaches, and this requires constant efforts in the field of security and privacy. Altogether, the educational environment seems to have a naturally unique relationship with information security and its layered approach, rigid architecture, and centralised governance (Borgman, 2018); (Hina and Dominic, 2018). Most universities usually do not have the resources required to provide centralised security services; hence they go for partial outsourcing of information security (Chapman, 2019); (Liu, Huang and Lucas, 2017). This enables efficiency and effective response to cyber-breaches, but on the other hand it enlarges academic institutions' digital footprint that requires adequate governance and security management. Due the different degrees of cybersecurity knowledge and practices in the universities, training initiative is quite challenging (Lane, 2007). This aspect is aggravated by the traditionally high turnover rate and by a general complacent attitude towards information security (Elham Rajabian Noghondar, Konrad Marfurt and Bernhard, 2012). From an attacker's viewpoint, times when universities seemed not to own any attractive asset are long gone: from computational power (used, for example, to mine cryptocurrencies, or to launch distributed-denial-of-service attacks) through personal data (for example, students' social security numbers in the US), to research data and intellectual property, universities are rapidly climbing hackers' interest lists (P. Riquelme and Román, 2014).

2.4 Generic Standards and Frameworks in Cyber security

Evaluation of threats and risks is generally done based on the probability of them causing unwanted events with a certain amount of damaging capacity (Shetty *et al.*, 2014). In case of the cyber world, cyber risks are perceived mainly as those that cause damage to the company's

information or technology in a way that might lead to future claims of neglect by suppliers, customers, or their own employees (Naumov and Kabanov, 2016). These risks may vary from just causing minor business disruptions to loss of money to affecting the reputation of the company. The organization's information system is connected to the internet by means of its servers, endpoint computers etc, that communicate with the external and internal devices. These enable data communications from and to the organization and supports its business activities. Because the organization's computers and network elements are connected to the Internet, they expose these companies to cyber risks. This has forced the companies to update their cyber protection policies and hire cyber experts who are responsible for mitigating the cyber vulnerabilities (Amin, 2019). Cyber defence technologies that are part of the cyber security control implementation plans that appear in frameworks such as NIST 800-53 and ISO 27001 (Mailloux, *et al.*, 2016) help in carrying out risk mitigation. But these frameworks only serve as guidelines, and it is the Chief Information Security Officers's job (CISOs) to ensure that a balance is struck between cyber security activities necessary to pursue the company's business and the prevalent cyber security governance best practices (ieeexplore.ieee.org, n.d.). Cyber-crimes generally happen because of negligence and lack of awareness among users (Schneier, 1993); (Albrechtsen, 2007). As per recent research (Jasper, 2017) the US has introduced threat intelligence frameworks to gather information from diverse sources and that must be carefully examined by experts. Besides this, machine learning techniques also help analyse threats, which is then used in responding to attack incidents (Thomas, Vijayaraghavan and Emmanuel, 2020). National Cyber Security Strategy 2016–2021 is introduced by the United Kingdom (von Solms and van Niekerk, 2013) and has assigned £1.9bn for the Cyber Security Programme (Office, 2016). Close to 70 nations have national cyber/information security strategies to address this issue. They also have noteworthy legislations explaining their cybersecurity defence strategies (Pipyros *et al.*, 2018). The cyber network guide details the

preplanning of vulnerabilities. This includes the judicious information exchange on the threats and will lead to protection of various entities like business, environment, infrastructure (Fiedelholtz, 2021).

Cybersecurity is often defined as a comprehensive term (www.iso27001security.com, n.d.). In a generalized term, cyber security is that which helps prevent cyber-attacks and can aid in cyber risk management. The Security architecture defines the two types of security attacks: active and passive, and also security objectives (Stallings and Hall, 2005).

Our intent is to study the various frameworks available for cybersecurity risk management and propose an easy-to-implement, cost-effective one for the education sector. In this regard, we have researched few of the widely used cybersecurity frameworks and come up with their usefulness and also their limitations.

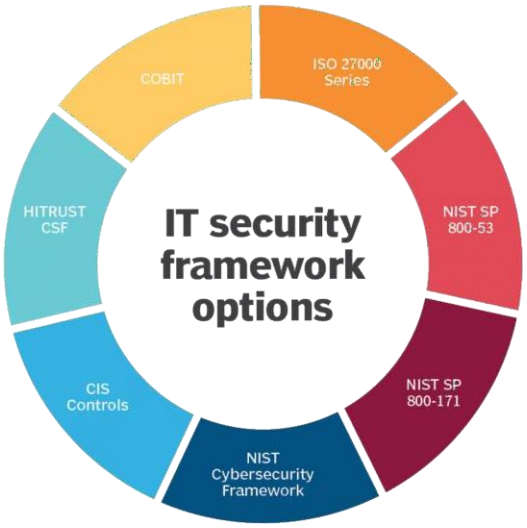

Figure 2.4: Common Cybersecurity Frameworks (Satori, n.d.)

The Cybersecurity Framework by The National Institute for Standards and Technology (NIST) is among the widely accepted approaches to facilitate cybersecurity risk management within organizations. Clearly recognising that the activities associated with managing cybersecurity

risk are specific to each organization is one of the important aspects of the NIST Cybersecurity Framework. It also recognizes that while an organization is evaluating cybersecurity risk management, it should be done on the cost–benefit basis. Being intentionally broad and flexible, this framework also provides a macro-overview of how organizations should approach cybersecurity risk management but leaves the details of the implementation to each organization (Krumay, Bernroider and Walser, 2018). It considers cybersecurity risks within scope of the organization's overall risk management process and thus directs that the cybersecurity activities should be guided by business. This framework addresses cybersecurity, including cybersecurity's effect on physical, cyber, and people dimensions in a very flexible way. The three major components of the framework are: the Framework Core, the Framework Implementation Tiers, and the Framework Profiles. Each of these components emphasizes the connection between business or mission drivers and cybersecurity activities (NIST, 2018). Each organization has unique cybersecurity needs, and to account for this, the framework is very flexible and can be used in a wide variety of ways. The decision on how to apply or use the different components of this framework is left to the implementing organization. Being flexible and comprehensive enough that it can cater to a variety of organizations also makes it difficult or too elaborate to implement in an educational institution which requires a simpler, ready to implement and use framework.

Another useful framework is the Cyber threat intelligence (CTI). This framework analyses information about the intent, also taking into account the capabilities and opportunities of adversaries in cyberspace, and hence making it a valuable resource for organizations. It also helps all the stakeholders in the cybersecurity process such as incident responders, security operations team members, network architects, and high-level decision makers, all of whom should be prepared for variety of threats challenging their organizations. CTI has been evolving as a mechanism to detect, respond, and prevent cybersecurity.

Another important framework is the CIS Controls. CIS controls is a set of 20 controls. This framework has the best ratio between resources spent on security protection and the gains realized by lowering the risk (Groš, 2021). CIS Controls goes with the basic idea that, much information is available on the net on information protection that it becomes contra-productive and hence less secure. To remedy this situation, CIS recommends having a single source of information and implementing a cut-down version of the proposed (CIS Controls, 2014) This seems good in theory, but with the kind of diverse information infrastructure, practically impossible.

2.5 Challenges for Educational Institutions

Figure 2.5: Cybersecurity: 6 worst performing sectors (Verizon, 2020)

Verizon, in their 2020 Data Breach Investigations report, out of 20 sectors the educational establishments experienced sixth highest number of cybersecurity incidents with 819 instances. When it comes to educational organizations, the information they possess is extremely sensitive and grows every year because of increased implementation of technology. Hence it is simply not feasible to safeguard it in a server that may not have enough protections which are commonplace in current times in highly rated data centres.

Most standards and guidelines for information security refer to either government agencies as discussed in the Federal Information Security Management Act of 2002 or large corporations as described in the Business Software Alliance's "Information Security Governance: Toward a Framework for Action," or TechNet's "Corporate Information Security Evaluation for CEOs". These guidelines are helpful in that they provide a useful starting point for educational institutions but will be difficult to introduce and implement because of issues of language and emphasis as well as complexity. For example, the information security governance assessment tools stress phrases such as "impact of downtime on revenues" and "expansions, mergers and acquisitions, new markets". These are not relevant in the educational world. Also, there will be issues of fit because of the very large degree of decentralization in many large educational institutions. In addition, all these guidelines would be much more effective in educational institutions if there were some additional motivations specific to the sector.

ISO 27001 is one of the most widely used standard for the overall cybersecurity of any organization, which prescribes and helps an organization establish and maintain their Information Security Management System (ISMS) (Beckers *et al.,* 2014); (www.iso27001security.com, n.d.). NIST is another one providing valuable framework for Cybersecurity. This has five core functions - "Identify", "Protect", "Detect", "Respond" and "Recover" (Eerikson, *et al.,* 2019). Along with these, there are many different standards, concepts, and frameworks for Cybersecurity – if successfully implemented, it not only lowers the cyber threat risks but also gives recognition as a cyber-matured organization.

But these frameworks are complex and costly (Wirht, 2017) which prevents it from being successful in the educational sector. Security needs are different for each sector. Each organization has unique requirements, and those requirements change over time. Security risks can be reduced by implementing right controls with the help of framework that focusses on the specific threats faced by these institutes (Jawarneh et al., 2021). Because of the budgetary

constraints faced by the institutes cost and ease of implementation will help their adaptation of security frameworks. In this regard, our goal is to develop a simplified cybersecurity framework for educational institutions.

2.6 Cyber Security Standards for Educational institutions

As discussed earlier, the education sector is now seeing tremendous amount of data breaches. Limited budget is one of the many challenges that the institutes face and hence very few educational institutions are prepared for potential cyber-attacks. These institutions usually need multiple software to secure their data along with multiple licenses for servers. Many of the institutes do not have the capacity or the purchasing power to deploy the security software needed in their institutes. This makes the education sector very vulnerable and prone to cyber-attacks. Besides, educational institutions, even if they know their security requirements, face major challenges in choosing the right security solutions for their environment. Due to the minimum amount of information and research to map Open-Source Security Software solutions to certain controls is limited today, choosing the right solution to cover a certain control is challenging. Educational institutions have limited resources and budget which will curtail their investigation to determine the suitable security solution required. Institutes may be aware of the software needed to secure its environment but may not have the budget or the investment capacity for such software (Shamma, 2018).

It is important that the security of the institute is not compromised due to limited financial budget. Complicated and expensive security solutions can be substituted with cost-effective and simple as well as ready to be deployed solutions, so that they get on the right security track. Sometimes just implementing the right policies and processes can improve an organization’s security posture multi-fold (Shamma, 2018).

There are various frameworks currently in the market for organisations to adopt and improve the effectiveness of their cybersecurity. These frameworks support actions at both an individual and organisational level (Aloul, 2012). Aloul (2012), in his study on 'the need for effective information security awareness' highlights that for any security improvement program to be the successful, students and staff should be trained and educated on information security. Security awareness trainings must be included in the risk assessment plan and should be adopted at all levels including staff, students, teachers, and all administrative employees (Aliyu, *et al.*, 2020). Security aware front-end users will serve as the first line of defence against cyber-attacks (Evans, *et al.*, 2019).

Security Framework	Description
National Institute of Standards and Technology (NIST) Cybersecurity Framework	Cybersecurity framework with five core areas: Identify, Protect, Detect, Respond, Recover (U.S. Department of Commerce, 2020). Both government and publicly-traded organizations follow this framework in their cybersecurity function.
Cloud Security Alliance (CSA) Cloud Controls Matrix	Framework of security controls for cloud computing environments that map to other frameworks such as NIST, Payment Card Industry Data Security Standards (Payment Card Industry Data Security Standards, 2021).
ISO 27001 Information Security Management (ISM)	International framework providing requirements for an information security management system (ISMS), enabling organizations to manage financial information, intellectual property, employee details or information entrusted by third parties (ISO Information Security Management, 2021).
Control Objectives for Information and Related Technology (COBIT)	Technology management framework by the Information Systems and Control Association (ISACA) to help businesses implement robust and controlled information management and governance strategies.

Table: 2.1: List of cybersecurity frameworks in education sector (Adam C, 2021)

Educational institutions are a unique set of organizations with their own specific needs with their focus mainly on education and research. As other organizations do, they also depend heavily on information technology for their day-to-day activities. As per ISM (information security management, data in education institutions is considered as a very high-value asset This includes teaching and learning data, research data, administrative data, and cultural data and these are very sensitive in nature (Gonzalez-Martınez, *et al.*, 2015). Institution members should take effective steps to secure their data as that is the target for most cyberattacks and threats (Carlton, *et al.*, 2017). Between 2005 and 2014, 324 educational institutes were attacked with 562 data breaches reported and most of these where research institutes (63%) (Dahlstrom and Bichsel, 2014). These breaches in an educational institute could negatively impact their

reputation as well as their finances (Ponemon, 2017). Despite these, the education industry is very slow to patch with only 18% of vulnerabilities addressed in a 12-week patch cycle (Smyth, 2017). If there is an attack on an educational institute, the effect is not just loss of PII or personally identifiable information belonging to students and employees, but also threat of exposure and misuse of research data. The impact may be operational, reputational, or financial or all of them. There may also be national security and privacy concerns if the institute is involved in government research projects. Because of this, educational institutes need good information security planning, education, and training in the overall Information Security Management Framework (ISMF). The educational institutes are facing challenges in finding an applicable ISMF (EDUCAUSE Review, n.d.). System management, institution policies, information security culture awareness, IT outsourcing, data backup policy, etc are all the factors that affect the choice of (Eloff and Eloff, 2005). Educational institutes will have to adhere to the institution's laws and regulations while implementing and enforcing security policies, procedures, and standards to safeguard and secure their information assets. There are many frameworks already in existance for various industries like ISO 27000 (Disterer, 2013), COBIT (Khther and Othman, 2013), ITIL (Tso, n.d.), CIS controls (Center for Internet Security, 2019), NIST (Newhouse, *et al.*, 2017), very few cater specifically to the Educational Sector.

2.7 Summary

The study shows that ISO 27000 is the most prevalent framework in academic institutions. It is also to be noted that, besides ISO 27000, the institutes usually implement a hybrid solution using specific controls and validation methods. Recently there has been some work going on in this regard and a few new frameworks like EDUCAUSE and COBIT are making the rounds. But the traditional ISO and NIST are still the most implemented frameworks for ISM in educational sector (Merchan-Lima, *et al.*, 2020).

Figure 2.6 below shows the IT Security spending trend as reported by the SANS institute. While this does not mean that spending on these exact technologies is right for every organization, it does suggest the order of importance for organisations on average. This can serve as a good starting point in deciding which elements of cybersecurity should be the focus.

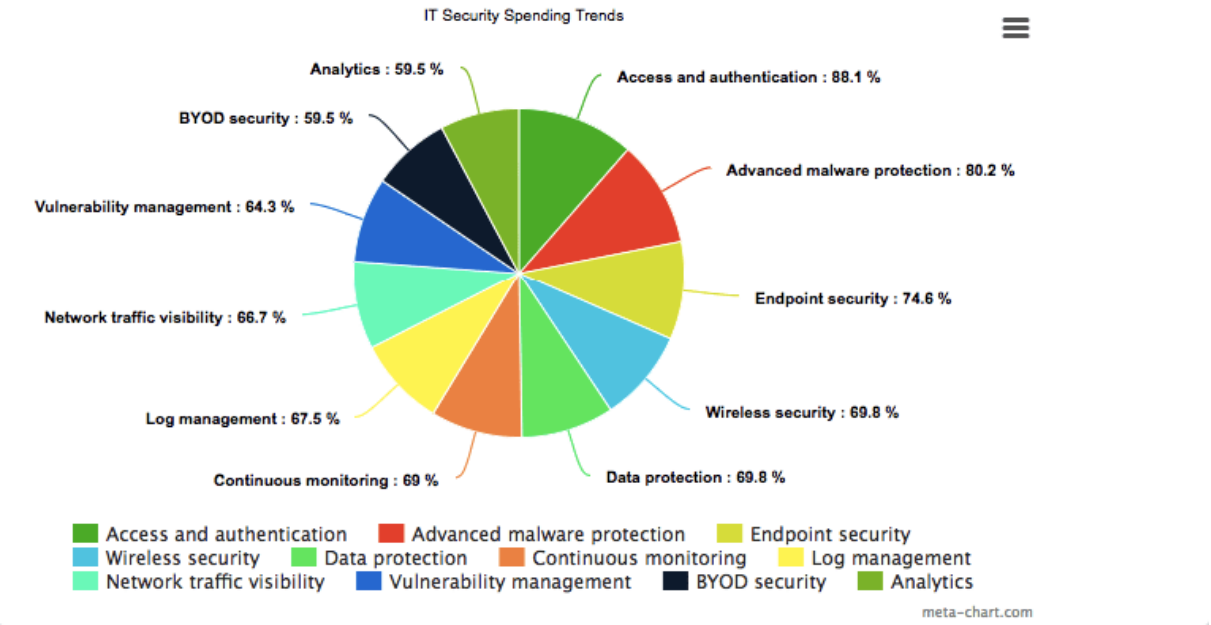

Figure 2.6: IT Security Spending Trends (www.stickmancyber.com, n.d.)

There is no limit to the availability of information on cybersecurity and its core concepts. And this helps in determining gaps and recommending solutions in the later sections.

CHAPTER III

RESEARCH METHODOLOGY

This section of the research proposal will discuss the research methodology that was used for our study.

3.1 Research Design and Data Collection

Research design is the blueprint of the research. It addresses the following issues: what questions should the research study; what data is relevant to the research and should be collected; who is target population for data collection; how the data is collected; and how is the data analysed.

We have used survey research, a quantitative method where researcher collects responses to a set of predetermined questions from a sample of individuals or an entire group. Survey using a comprehensive questionnaire is employed in this study for collection of data regarding IT infrastructure and the cybersecurity controls that are currently present in educational institutions. There are also questions to understand the awareness levels of the staff and student community as well as any breaches faced so far. Survey research is among the best data-collection methods to use when the goal is to gain a representative picture of the characteristics of a large group.

Suitable participants for this survey are chosen as top management, directors, and heads of institutions along with the IT department heads as they have insights about the internal cybersecurity posture of the institute. Also, participant institutes are chosen across various states of India and spanned across categories. The target population were reached through various ways such as messaging, emails, etc. This research survey is created to get important understandings on the status of institutes' cybersecurity as well as the key problem areas that are encountered while planning and implementing cybersecurity controls. This gives the

research multiple viewpoint on the cybersecurity adoption status by educational institutions, thus providing better understanding of the issue under study.

To understand the current cybersecurity posture in the educational sector the authors conducted the research survey with a few key questions like –

- "How old is the Institute?"
- "Does the Institute currently have any of cybersecurity standard or framework implemented?"
- "Does the Institute have its security control in place?"
- "What is the frequency of Security awareness trainings for the staff?"
- "Which is the biggest problem faced while implementing or deciding/planning to implement Cybersecurity Control for the Institute?"
- "Has the organization undergone any cyber-attack?"
- "What is the expectation from security standard or framework specifically as an educational institute?

This survey helped in getting a good understanding on the current cybersecurity posture in the education sector. It also gave a good measure of the current problems and awareness levels survey results were analysed. After analysing the results, a tailored cybersecurity program that will remedy the highlighted concerns based on existing basic cybersecurity ideas is proposed.

One limitation of the survey was the number of respondents to the questionnaire. Though a few hundred institutes' top management were approached, not all of these institutes voluntarily participated in this research survey as it touches sensitive internal cybersecurity posture-related information. To circumvent the problem of skewed sampling, the author chose the responses from different categories of institutes in terms of size and location from both professional and

non-professional sectors. The aim of the sampling was to obtain reliable data about determinants.

The questionnaire was kept simple so that the participant would not have to spend too much time answering. The questionnaire tried to capture all aspects of the IT infrastructure and its spread, the kind of cybersecurity controls in place, the security awareness level among the users and touches the budgetary and other constraints. The questionnaire was divided into two parts. The first part focuses on the demographics of the institute including the category, the size etc. The second part focuses on the IT infrastructure and the cybersecurity controls in place.

Research survey questions and their purpose is detailed below:

Q1. How old is the Institute?

Age of the participant institute has a bearing on the depth of understanding of business maturity concerning cybersecurity, hence a question was asked regarding this. The representative was asked to choose any of the following options:

(a) 0 to 5 years

(b) 5 to 10 years

(c) 10 to 20 years

(d) Over 20 years

Q2. Has institute adopted any standards or frameworks?

Many standards and frameworks are being adopted by organizations globally. To check which of those are adopted by participant institutes, the survey provided the option to choose from among the following:

(a) ISO 27001

(b) NIST Cybersecurity Framework (CSF)

(c) COBIT 5

(d) CMMI

(e) SOC2

(f) GDPR

(g) Others (specify)

If the institute was using any other framework that was not listed, a textbox was provided for the input with the “Other” option.

Q3. Does the institute use any security controls?

The survey captured input to identify any security controls that the institutes have already implemented. Sometimes, institutes may be using individual controls without adopting any standard framework. Hence, irrespective of the answer to question 2, the participants were asked to answer this question. The survey provided three options for this:

(a) Yes

(b) No

(c) Maybe

Q4. What are the Physical security controls used in the institute?

This information is quite sensitive, and institute may be reluctant to share, but since it is important to the research, it was asked. The participants were told to choose multiple options if required from the following:

(a) Fences

(b) Gates

(c) Guards

(d) Security badges

(e) Access cards

(f) Biometric access controls

(g) Security lighting

(h) CCTVs

(i) Surveillance cameras

(j) Motion sensors

(k) Other

This question was asked to understand what kind of physical security the institutes had. A text box against the 'Other' option was available to enter any other control that was not listed and 'NA' if no physical controls were implemented.

Q5. What Technical Security controls are implemented in the institute?

This information was again very sensitive in nature but was important to understand the security state of the institute. The survey asked the participant institutions to choose any or multiple options from among the following:

(a) Access control lists (ACLs),

(b) Anti-virus software,

(c) Authentication solutions,

(d) Firewalls,

(e) Encryption methods,

(f) Others

This question was asked to understand if the institute had any technical security controls in place. A text box against the 'Other' option was available to enter any other control that was not listed and 'NA' if no technical controls were implemented.

Q6. Does the institute have any Administrative controls implemented?

This information is very sensitive for the institute but was important to be captured during the survey, hence was asked the participant institutions could choose from among the below options. They could choose more than one option.

(a) Security Policies

(b) Security Procedures

(c) Security Guidelines

(d) Other

A text box against the ‘Other’ option was available to enter any other control that was not listed and ‘NA’ if no administrative controls were implemented.

Q7. What is the frequency of Security awareness trainings for the staff?

The most vulnerable part in any security framework is the people. Hence it is important to train them on security awareness and this is one of the many ways to be cyber secure. Hence, the survey determined this by asking the above question and providing the below options to be chosen as an answer-

(a) Never

(b) Yearly

(c) Every Six Months

(d) Every Three Months

(e) Every Month

(f) Other

The survey provided the ‘Other’ option along with a text box to capture any other input related to security training that was not be present in the options.

Q8. Are there any appropriate mechanisms so that staff/students can report suspicious emails quickly and effectively?

It is vital to have processes and procedures in place so that staff and students report any untoward incident without delay, hence this question. Options given were:

(a) Yes

(b) No

(c) Maybe

Q9. Does the staff and students understand the risks of using public WiFi?

Public WiFi is among the most vulnerable fragment of an organization's cyber security framework. But it is an inevitable part of any educational institute. Hence, the user is required to understand the risks involved in using this. This question was asked to see the awareness level of the staff and students in the institute. Options given were:

(a) Yes

(b) No

(c) Maybe

Q10. Is there any manpower with Cybersecurity knowledge to identify the risks and threats?

It is essential for the institute to employee people with good Cybersecurity knowledge in the IT department so that they can identify and mitigate any risks. Options given were:

(a) Yes

(b) No

(c) Maybe

Q11. Is Data backup taken regularly?

Taking regular backup of institute's data is the best contingency policies in case of an attack. Options given were:

(a) Yes

(b) No

Q12. Is backup data encrypted?

Encrypting the institute's data is the best ways of securing it. Options given were:

(a) Yes

(b) No

Q13. Is data classified by sensitivity and risk?

Not all data requires the same kind of security protocol. It is essential to understand the sensitivity and accordingly provide required security controls. Hence classification of data based on its sensitivity becomes important. Hence this question. Options given were:

(a) Yes

(b) No

Q14. Has the institute under gone any cyber-attack?

The survey tried to understand from the participants if they had faced any cyber-attacks. This question helped to understand the seriousness of problem. The options provided were:

(a) Yes

(b) No

(c) Maybe

In continuation, the survey tried to identify the kind of cyber-attack that was faced by the institute. The choices were provided from the common kinds of attacks encountered in the

sector. But also gave the ‘Other’ option along with a text box for any other input. The participants were advised to enter ‘NA’ if they had not faced any attack.

(a) Insider Threats

(b) Ransomware

(c) Malware Attacks

(d) Web Attacks

(e) Phishing Attacks

(f) Man-in-the-middle (MITM) Attack

(g) Denial-of Service (DoS) Attack

(h) Other

Q15. Is network traffic monitoring done on a regular basis through NOC/SOC for any malicious traffic?

Any security system is successful only if there is continuous monitoring, hence the participants were asked this question. Options given were:

(a) Yes

(b) No

(c) Maybe

Q16. What is the biggest challenge faced by the institute while deciding and/or implementing Cybersecurity Controls?

The survey tried to capture this information to understand all the problems and challenges the institutes were facing while planning and implementing cybersecurity implementation. This was a very important input for the research. Multiple options were provided from among the general challenges and the respondents were allowed to choose as many of the relevant options. Below were the options provided:

(a) Huge cost involved in implementing standard Cybersecurity controls.

(b) Difficult to decide the controls that suit the institute's requirements.

(c) Lack of skilled resources to implement and maintain.

(d) Other businesses take priority.

(e) No clear roadmap to invest in the cybersecurity program.

(f) Available cybersecurity standards or frameworks take very long to implement and realise gains.

(g) Other

The survey also provided the 'Other' option along with a text box to capture any other input related to problems they faced but were not listed.

Q17. Is there any security roadmap, to review regularly against the overall IT roadmap strategy?

With the cyber scenario changing at a very fast pace, institutes should have a futuristic roadmap on cybersecurity that aligns with the overall IT roadmap. Hence this question. Options given were:

(a) Yes

(b) No

Q18. Is IT security operations outsourced?

Many of the organizations do not manage their IT infrastructure and their security on their own. They outsource the operation to third parties who specialize in this area. This will reduce the burden on the organization, though it may work out expensive in some cases. Options given were:

(a) Yes

(b) No

Q19. Is there any methodology to handle Data privacy and Protection?

This was an open question where the participants were asked about the way they handle data, its privacy and protection like encryption, access control etc. The responses would help understand the level of Data security awareness as well as how effectively it is protected in an institute.

Q20. What are objectives that the institute wants to achieve by implementing security standards or framework?

This was an open question that was asked to understand their expectations from cybersecurity standards or frameworks. This provided the foundation for the solution the study recommended. The research discusses in-depth on this topic in the upcoming sections.

3.2 Target Population and Sample

The research contributors were selected from diverse higher educational institutions such as Engineering and technological colleges, Management institutes, Universities of higher education from field of humanities, commerce, and pure sciences. The survey was used to gain insights into the current state of cybersecurity in the institutes, information regarding any cyber threats or data breaches that these institutes may have faced, and such sensitive internal information. Due to the sensitive nature of the information sought, there was predictable reluctance to participate by some institutes. However, we got an adequate quantity of responses that helped provide the required insight.

Table 3.1 shows the actual response received from the participating institutes versus the total sample size selected for this research. While survey questionnaire was sent to 300 institutes, only 150 volunteered information and participated in the study.

Category	Total Samples	Responses
Engineering/Technical college	55	36
Management Institute	47	30
Medical College	53	24
Multi-disciplinary College	68	20
Multi-disciplinary University	77	40
Total	300	150

Table 3.1: Survey sample and actual responses category wise

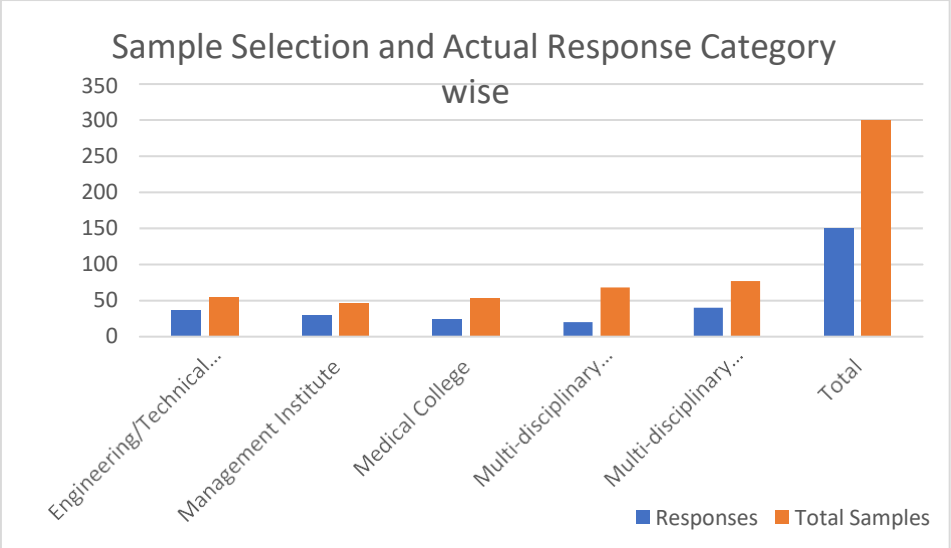

Figure 3.1: Survey sample and actual responses category wise

Segment	Total Samples	Responses
Aided	82	48
Government	120	36
Private	98	66
Total	300	150

Table 3.2: Survey sample and actual responses segment wise

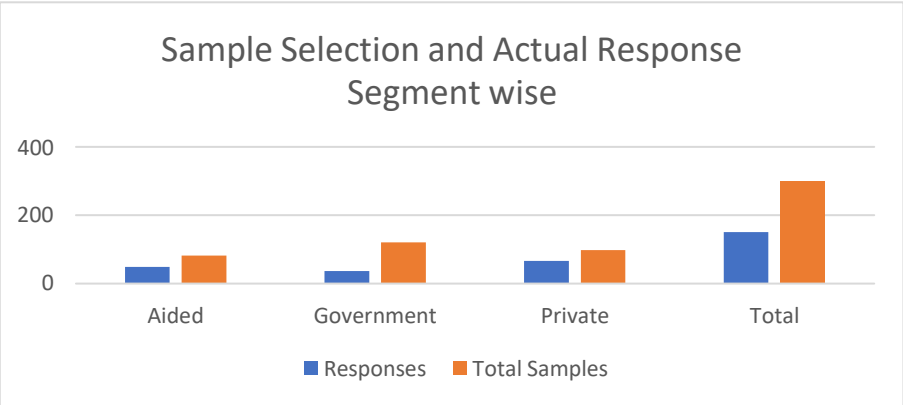

Figure 3.2: Survey sample and actual responses segment wise

Age	Total Samples	Responses
0-5 years	65	34
5-10 years	85	60
10-20 years	64	32
above 20 years	86	24
Total	300	150

Table 3.3: Survey sample and actual responses institutes' age wise

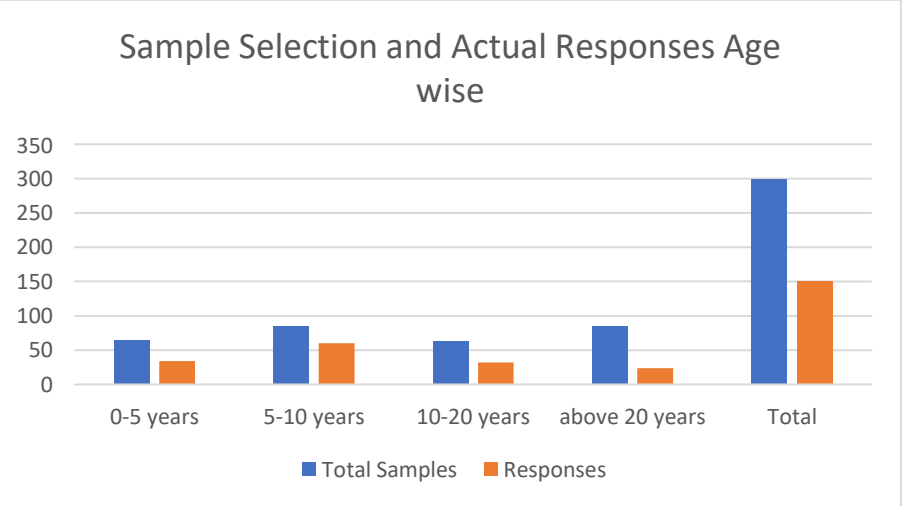

Figure 3.3: Survey sample and actual responses institutes'age wise

Table 3.4 shows that maximum responses were received from Multi-disciplinary Universities, followed by Engineering/Technical Colleges.

Category	Count	Percent
Engineering/Technical college	36	24%
Management Institute	30	20%
Medical College	24	16%
Multi-disciplinary College	20	13%
Multi-disciplinary University	40	27%
Total	150	

Table 3.4: Category wise Participation

Segment	Count	Percent
Aided	48	32%
Government	36	24%
Private	66	44%
Total	150	

Table 3.5: Segment wise Participation

Age	Count	Percent
0-5 years	34	23%
5-10 years	60	40%
10-20 years	32	21%
above 20 years	24	16%
Total	150	

Table 3.6: Age wise Participation

3.3 Data Collection Process

The design of the survey questionnaire was done with the objective of getting information from the participating institutes with minimum time and effort. With an easy and simple format, the participants were able to understand and answer within a few minutes. Most of the questions had multiple options to choose from and made answering easy. A free text option was provided where necessary to capture additional information or any other inputs that were not listed in the options. Questionnaire was in a digital format and the participant submitted the answers online. The participants were given a timeframe to complete the questionnaire and submit their

responses. Data was then extracted in tabular format for further analysis. In the later part of the research, telephonic and face-to-face interviews were also conducted. This interview data was captured as notes and then converted to digital format.

	Type	Segment	Age	Q2	Q2a	Q3	Q4	Q5	Q6	Q7	...	Q16a	Q16b	Q16c	Q16d	Q16e	Q16f	Q17	Q18	Q19	Q20
0	Engineering/Technical college	Government	0-5 years	No	None	Yes	Yes	Yes	Yes	Once Every Six Months	...	No	No	No	No	No	No	Yes	Yes	NaN	NaN
1	Multi-disciplinary University	Aided	5-10 years	No	None	No	Yes	Yes	Yes	Once Every Six Months	...	Yes	No	Yes	Yes	Yes	Yes	No	Yes	NaN	NaN
2	Multi-disciplinary College	Private	10-20 years	Yes	ISO27001	Yes	Yes	Yes	No	Never	...	No	No	No	No	No	No	Yes	No	NaN	NaN
3	Management Institute	Government	above 20 years	No	None	No	Yes	No	No	Never	...	Yes	Yes	Yes	Yes	Yes	Yes	No	No	NaN	NaN
4	Medical College	Private	0-5 years	Yes	CSF	Yes	Yes	Yes	No	Never	...	Yes	No	No	Yes	No	Yes	Yes	No	NaN	NaN
...	...	...	...	...	...	...	...	...	...	...	...	...	...	...	...	...	...	...	...	...	...
145	Multi-disciplinary University	Aided	5-10 years	No	None	No	Yes	No	No	Never	...	Yes	Yes	Yes	No	Yes	Yes	No	No	NaN	NaN
146	Multi-disciplinary University	Aided	above 20 years	No	None	No	Yes	No	No	Never	...	Yes	Yes	Yes	Yes	Yes	Yes	No	No	NaN	NaN
147	Multi-disciplinary University	Aided	10-20 years	No	None	Maybe	Yes	No	No	Never	...	Yes	No	No	Yes	Yes	Yes	Yes	No	NaN	NaN
148	Multi-disciplinary University	Aided	5-10 years	No	None	Maybe	Yes	Yes	No	Never	...	Yes	Yes	Yes	Yes	No	Yes	No	No	NaN	NaN
149	Multi-disciplinary University	Aided	0-5 years	No	None	Maybe	Yes	Yes	No	Never	...	Yes	Yes	Yes	No	Yes	No	No	No	NaN	NaN

150 rows × 29 columns

Figure 3.4: Snippet of data collected and tabulated

3.4 Data Analysis

Data analysis deals with identifying patterns to extract insights that help in decision making. Once the data was collected, tabulated, and analysed, the author established patterns and gained inferences. These insights were then used for recommending the appropriate cybersecurity approach for the educational institutes.

Microsoft Excel and Python tools were employed for data analysis. Pivot tables were created in excel and responses were analysed in detail to decipher patterns and trends. It was then converted into graphical format for better understanding and easy interpretation. Python was used for exploratory data analysis that helped in understanding the data. This also helped

understand the significance of all the factors and predictive analysis was carried out using logistic regression to understand the probability of cyber-attack.

3.5 Limitations of Research Design

This research was designed and conducted to understand the internal cybersecurity controls implemented in the institutes and problems and challenges involved and risks faced. As this was sensitive information, over 50% of the institutes declined to participate. Around 300 institutes were approached for the survey but only 150 participants volunteered information for this research. This research was restricted to higher educational institutes as these were expected to have elaborate IT infrastructure. Also, the survey mostly targeted IT heads, directors, and owners, getting their valuable time was a challenge.

3.6 Conclusion

Below is the summary of steps that were followed during the research process:

- We reviewed the interrelations of the cybersecurity concepts in the various existing standards.
- We developed a questionnaire to assess the current state of policies for cybersecurity enforcement in educational institutions.
- We conducted a survey using this questionnaire, and then collected and analysed the data.
- We analysed the current state of cybersecurity standards from various organisations.
- We identified the open issues and challenges faced by the institutions.
- We identified the cybersecurity practices that was required to be developed because of the dynamic and socio-technical nature of the educational institutions and came up with a framework optimal for the education sector.

The study throws light on the existing cybersecurity controls in the educational institutions, and the threats and breaches they have faced. Using a well-designed research survey, this study provided us an opportunity get inputs from top educational institutes that helped us understand their current cybersecurity posture along with the problems they are facing relate to cybersecurity controls. Though the cybersecurity of an organization is very important, the participation in the survey was average, as only 150 institutes out of 300 voluntarily took part in this survey. IT personnel of 50 institutes shared direct inputs by joining in the research interviews during the solution design. It is to be noted that participation may not have been very enthusiastic as the information being collected was very sensitivity in nature.

CHAPTER IV

RESULTS

In this chapter, we will discuss the results from the survey of the educational institutes from different domains and segments. Their survey results helped understand both the good things and the pain areas as it applies to cybersecurity implementation in the institutes.

4.1 Age of the Institute

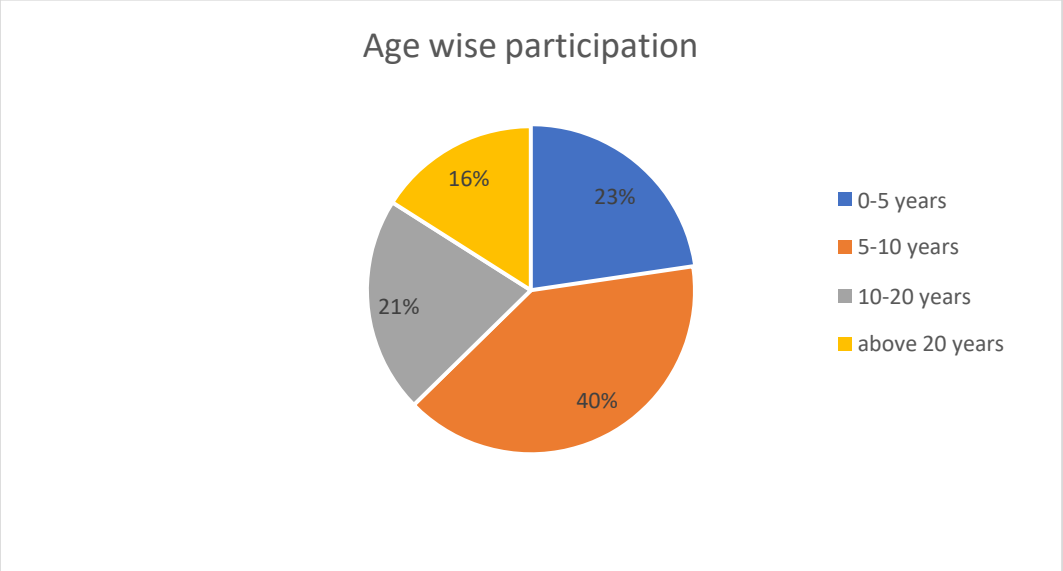

Figure 4.1: Age wise Participation

Survey analysis revealed that age of the institute played a significant role in the way they participated in the survey. It is interesting to note that only 16% of the older institutes responded. 5-10 years old institutes constituted majority of the respondents. Newer institutes and the slightly older (10-20 years old) were average in their participation. Older institutes seemed to be more reluctant in responding to the survey. This was probably due to lack of awareness or interest among the stakeholders. Newer institutes were more forthcoming in sharing their knowledge and experiences.

Institutes in the 5-10 years age group (around 40%) were among those that voluntarily participated in this important survey, as depicted in Figure 4.1. Additionally, more than 23% of institutes that were less than 5 years old and 21% in the age group of 10-20 years took part. As seen in the above table it was the older institutes over 20 years that seem reluctant to participate. Below figure 4.2 shows that institutes in the age group of 5-10 years are most likely to have security controls in place. This correlates with the participation figures too.

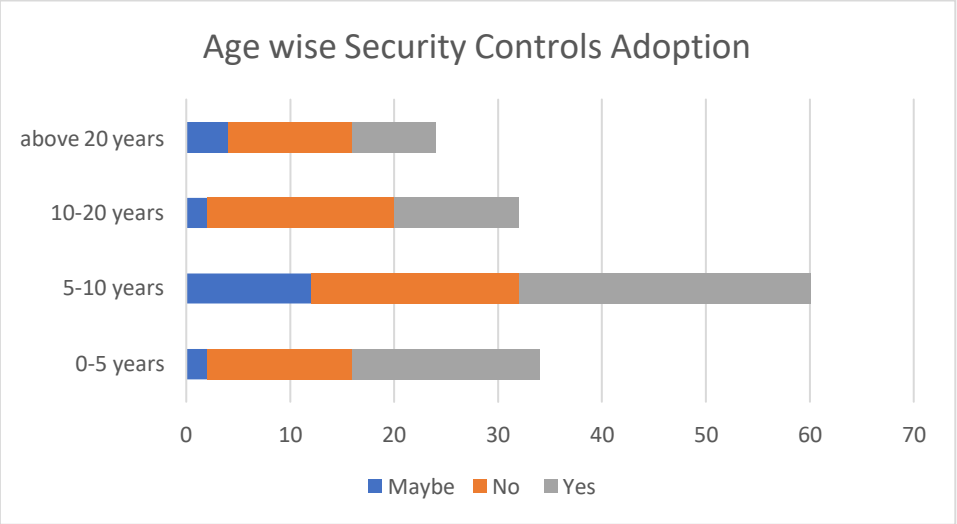

Figure 4.2: Age wise Security Controls Adoption

4.2 Category of the Institute

The type of institute is another attribute that was analysed extensively and seems to have a bearing on the responses received and the level of security that is in place. As can be seen, Engineering/Technical and Management institutes have responded well for the survey. Multi-disciplinary Colleges are the least responsive.

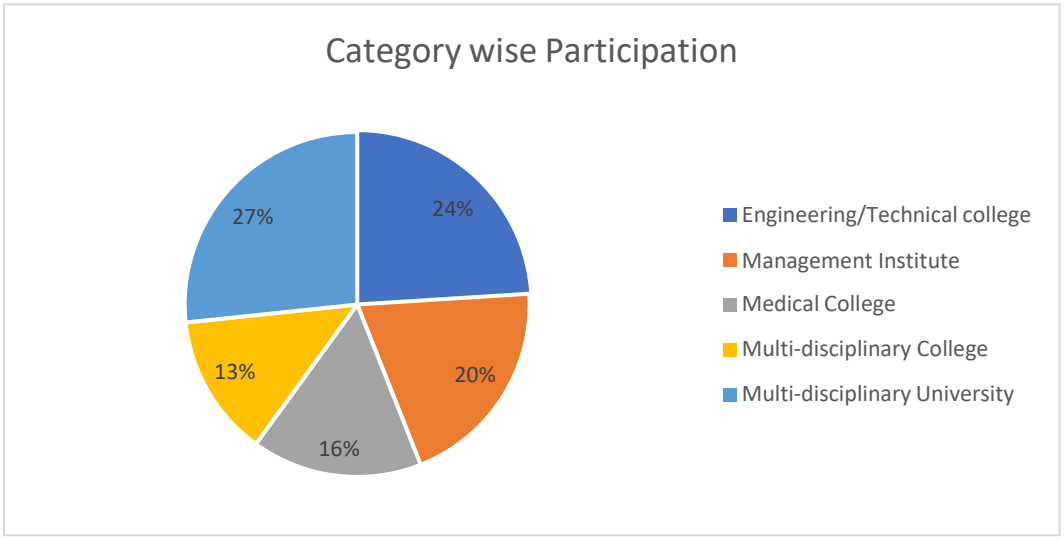

Figure 4.3: Category wise Participation

Percentage participation wise, it is in the Engineering/Technical colleges followed by multi-disciplinary universities that responded well. Medical and multi-disciplinary colleges were comparatively reluctant to answer the survey. This demonstrates that the technical institutes were more in tune with the innovations in technology and were more adaptive. They were also the ones that have security controls in place.

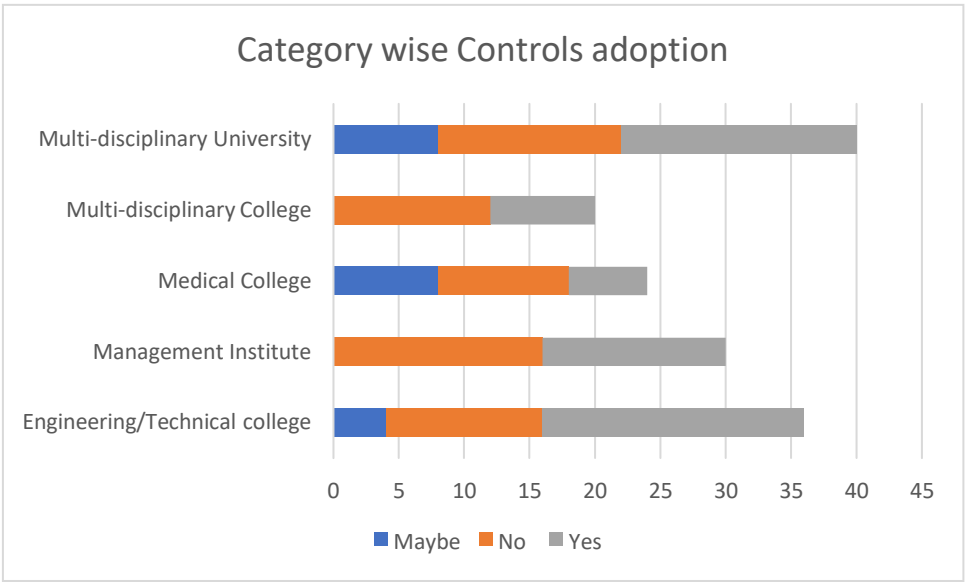

Figure 4.4: Category wise controls adoption

4.3 Segment of the Institute

The governing body and the funding for running the institute decides the segment of the institute. Government institutions are funded and run by the government, Aided institutes are partially or fully funded by the government but run by a private body though they follow all the rules and regulations of the government. Private institutions are both funded and run by private bodies and have their own rules and regulations. The table below shows that the private institutions were more responsive for the survey followed by the aided colleges.

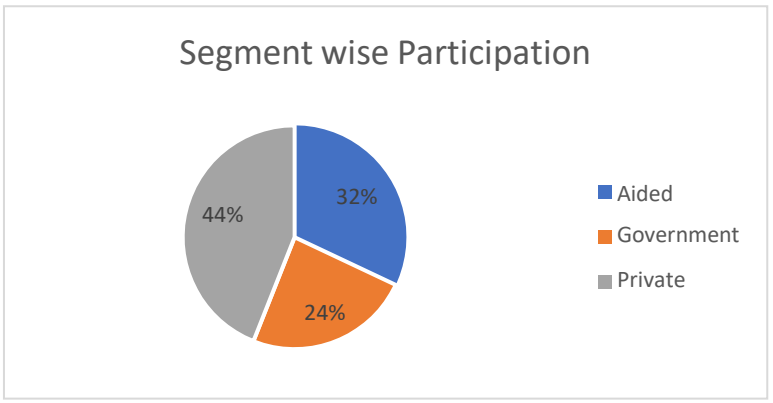

Figure 4.5: Segment wise Participation

When it comes to adaption to security controls too, it was the private sector that fared better than the other two segments. This likely because of the availability of funds and also because the implementation would not have too many bureaucratic hurdles.

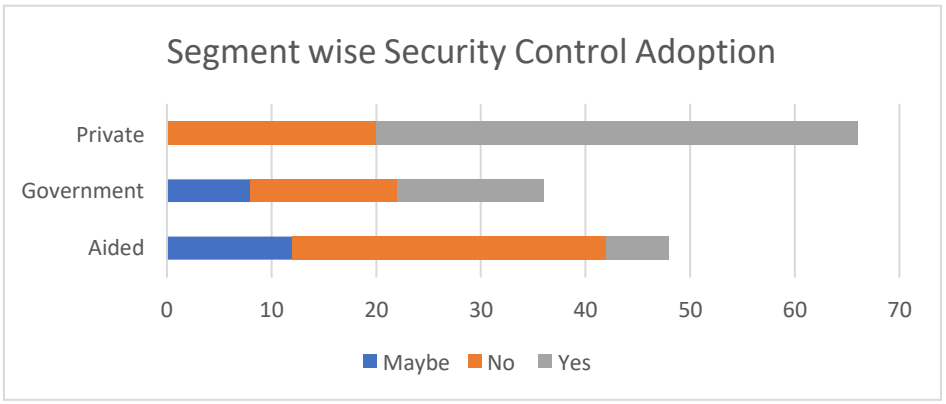

Figure 4.6: Segment wise Security Controls Adoption

4.4 Current State of Security Preparedness

Physical Security	Count	Percentage
No	4	3%
Yes	146	97%
Total	150	

Technical Security	Count	Percentage
No	66	44%
Yes	84	56%
Total	150	

Administrative Security	Count	Percentage
No	116	77%
Yes	34	23%
Total	150	

Table 4.1 Current state of security preparedness

Table above show that over 97% institutes have some kind of physical security in place. This includes Gates, Fences, Security Guards, Security badges etc. 56% have some kind of technical security in place which includes Access cards, Biometric access controls, Security lighting, CCTVs, Surveillance cameras etc. When we did a deeper analysis on these, it was noted that most of them were limited to Access cards and CCTVs. Though access cards were used at the doors of some sensitive areas like computer labs and document libraries, it was found to be easily surpassed by students and staff alike.

Very few, about 23%, have some kind of Security policy in place. This includes Security Policies, Security Procedures and Security Guidelines. Table 4.4 shows that approximately 77% of the institutes lack administrative cybersecurity controls, leaving them vulnerable to cyber threats. There must be good reasons that are preventing them from adopting these controls. Below tables and charts show these institutes' distribution by type, segment, and Age.

Category	Count	Percent
Engineering/Technical college	8	24%
Management Institute	14	20%
Medical College	4	16%
Multi-disciplinary College	2	13%
Multi-disciplinary University	12	27%
	40	

Table 4.2 Category wise security preparedness

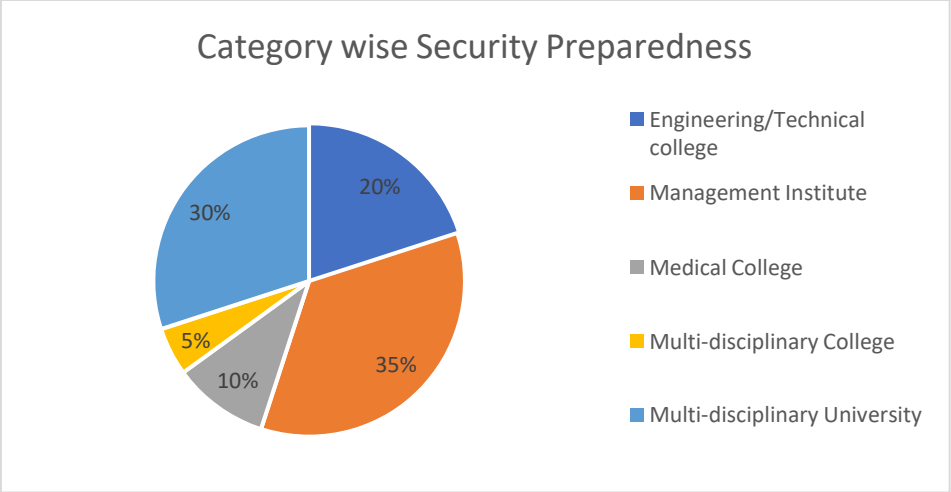

Figure 4.7: Category wise security preparedness

As we can see in the figure above, it is the Engineering/Technical colleges that are most adaptive to the current environment and have some kind of Security policies in place followed by multi-disciplinary universities. Again, this is in direct correlation with the responsiveness of the institutes.

Segment	Count	Percent
Aided	4	10%
Government	4	10%
Private	32	80%
	40	

Table 4.3: Segment wise security preparedness

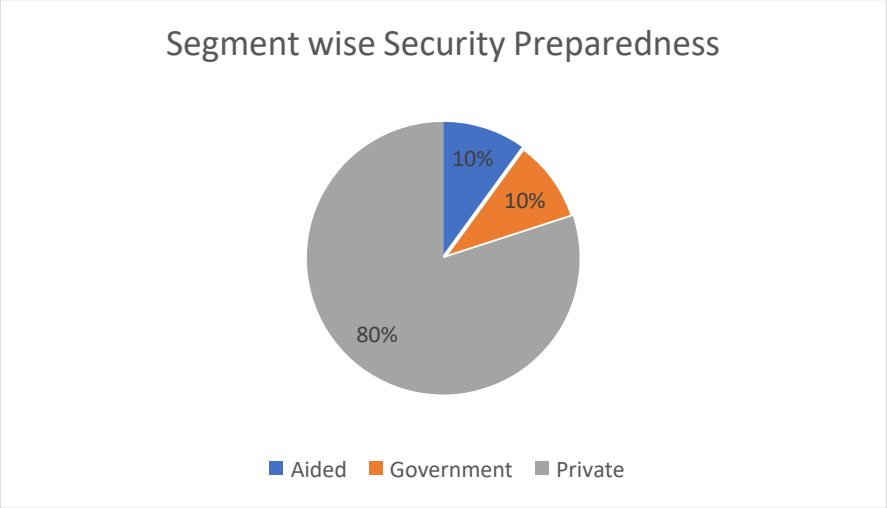

Figure 4.8: Segment wise security preparedness

Figure 4.8 shows, among those that have cyber security in place, 80% are private institutes. Government and aided institutes seem to be more reluctant to adopt which indicates there must be some problems that are preventing them from adopting the available cybersecurity standards or frameworks. The research tries to investigate and recommend suitable solution for the problems.

Age	Count	Percent
0-5 years	16	40%
5-10 years	22	55%
10-20 years	2	5%
above 20 years	0	0%
	40	

Table 4.4: Age wise security preparedness

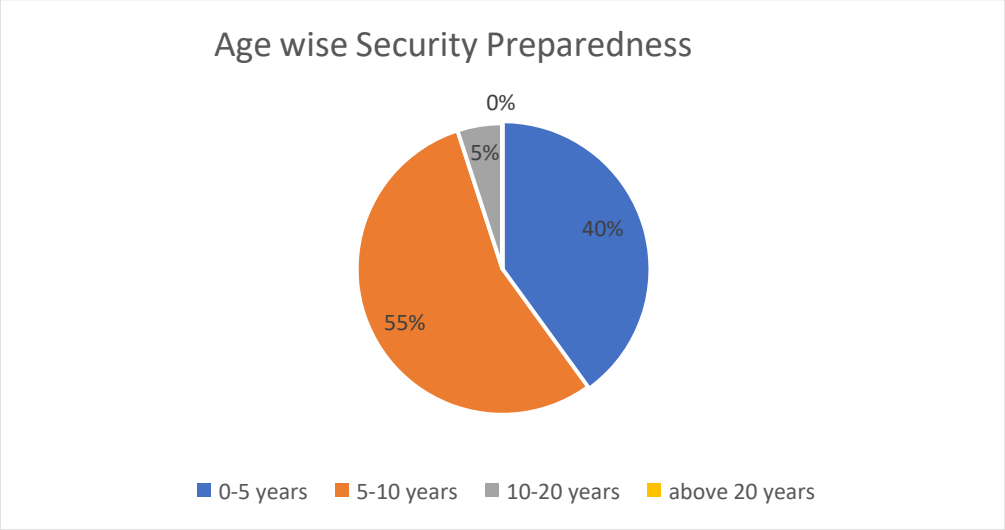

Figure 4.9: Age wise security preparedness

Figure 4.9 shows that more than 95% of institutes that have adopted cybersecurity are below 10 years old revealing that the newer colleges are more open to this change.

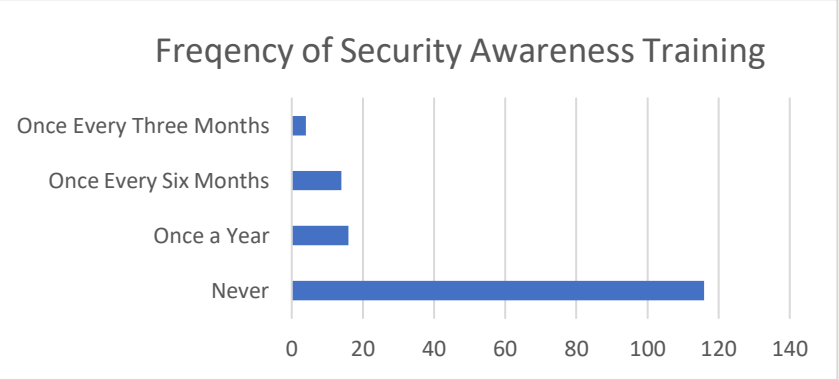

Figure 4.10: Security Awareness Training Frequency

It can be seen from figures 4.10 that staff and students of almost 77% of the institutes have never undergone security awareness training and this is a big risk. Even among the 33% that provide the training, 11% do it only once a year.

4.5 Cybersecurity Controls Adoption Challenges

Because colleges and universities were so early in adopting digital tools and interfaces, many institutions of higher learning still rely on legacy systems that are particularly vulnerable to

attacks. Cyber-attackers use cutting edge technologies and methods and can exploit university systems because, in general, these IT systems are woefully outdated and outmatched. Typically, university IT infrastructure is often characterized by a decentralized and haphazard set of systems that attackers can easily exploit.

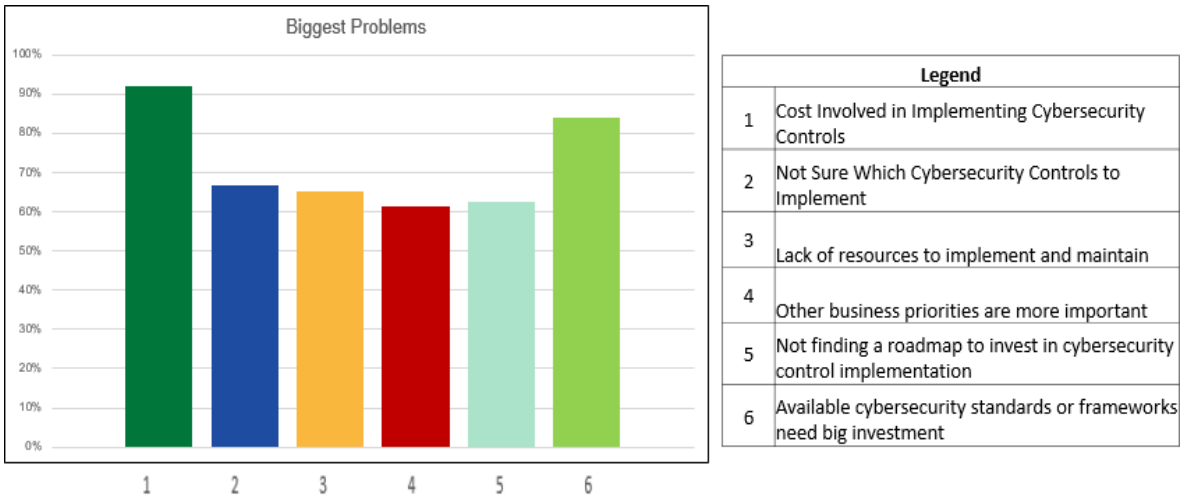

Figure 4.11: The biggest challenges for implementation of Cybersecurity Controls

As seen in figure 4.11, cost of implementation is the largest problems faced by institutes while considering cybersecurity implementation followed by Complexity of existing standards/framework (84%) with far too many controls. This requires serious consideration while coming up with an optimum framework for this segment.

4.6 Exploratory Data Analysis of Survey Data

Statistical analysis is done on the survey data. The data was gathered from different participants from several types of institutes through the survey to understand the current setups at the institutes. The data also gave an understanding on how the institutes are functioning with respect to security and the type of protocols that are being followed. The survey data was analysed taking the different attributes gathered from the institutes like the type of institute, segment, institute's age, what type of standards or framework is implemented if any, and if

there are security controls implemented, then the type of security controls and how many. In addition to these, the data showed the type of technical and administrative controls, if any, in place. Frequency of security awareness training conducted for the staff and students in the institute, and their awareness levels was another important attribute that was analysed from the data gathered. Information on the way the institutes treat its data, whether it is regularly backed up, encrypted, and classified based on sensitivity etc., was collected and analysed. Information on the types of problems being faced while planning or implementing cybersecurity controls was collected. Lastly, the institutes were also asked about the cyber-attacks that they faced. An exploratory data analysis on this collected data was conducted to gain some insights and draw some inferences.

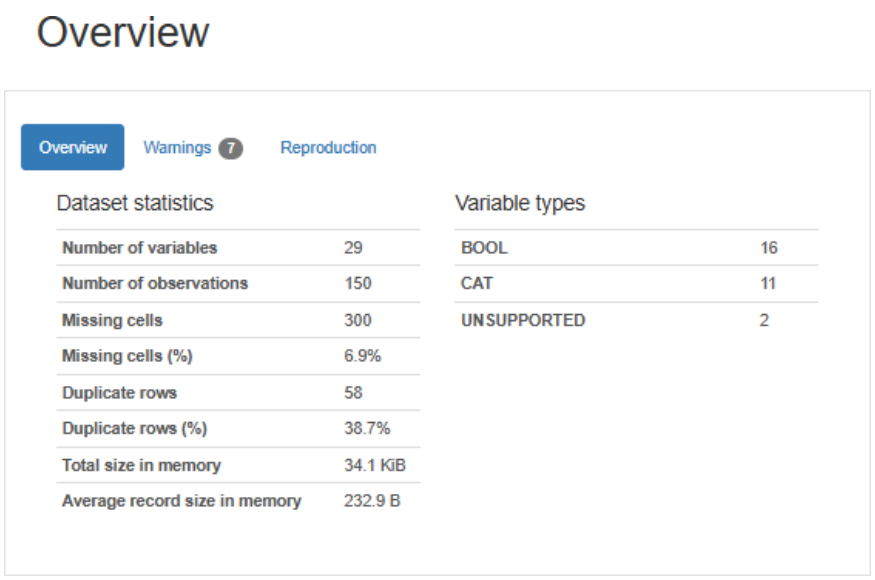

Figure 4.12: Overview of data giving the number of observations across multiple attributes.

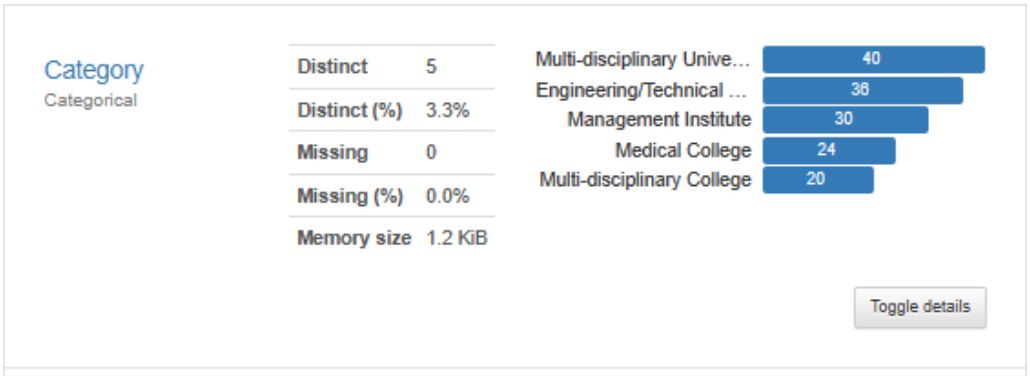

Figure 4.13: Participation across different categories of institutes

Figure 4.13 shows the distribution across types of institutes. We can see that among the respondents, Multi-disciplinary Universities and Engineering/Technical colleges were the majority.

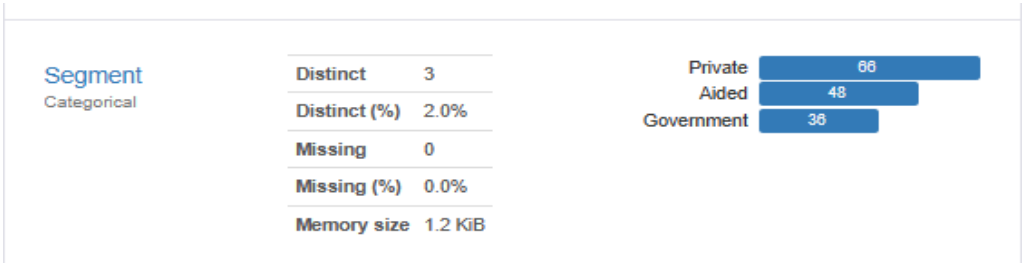

Figure 4.14: Participation across different segments of institutes

Figure 4.14 shows the distribution across different segments. Private sector institutes were more forthcoming in their response to our survey.

Figure 4.15: Participation across different age groups

Figure 4.15 shows age wise distribution. 5-10 year old institute were more enthusiastic in their responses. It is our understanding that older institutes over 10 years are generally set in their ways and slow to respond to new initiatives. The new institutes are still in the process of establishing themselves and are yet to implement governing processes. Hence, we see that the majority of the respondents belong to the mid age group.

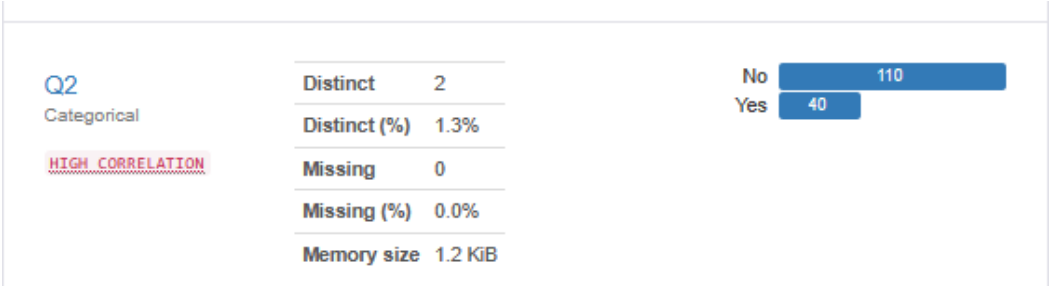

Figure 4.16: Institutes having security controls in place

Figure 4.16 shows the responses to the question on whether the institute has security control in place. The data distribution gives us a basic idea on the number of institutes actually using security controls. It is also to be noted that there are many institutes that mention having security controls, but most of them do not use them effectively or are not fully aware of it.

Figure 4.17: Types of Security Controls (Swanagan, 2020)

The three main types of IT security controls are technical, administrative, and physical. Security controls are primarily implemented for preventative, detective, corrective, compensatory reasons, or to act as a deterrent. The lack of security controls means

confidentiality, integrity, and availability of information at risk. These risks are not just confined to data but also extend to the safety of people and assets in the organization.

TYPES OF SECURITY CONTROLS	CONTROL FUNCTIONS		
	PREVENTATIVE	DETECTIVE	CORRECTIVE
PHYSICAL CONTROLS	• Fences • Gates • Locks	• CCTV • Surveillance Cameras	• Repair physical damage • Re-issue access cards
TECHNICAL CONTROLS	• Firewall • IPS • MFA • Antivirus	• IDS • Honeypots	• Vulnerability patching • Reboot a system • Quarantine a virus
ADMINISTRATIVE CONTROLS	• Hiring & termination policies • Separation of duties • Data classification	• Review access rights • Audit logs and unauthorized changes	• Implement a business continuity plan • Have an incident response plan

Table 4.5: Types of Security Controls and their Functions (Swanagan, 2020)

The overall purpose of implementing security controls is to help reduce cyber-attack risks in an organization or to reduce the impact of a security incident. Security controls can be effectively implemented based on its classification in relation to the security incident. Below are some of the common classification types:

- Preventive controls are used to prevent an incident from occurring.
- Detective controls are used to detect incidents after they have occurred.
- Corrective controls are used to reverse the impact of an incident.
- Deterrent controls are used to discourage individuals from causing an incident.
- Compensating controls – these are alternative controls used when a primary control is not viable.

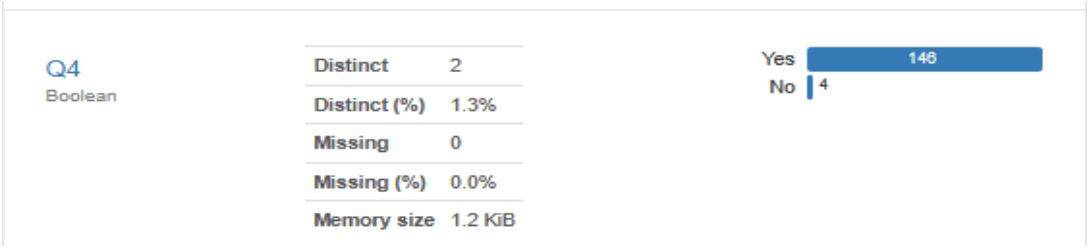

Figure 4.18: Institutes having physical security controls in place

Physical controls are generally used to deter or prevent unauthorized access to sensitive material through physical means like security guards, access control doors etc. Figure 4.18 shows that almost all the institute have some kind of physical security in place. These include Guarded fences, Security Gates, Guards, Security badges, Access cards, Security lighting, CCTVs, Surveillance cameras, etc.

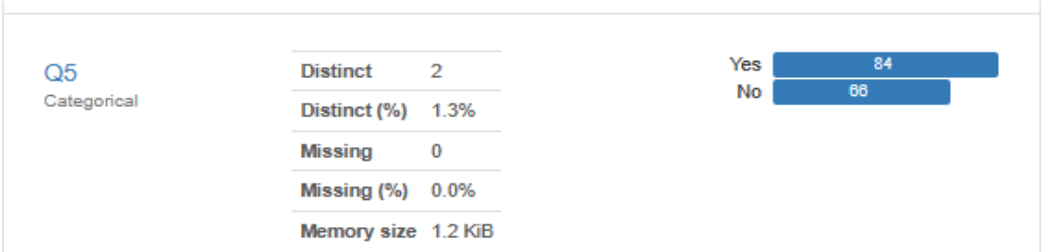

Figure 4.19: Institutes having technical security controls in place

Technical controls or logic controls are those that use technology to reduce vulnerabilities or weakness in hardware and software. Generally automated software tools like anti-virus software, firewalls etc are installed and configured to protect the assets. Figure 4.19 shows that almost 56% of the institute have some kind of technical security in place. These include Access control lists (ACLs), Anti-virus software, Authentication solutions, Firewalls, Encryption methods, etc.

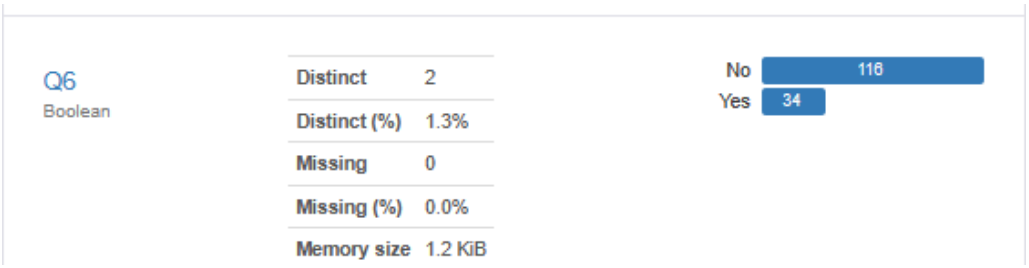

Figure 4.20: Institutes having administrative security controls in place

Administrative security controls relate to policies, procedures, and/or guidelines that clearly define operational or business practices to meet the organization's security goals. Figure 4.20 shows that only about 23% of the institutes have an actual cybersecurity policy in place. These

institutes have some kind of security policy and follow procedures to ensure cybersecurity and have guidelines in place for any incident management.

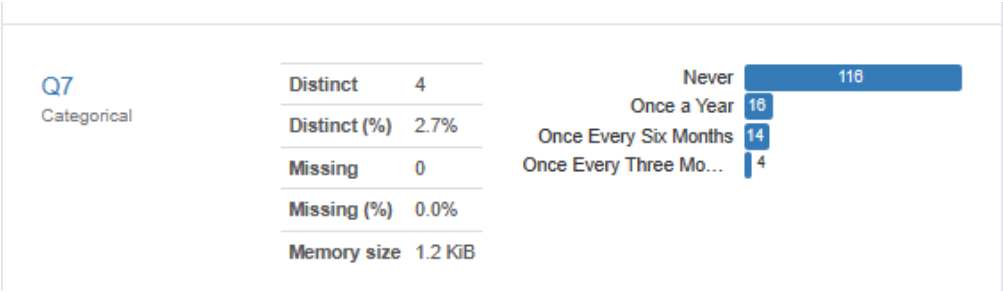

Figure 4.21: Frequency of cybersecurity trainings provided by the institutes

Cybersecurity awareness trainings are conducted to provide formal cybersecurity education to all the stakeholders about information security threats and the organization's policies and procedures for addressing them. Figure 4.21 shows that only over 77% of the institutes never had their staff/students trained on cybersecurity. This is in accordance with the similar percentage not having a proper cybersecurity policy in place.

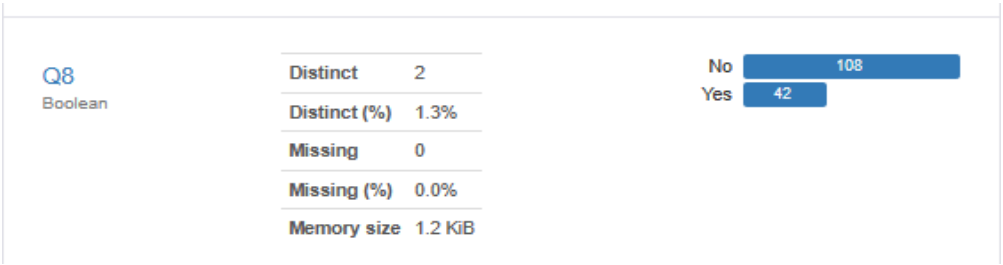

Figure 4.22: Institutes having mechanisms for reporting suspicious activity

Suspicious activity can refer to several behaviours involving abnormal access patterns, database activities, file changes, spam mails and other out-of-the-ordinary actions that can indicate an attack or data breach. To identify the source and nature of the breach, it is important to recognize these activities which will then allow to quickly act on it to minimize damage. Figure 4.22 shows the number of institutes having some kind of mechanisms for staff/students to be able to report suspicious emails quickly and effectively.

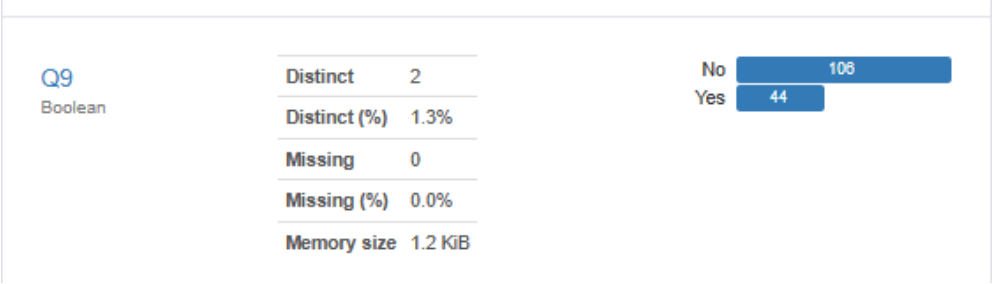

Figure 4.23: Institutes where people understand the risk of using public WiFi

Public Wi-Fi's biggest risk is that it is unsecured and vulnerable to attack. Hackers can use this weakness to install malicious software on devices or steal personal information without owner's knowledge. With the number of people relying on public Wi-Fi networks increasing daily, it is important to understand the dangers and take preventive measures to protect. Figure 4.23 shows the number of institutes where the staff and students understand the risks of using public WiFi.

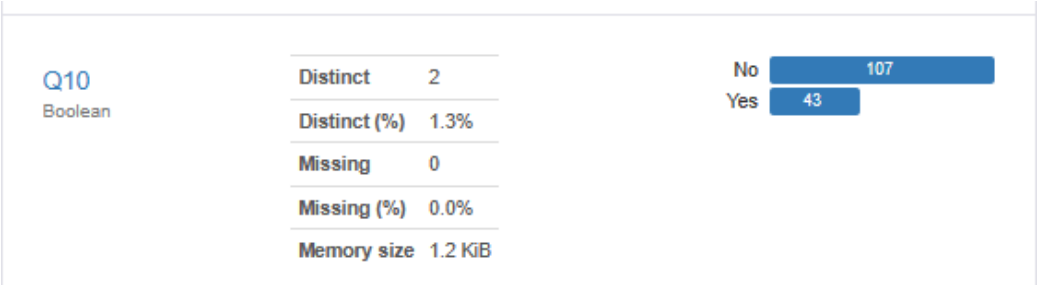

Figure 4.24: Institutes having manpower with Cyber Security.

Skilled and trained individuals who secure the IT systems, networks and devices along with the data from malicious threats, cyber-attacks, phishing attacks, and unauthorized access are cyber security professionals. Due to the complexity of the systems and the ever-changing IT landscape, this is a very challenging job. Figure 4.24 shows that less than 30% of the institutes have trained manpower with Cyber Security knowledge and are able to identify the risks and threats.

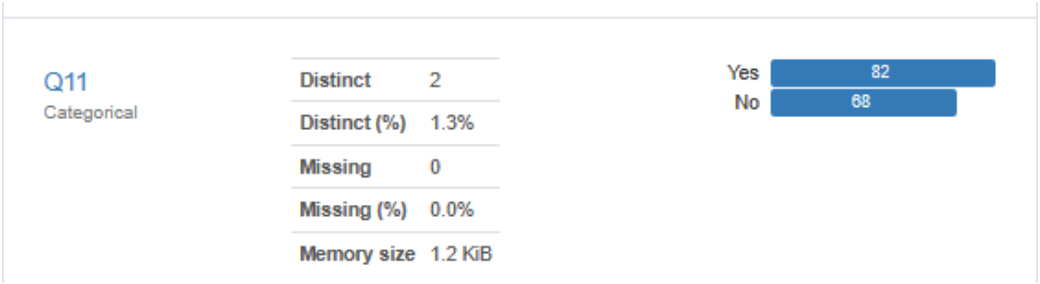

Figure 4.25: Institutes that take regular backup of data

The process of making a copy of digitized data and other business information is called Data Backup. In case the data is damaged, deleted or lost, this backed up copy is used to recover or restore original data to ensure business continuity. The survey results show that more than 55% of the institutes do take backup of their data. But there is still a high percentage (45%) that do not, which poses a big risk for these organizations, in the event of an attack.

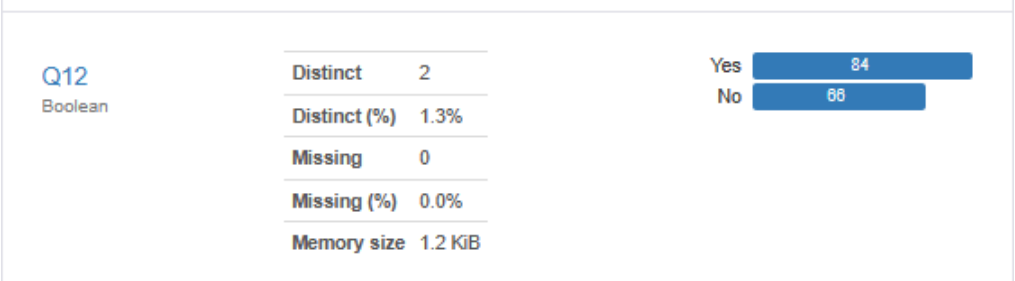

Figure 4.26: Institutes where backup data encrypted

A security method wherein the information is encoded so that it can only be accessed or decrypted by a user with the correct encryption key is Data encryption. Cipher text or the encrypted data generally appears scrambled and is unreadable to anybody accessing it without permission. It is one of the easiest methods of ensuring data privacy. Figure above shows over 56% of the institutes use encryption. But those which do not use (about 44%) face a big risk.

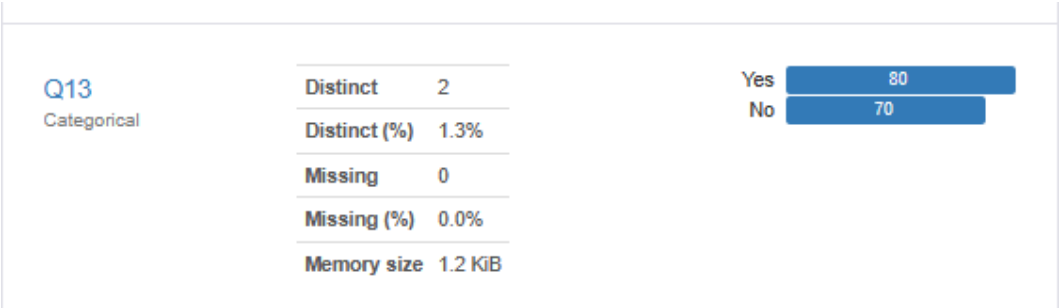

Figure 4.27: Institutes classify data by sensitivity and risk

Classification of data according to its type, sensitivity, and value to the organization is very important. It helps in understanding the value of the data, determining what data should be under what type of security control so that proper controls can be implemented to mitigate risks.

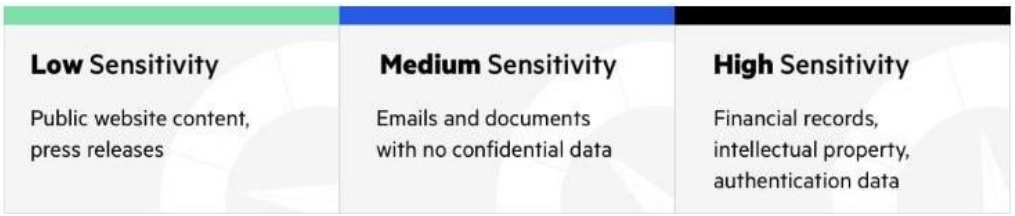

Figure 4.28: Typical classification of data by sensitivity (Imperva, 2021)

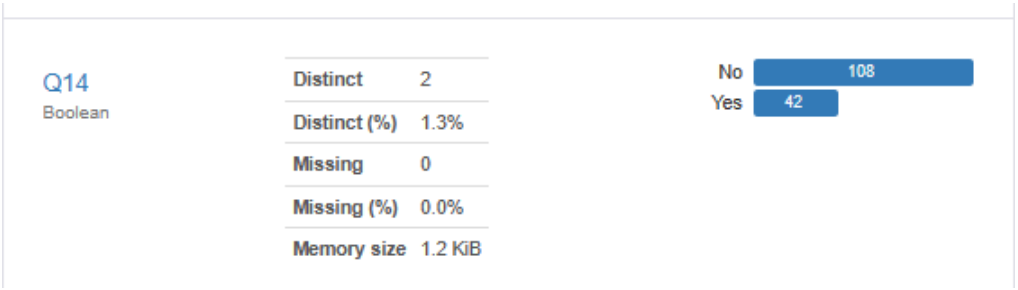

Figure 4.29: Institutes that have undergone Cyber-attacks

Data was gathered to see if the institutes have undergone any cyberattacks, and if so, the type of attack they faced. Analysis was also done to understand if the institutes that have undergone

cyber-attacks had any controls in place. Analysis shows that there is significant correlation between the two classes.

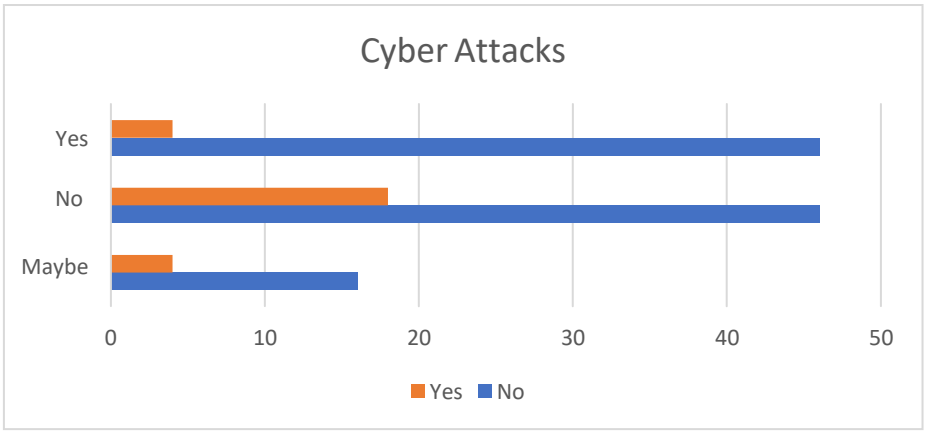

Figure 4.30: Correlation of Cyber-attacks to Institutes having Security Controls

The above table shows the correlation between institutes that do not have security controls and those which have undergone cyberattacks. As can be seen, the percentage of institutes that have undergone cyberattacks is more in the institutes that lack security controls. Only a small percentage (15%) of those having controls have faced cyberattack. This clearly shows that adoption of good security controls will help prevent cyberattacks.

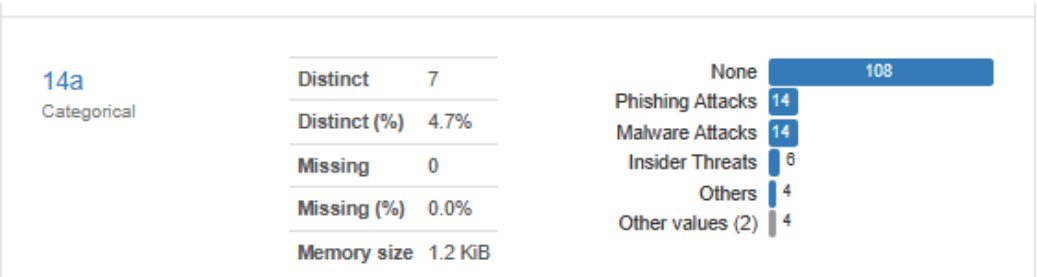

Figure 4.31: Types of Cyber-attacks on the institutes

Different cyber-attacks affect the organizations' critical resources. While predicting if an institute has undergone any cyber-attack, an analysis was done to understand the type of cyberattack that might occur. The data distribution shown in figure 4.31, indicates that malware, phishing attacks contribute the most to the attacks types in the institutes surveyed.

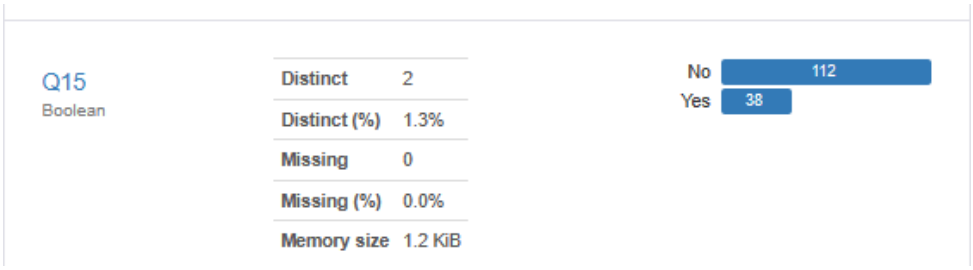

Figure 4.32: Institutes monitoring network for malicious traffic

Despite the evolution in communications and information technology, there will always exist data in motion and hackers will always target them, their focus being the main arteries and thoroughfares of data flow. Hence monitoring network traffic is crucial for any organizations irrespective of their shapes and sizes. Monitoring network traffic is generally used to maintain network performance and speed, though it can be used to give early warnings in case of potential problems and safeguard against cyber-attacks. Figure 4.32 shows that very less percentage of institutes monitor their network traffic on a regular basis through NOC/SOC for any malicious traffic. The study did not cover the efficiency of the network monitoring systems in use and hence cannot ascertain whether all institutes that claim to have a monitoring system in place are effective.

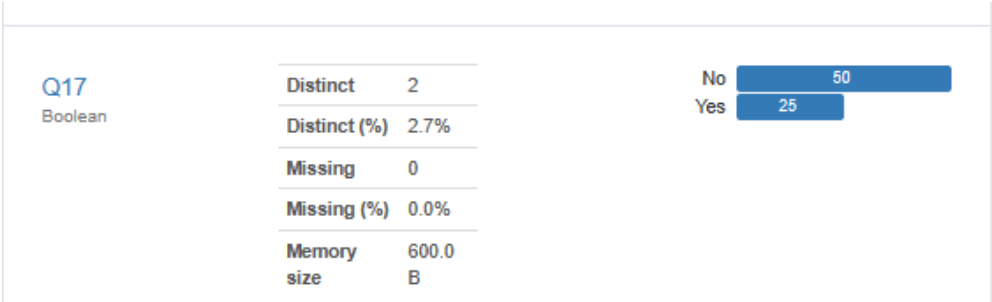

Figure 4.33: Institutes having a security roadmap

A strategic guide that helps organizations understand and manage cyber risk is referred to as a cyber security roadmap. For an educational institute, it is difficult to protect data and align its IT security with the institute's overall objectives either due to insufficient funds or inadequate

resources. Hence it is important for the institutes to undertake new security strategies to minimise these gaps. That is where having a good roadmap that aligns with the overall IT policy of the organization helps. Figure 4.33 shows the number of institutes that claim to have a security roadmap, that are reviewed against their overall IT roadmap on a regular basis.

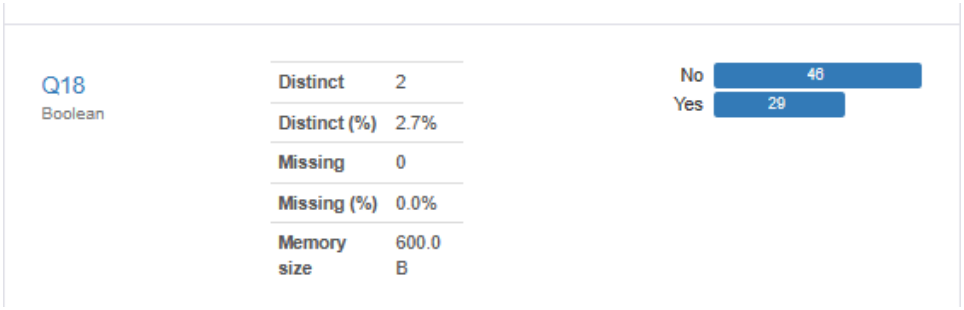

Figure 4.34: Institutes that outsourced IT security operations

Outsourcing cybersecurity is one of the ways of protecting organizations against various cyber threats. There are many third-party certified Managed Security Service Providers (MSSP) that an organization can use. These third-party agencies provide services that include methods to protect organizations against security threats like DDoS, phishing, etc. With internal SOC, an organization does not need to rely upon a third-party provider for anything and has full control on their security infrastructure. Conversely, with an outsourced SOC operation, the organization places the responsibility of security with an agency which specializes in cybersecurity which is more effective. This enables an organization to take advantage of their expertise and reduce costs. Figure 4.34 above shows the number of institutes that have outsourced their IT security operations.

4.7 Existing Cyber Security Controls Frameworks

It is very important to understand the type of frameworks or standards that an institute has implemented, as this will give a better understanding of current security posture in the organization. Institutes with standards or frameworks means better security control

implementation. Data distribution implemented standards or frameworks is shown in figure 4.35. Though the figure shows that ISO 27001 cybersecurity frameworks is the most popular one, we can also see that a considerable number do not have any frameworks or any standards implemented.

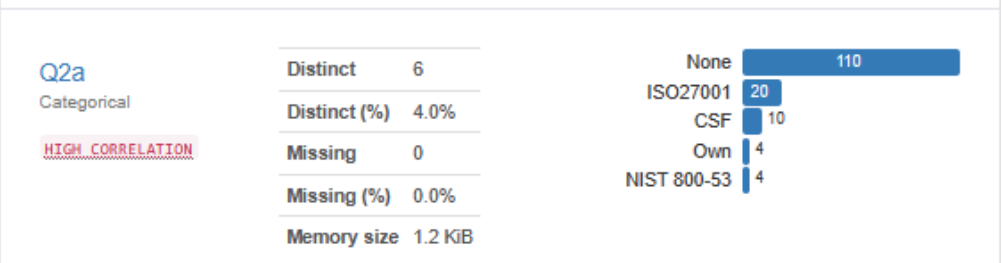

Figure 4.35: Existing Cybersecurity Frameworks

4.8 Predictive Analysis

Predictive analysis of the survey data was done to predict if an organization will undergo a cyberattack or not. To conduct a predictive analysis, various features, such as the age, category, segment of institute, awareness level of the institute, the types of cybersecurity controls implemented etc were used.

Based on the key regression coefficient calculations, below is the list of attributes (key predictors) that have bearing on the outcome (if there is an attack).

1. Q3: Does the organization have security controls in place?
2. Q11: Backup of data taken regularly?
3. Q15: Is network traffic monitoring done regularly through NOC/SOC for any malicious traffic?
4. Segment the institute belongs to.
5. Age of the institute.
6. Q7: How frequently is Security awareness training conducted for the staff?

7. Q8: Is there any appropriate mechanisms for staff/students so that they can report suspicious emails quickly and effectively?

We used the hypothesis that states, if an institute uses security controls, the probability that it will not undergo a cyber-attack is high. Which means, it is a possible to avoid cyberattacks by using appropriate security controls and measures. To support this hypothesis, a classification algorithm was built to predict if an institute will undergo a cyber-attack or not. Here, 0 means “Yes”, 1 means "No". The classification report shows that there is a high accuracy that an institute will not undergo a cyber-attack and the chance that it will undergo a security attack is lower. Classification Algorithm report is shown in figure 4.36. A logistic function was used to model the probability of possible outcomes in this algorithm. Logistic regression is mostly used to analyse the influence of multiple dependent variables on single outcome variable and is designed for classification.

```
Accuracy score
0.660377358490566
Precision/Recall
              precision    recall  f1-score   support

           0       0.69      0.85      0.76        34
           1       0.55      0.32      0.40        19

    accuracy                           0.66        53
   macro avg       0.62      0.58      0.58        53
weighted avg       0.64      0.66      0.63        53

AUC

: 0.5843653250773995
```

Figure 4.36: Classification Report of the Logistic Regression

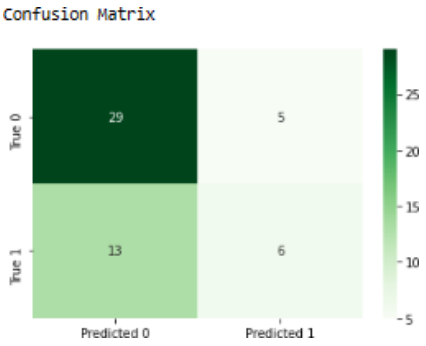

Figure 4.37: Confusion matrix

4.9 Summary

It is evident from the analysis that more than 75% of institutes are behind in terms in implementing cybersecurity controls. It is also to be noted that the institutes with limited cybersecurity controls are also not able to protect their people from cyber risks. We will go through each category and segment and their cybersecurity posture in greater detail in the coming chapter.

CHAPTER V

DISCUSSION

5.1 Results Discussion

It is important that the cybersecurity controls implementation in an educational institute should contribute to its domain-specific demands. It will be more attractive to the institutes if they are assured of tangible advantage in implementing cybersecurity measures and will persuade them to invest in the implementation. Many times, the common cybersecurity standards or frameworks force organizations to implement a broad set of controls, many of these may or may not be relevant to this sector. Any domain or sector has its own unique set of critical assets that should be taken into consideration while implementing security controls.

It is imperative to establish link between the themes, correlations, and literature discussions as shown by the triangulation below. It will be further discussed in the later sections.

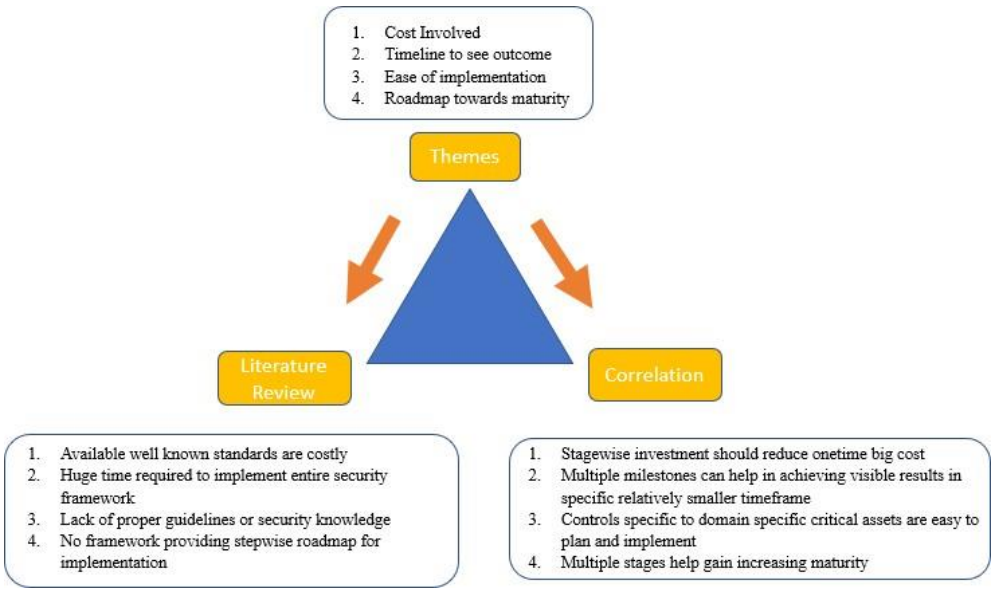

Figure 5.1: Triangulation

This chapter will go into the specifics of the research findings, in correlation with the existing literature and suggested conceptual framework. Emphasis will be placed on those attributes

that came up as the most significant during the analysis, though other attributes that seemed important for the stakeholders (inferred during the interview process) will also be touched upon.

5.2 Research Questions Discussion

In the following subsections, valuable inputs from participant institutes will be discussed in detail.

5.2.1 Segment of the institute

When it comes to predicting what type of institute is more prone to cyber-attacks, we must analyse which type of institutes have adopted good cybersecurity controls. It is noted that the private sector institutes have a decided advantage over the other two segments – government and aided. Private sector institutes are governed by independent bodies and hence can make decisions more easily without having to go through bureaucratic hassle. Availability of funds is also another advantage for these institutes. But big research institutes both government and private are very much vulnerable to cyber-attacks and hence are more equipped with very good cybersecurity controls. Institutes like Indian Institute of Science, Tata Institute of Fundamental Research, All India Institute of Medical Sciences are some of the bigger institutes which have adopted very sophisticated cybersecurity controls. Among the institutes that responded to our survey, 80% of the institutes that have some kind of cybersecurity controls are private organizations. This clearly indicates that government and aided institutes that are less likely to have security controls are more prone to cyber-attacks.

5.2.2 Age of the Institute

It is noteworthy that nearly two-thirds of the participants belong to less than 10 years category. This demonstrates that institutes with a longer history were not eager to give information and

were reluctant to discuss the issues they must have faced. The newer institutes were more forthcoming. It is possible that the older institutes also did not have much in terms of security controls and hence were reluctant to share their inputs. The newer institutes seemed to be more adoptive to the changes in technology and were more forthcoming in sharing the information. Risk of cyber-attacks is higher with the older institutes as their IT systems may be outdated and they are less likely to have good controls in place.

5.2.3 Current State Standards or Frameworks Implementation

There are numerous mature cybersecurity standards and frameworks that are universally used in the market. Organization that does not have such measures in place lacks an organized defence against cyber-attacks. This is a weakness that cybercriminals can exploit and can lead to financial loss as well as damage their reputation and brand value. The survey demonstrated that more than 70% of institutes do not have any kind of cybersecurity framework or standards adopted, and this is a huge risk. Despite this high risk, if the institutes have not adopted a good cybersecurity controls framework, there must be a very good reason. It is the aim of this research to understand these reasons and try to address them while recommending a good framework for the education sector.

5.2.4 Current State of Security Controls in Educational Institutes

There are organizations that have implemented a few security controls without referencing any framework. So, regardless of their answer to the question about the institute having implemented any security framework, the survey tried to collect data on the security controls the institutes have implemented. The aim was to check if the institutes have cybersecurity controls implemented without referencing any particular standard or framework. Approximately 45% of the institutes have security controls implemented, either independently or as part of a framework that they have adopted. Institutes that were unsure whether their

organization had any cybersecurity controls in place ranged about 13%. This clearly shows a lack of competency in understanding cybersecurity controls. The remaining 43% institutes did not have any cybersecurity controls in place and these are at risk of cybercrime.

Figure 5.2: Types of Security Controls (www.theamegroup.com, n.d.)

Confidentiality, integrity, and availability of information is at risk if there are no adequate security controls in place. These risks are not limited to the data and information only but may extend to the security and safety of the people and assets within an organization.

5.2.5 Physical Security Controls Scenario in the Institutes

These are security measures implemented on physical structures to prevent or deter unauthorized individuals from accessing an organization's valuable assets. Despite its low probability, lack of physical security often results in significant damage and hence it is crucial to an organization. There are many things that can compromise physical security ranging from natural disasters to power outages. Security gates, biometric identification systems, thermal alarm systems, motion alarm systems, closed-circuit surveillance cameras, security guards, security dogs, and photo ID are examples of physical security controls. Hackers can gain access to internal assets of the organization, such as IT systems and critical data if physical controls are not employed. Most institutes have implemented physical security like access cards, CCTV

cameras, security guards, photo IDs etc. Though sophisticated methods like biometrics (includes fingerprint, voice, face, iris, handwriting, and other automated methods used to recognize individuals), motion alarm systems, thermal alarm systems are not very prevalent. Access controls is generally through photo ID cards, but there does not seem to be many institutes where access is area and role specific. This means, once a person gains entry into the institute premises, he or she is allowed in almost all places within. Very few institutes employ restricted access to labs and other sensitive areas. One other detective control method that is commonly seen in the institute is the visitor logs. But this is only effective with regular log monitoring which is very infrequent in most institutes.

5.2.6 Technical Security Controls Scenario in the Institutes

Security of important information or data via the organization's network is ensured by using technical or logical controls. Regulation access or use is done using technology. Network authentication, antivirus software, encryption mechanisms, smart cards, and access control lists (also known as ACLs) are the commonly used technical controls. Improper implementation of technical controls may lead to cyber-criminal accessing important data. Most of the institutes that responded to the survey used antivirus and anti-malware software, firewalls, and data encryption. But other more advanced methods like ACLs, encryption, Security Information and Event Management (SIEM) etc were used only by a few. It was also noted that antivirus and anti-malware software used by a few institutes were outdated and not upgraded to the latest version. Encryption was used by about 56% of the institutes.

5.2.7 Administrative Security Controls Scenario in the Institutes

Security policies help an organization in defining a set of rules and procedures used to establish the requirements for achieving their security goals. Security controls that define clear

processes, procedures, and guidelines for the organization come under the purview of administrative controls. This includes disaster preparedness, disaster recovery plans, separation of roles, and many more areas, training and awareness. Administrative controls assist operations of the organisation by supplying crucial plans like Incident Response (IR) plan that helps in responding to a cyber-threat and avoid the negative effects of a successful cyber-attack (Naseer, 2021). In general, administrative controls control the behaviour of the people of the organization or change the way of working. Since human beings are considered the weakest link, implementing these controls becomes very important. To succeed in the implementation of cybersecurity for any organization, people's involvement is essential. It is important for all the stakeholder to be aware of the security processes, procedures, and guidelines. To implement administrative controls, it is essential to have additional security controls for continuous monitoring and enforcement. Below processes are essential to enforce the administrative controls:

Management controls: These are the controls that focus on the management of information system security and the risks involved.

Operational controls: These are controls that are mainly implemented and executed by people (as opposed to systems).

For example, a security policy comes under management control. The security requirements under that policy are implemented by people which is operational control, and systems which is technical control.

An organization may have an adequate user policy to guide the conduct of users so that they do not visit malicious websites. This is management control. A web content filter may be applied to monitor and enforce this policy along with logging. This is operational and technical control. Hence it is very important to have both policy and procedure to be effective in

cybersecurity. According to our survey, only about 23% of the institutes have adopted cybersecurity policies and procedures. Though, over 56% have technical controls in place, without good policies and procedures, technical controls will not be as effective as they can be.

5.2.8 Data Backup

Data Backup is the process of making a copy of the digitized data and other business information when can later be used for recovery if the data is damaged, deleted or lost to ensure business continuity. The goal of the backup is to deposit the backed-up data to a separate, secure location from where it can be retrieved when necessary. Securing data will help prevent:

- Accidental damage to data or malicious modification of data
- Theft of valuable data
- Breach of confidentiality agreements and privacy laws
- Premature release of data, which can lead to voiding of intellectual property claims.
- Release of data before it is completely checked for accuracy and authenticity.

Keeping reliable backups is among the most important aspect of data management. Regular backups protect against the risk of damage or loss due to software or media faults, hardware failure, power failure, viruses or hacking, or even human errors. Survey data analysis showed that only about 55% of the institutes follow the practice of regular data backup. This is a high-risk scenario. Data stored in the institute servers are generally backed up as a regular part of the IT operational procedures. But the data that is stored in the individual laptops, desktops, phones, tabs etc are most prone to risk of loss. There is high possibility that these personal gadgets contain research data that are valuable to the institute. Hence, there is a requirement to formulate procedures that enable backing up of data in these personal gadgets if these contain institutions data.

5.2.9 Regular Monitoring of Network Traffic

Most of the cyber-attacks happen over the network. This makes the network an ideal source of information about threats to an organization and its systems. Generally, network traffic analysis is used to monitor network traffic and few other network issues. But this process can also extract information about potential security threats. The IT infrastructure of an organization consists of a variety of different systems, environments, and endpoints. This increases the difficulty of monitoring and securing the IT architecture. All these systems are connected over the network, and this may be how threats enter an organization's environment and travel between systems. Monitoring for anomalies in the network traffic helps prompt an organization about possible cyberattack or other issues. Network traffic analysis refers to the practice of intercepting, recording, and analysing network traffic communication patterns to discover and respond to security concerns. Implementing a system that can continuously monitor network traffic can provide information that is needed to improve network performance, reduce attack surface, boost security, and better manage the IT resources. Survey data for educational institutes showed that only about 56% of the institutes employ some kind of network monitoring process. The other 44% are at high-risk for any cyber-attacks. Of the 55% that do monitor the network, it will be interesting to understand the purpose and efficiency of these monitoring systems. If these monitoring systems are used only for the purpose of improving network performance and does not detect potential threats, even these institutes are at risk.

5.2.10 Security Awareness Training Frequency

For the staff and students at an institute, it is very important to regularly go through security awareness trainings. Security awareness trainings are used for providing formal cybersecurity education to the organization's workforce about the variety of information security threats and

the organization's policies and procedures for addressing them. The most vulnerable link in the systems is its people. Even if an institute invests in the best technical tools and processes, it still requires human leadership. The biggest risk to an organisation is if the people working within or for it are bypassing cybersecurity measures in any way. Having security policies is not sufficient if the people are not adequately trained to follow to those procedures. Instilling the importance of cybersecurity in each person's behaviour and actions therefore becomes very critical (Li, 2021). Cybersecurity awareness training which emphasizes the significance of the subject and also details the procedures to be followed is very important. Organization's risks are reduced by number of cybersecurity awareness trainings conducted each year. Every organization should have a policy that requires new joiners' to complete security awareness training and be aware of the organization's environment and assets before being they are granted access to its resources. Well-involved and trained staff are the first line of defence against cyberattacks (Ponsard, 2019). Cybersecurity awareness training will prepare the staff with skills and knowledge to avoid being a victim of cyber-attack tricks. Despite the importance of this training, it is seen that only 23% of the institutes follow this. This number is similar to the ones that have administrative controls. This may be because, one of the important processes in any cybersecurity guidelines is creating awareness among the staff through trainings. So, it can be interpreted that the institutes that have administrative controls (policies and procedures) are the once that impart security awareness trainings to their staff and students.

5.2.11 Biggest Problems Faced by the Institutes

The first step in any journey is always more important than the rest. Deciding which type of controls or framework best suits the organization's Cybersecurity needs is the first step in process of implementing Cybersecurity controls. And the biggest challenge faced by the institutes is because of the complexity and extensive controls in the existing frameworks. Successful cybersecurity implementation also necessitates huge investment and a large number

of dedicated resources to be available. Most of cybersecurity standards work in such a way that the enterprise either implement them entirely or don't do it at all. This means the value is not realized until the end, which will not provide investors with confidence. These three major issues make institutes believe that investing in cybersecurity is an overkill because of the large investment required and the hardships faced during implementation. It is the inability to identify a path to invest step by step and realize the gains at each milestone and the complexity of the available cybersecurity standards or frameworks as well as lack of knowledge, are all challenges that prevent the institutes from moving forward with the implementation of existing cybersecurity controls. Also, the huge time required to establish total cybersecurity safeguards is cited by the institutes as one of the major issues.

5.2.12 Experience of Cyber-Attacks Faced by the Institutes

In this post-pandemic world cybersecurity has become an enormous concern for colleges and universities. Even before the pandemic hit, institutions of higher education were collecting huge amounts of data from their students and faculty. This has increased many folds now that many colleges and universities are offering hybrid or fully remote curriculums.

Figure 5.3: Different types of cyber-attacks faced by organizations (Data Communication and Computer Network, 2020)

Below are some world-wide statistics (Lukehart, 2022) on Cyber-attacks in education sector:

- Of all the ransomware attacks, 5% were directed at education sectors in 2022.
- 3.86 million dollars is the average data breach cost in education sector.
- Educational services industry saw a huge increase in ransomware attacks, it accounted for more than 30% of the breaches in 2022.

Because of the massive amounts of data that colleges and universities store, they often become targets for hackers and other cyber criminals. Cyber-attack statistics reflect this. In fact, there were 1,851 data breaches in educational institutions between 2005 and 2021 (Lukehart A, 2022). Also, most of the universities and colleges have outdated systems or poorly constructed cybersecurity controls. This makes them more vulnerable to cyber-attacks.

According to our survey Phishing and Malware attacks were the most common problems faced by the institutes. In a phishing attack, the hacker will pose as a trusted entity and exploit that trust to trick the user into providing sensitive information like passwords or even social security numbers. Phishing generally occurs through email or social media messaging. There are a few ways that hackers typically choose to target colleges and universities via phishing. The first is by posing as the college to get student or faculty credentials. The hacker may later use this information to access the university's digital systems and valuable data. Another strategy is to target important people in the university's management or faculty members who may have access to specific pieces of data that hackers value. The hacker may use "spear phishing" or "whaling" strategy, which involves the study of the target individual's behaviour to find the most effective way to gain their trust. Phishing is among most effective types of cyber-attacks since they are very difficult to identify and block. Educating the students and staff on how to recognize phishing messages can be incredibly effective at preventing successful attacks. This is particularly important because many students and faculty use their own devices like laptops

and smartphones on campus, which may not have adequate security protection. Using two-factor authentication can also be very effective at preventing phishing attacks. Two-factor authentication involves the person to enter a code sent to his or her email or phone number in addition to the password to log in to the university's system. There are some good apps like Google Authenticator which make this relatively easy to implement.

Cyber-attacks that are carried out with the help of malicious software are called Malware attacks. These includes adware, malvertising, computer viruses, worms, trojans, and spyware, etc. Because emails can overcome firewalls, two-factor authentication, and other security measures, technical safeguards are almost always not effective against phishing and malware attacks. Also, it is very challenging to restrict a few that are generally open to receiving emails from the public.

Hence it is essential for all users of an organization to have a high level of cybersecurity awareness so that they can avoid such cyber-attack techniques (source: Hong, 2012). Often insiders who frequently access critical assets in the organization may be involved in the cybercriminal operations directed against it. Recent attack trends show that insider risks are increasing. Cyber-attacks generally happen when a person or a group ignores or neglects security policies (Greitzer, 2011). Hence it is important that the individuals working for the institute follows well-established cybersecurity policies, procedures and guidelines. All the gadgets owned by the institute like laptops, desktops generally have appropriate restrictions installed, but devices owned by the staff, students, guests, or even visitors, require a "Bring Your Own Device (BYOD)" policy. These outsider devices are a danger to the institute. Insider threats are reduced to a large extent by the BYOD policy (Baillette, 2018). Knowledge management is very crucial to an organization, hence it is required to strike a balance between the degree of freedom to access critical information and the security safeguards that need to be

followed. It is critical to have regular trainings on security policies but also to clearly define specific methods to minimize the disclosure of institutes knowledge to outsiders. Motivation and recognition, the organisation's attitude toward its staff, and proper treatment for any process infraction also help reduce risk (Popescul, 2011).

Due to the transition to cloud-based environments, web applications and their security are becoming critical. Web attacks are increasingly being used by cybercriminals to gain access to organization's critical information. They may also be used to disrupt or leak information flow that is essential to an organization's survival. Proper authentication and authorization with user credentials should be implemented by the organization. Basic cyber hygiene recommendations like complicated password usage, multi-factor authentication, multiple passwords for different applications, and such things should be taught during security awareness training (Bang, 2012). Because web platforms hold information about research as well as student personal information, they become targets for phishing attempts. It may even require payment of ransom to avoid exposure on black sites.

During our survey, many institutes voluntarily contributed critical information on the cyber-attacks they faced. Apart from phishing and malware attacks, various other types are also experienced by institutes. Hackers often target organization's servers, gain access to critical data, sometime make a copy of the data before encrypting it. The data becomes unusable and will require a decryption key to restore it. Hacker may demand hefty ransom to provide decryption key and/or prevent the data from being leaked. Sometimes hackers may try to overload the network, which makes it inaccessible to authorized users. This is called denial-of-service attack. At times, cybercriminals can read and/or change information through active eavesdropping, which is called as Man-In-The-Middle attack and this generally happens on data in transit.

As per the survey data, malware attacks and phishing assaults are the top areas of worry for educational institutes. Insider threats, web attacks, and ransomware are some of the other areas that are cause for worry. It is possible to stop all these types of attacks by using appropriate technical controls, but most importantly cybersecurity awareness training helps to reduce the risk. It is required to have strong rules as well as relevant technical controls to reduce the dangers from insider attacks. Administrative controls including policies, rules, and procedures will improve the effectiveness of technical and physical controls and together these form a solid cybersecurity wall for the organization and its important assets.

5.2.13 Expectations of Security Standard or Framework from Institutes

The study gave an interesting insight into the present state of cybersecurity control implementations in educational institutes and how they contribute to cyber risk exposure for them, along with the challenges they are facing during the planning and implementation of cybersecurity controls. Most institutes were wary of the complex frameworks currently in the market and their costs. Number of controls and the complexity of compliance audits were also mentioned as deterrents. A simplified framework with limited controls, ease of implementation and cost were the three most important points mentioned by the participants of the survey.

5.3 Discussion of Hypothesis

During the course of research, it was noted that institutes are lagging in the implementation of technical, and administrative controls. Also, there were certain gaps in the important aspects of a good cybersecurity implementation like cybersecurity awareness training frequency, proper classification of data, regular backup of data and encryption, effective procedures for monitoring and detection of cyber threats. Research also showed that very few institutes have adopted cybersecurity standards and frameworks currently prevalent in the market. This study

hypothesizes that the state of existing cybersecurity posture in educational sector is not good due to various problems.

5.3.1 Cybersecurity Implementation is Expensive

To implement existing standards or cybersecurity control frameworks requires both financial and other resource investment and this is major issue faced by the institutes. During our analysis, it was seen that most of the time the institute's management were unable to see the benefit of the investment made in cybersecurity standards implementation towards their operational goals. This is because each sector or domain is different in terms of its security needs and has unique business-critical assets. If such a critical asset gets threatened, it may cause serious issues for the institute's sustenance or growth as well as its reputation. Cybersecurity costs will generally add about 10-25% to every product that is bought for the organization's IT system. The additional cost is due to the added safety features for the equipment, cybersecurity insurance, or even the regular cybersecurity audits to ensure the system is safe. Sometimes it may not be necessary to spend exorbitantly on cybersecurity as there is only so much that can be done to keep up with the fast-learning hackers. But it is important to make sure there is enough protection to make the system challenging enough for hackers to access easily.

Considering how expensive an actual hack can be for an organisation, this goes a long way and is essentially just another form of insurance that organizations need to remain safe. Being a victim of a cyber-attack can be devastating to an organisation. While it might seem intimidating and confusing, keeping an organisation safe from cybercrime is easier and less expensive than is generally expected. From protecting the institutes research data to the institute's reputation, even a little bit of cybersecurity can go a long way.

5.3.2 Cybersecurity Implementation Takes a Long Time

The existing cybersecurity standards and frameworks come with a long list of cybersecurity controls that require quite a long time to implement and see the results. **Top management can realise the benefits only after investing in this long.** The type of cybersecurity controls that is required to implement determines the timeline and this kind of investment requires executive-level buy-in (Convocar, n.d.). It is essential to come up with an effective security program that creates a security-first culture within the organization, and this should be done by a joint team consisting of members from both organization's side and the implementing agency. This itself takes months, sometime even years.

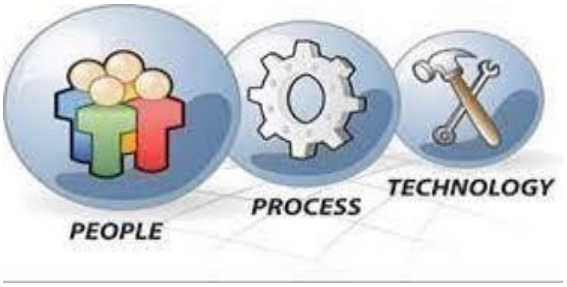

Figure 5.4: Factors affecting Cybersecurity Implementation Timelines

(www.linkedin.com, n.d.)

5.3.3 Ease of Implementation is Missing

A cybersecurity strategy implementation plan is a written guide to follow and improve defences against the on-going threat of cybercrime and overall risk management. This involves designing secure applications architecture, writing secure code, implementing strong validation of input data, threat modelling and many more so that the likelihood of any unauthorized access or modification of application resources is minimized. Most of the available standards or frameworks are lagging in providing a starting point for implementation of cybersecurity controls. These cybersecurity frameworks give organizations a systematic, repeatable, and

reliable way to manage cyber risks irrespective of the environment and its complexities. But these frameworks are generic and try to address the issues that may not be relevant to the educational institutes. This may sometimes lead to implementing controls that may not be really necessary and thus complicating the process as well as adding to cost and time. Because of the complexity and number of controls, the implementation requires lots of effort by skilled resources and sparing them is always a challenge for the institutes. Ease of implementation is seen as a major factor that can positively influence to the adoption of Cybersecurity controls by educational institutions.

5.3.4 No Road Map Towards Maturity

There are five distinct maturity levels as defined by the cyber maturity assessment framework that indicate the degree to which an organization has optimized its security systems and processes. While traversing from level one to level five, the organization will develop, refine, and enhance its cybersecurity posture. This takes a long time and the cost to reach the end point is quite high.

Figure 5.5: Cybersecurity maturity levels (Egnyte, 2022).

The cybersecurity standards or frameworks currently in the market do not provide for staged implementation of the controls. Because there is lack of clear roadmap, management will not

have the motivation, though implementing cybersecurity controls will help their operational goals. There are many instances of implementations being abandoned half-way because the stakeholders could not see the effectiveness or interim successes. Hence these frameworks are seen as another tedious item on an already long to-do list by most institutes. If a cybersecurity controls implementation is to be successful, there should be clear roadmap and a step-by-step approach with intermittent milestones so that stakeholders can visualize success at regular intervals.

5.3.5 Conclusion of Hypothesis

Our research clearly showed the wide gap between expectation of the institutes and what is possible to achieve using existing cybersecurity standards or frameworks. These frameworks do not cater to the unique needs of the education sector, hence the overall benefit for the institutes to relate to or invest in the same is missing. All of these existing frameworks are complex, requires changes in the organization and also requires new skills. So, it is important to have a buy-in from all the stakeholders for the framework and its implementation. This will happen only if it is customized to the specific sector and trimmed off of all the unrelated and time-consuming details.

CHAPTER VI

COMPARATIVE STUDY OF EXISTING FRAMEWORKS

6.1 Summary of Existing Frameworks

A collection of international standards and best practises on cybersecurity is collectively referred to as a framework (Atoum et al., 2014); (Mustafa, Alzubi and Alshare, 2020), (Bian et al., 2022). The framework includes set of principles that are accepted internationally for keeping networks secure and is necessary for the ease of implementing protective controls for information and IT infrastructure against cyber-attacks and other security risks. It is possible for organizations to utilise the frameworks as a jumping off point in order to improve the security of their computer networks. Cybersecurity frameworks are designed primarily to assist businesses and other organisations if there is a cyberattack by assisting them in analysing the situation, keeping track of threats, and taking the required action. Organizations are able to manage their cyber security risks in a way that is both voluntary and straightforward because of the frameworks for, which are based on a set of previously tested and proven principles and standards. Both the government and the private sector have contributed to the construction and development of cyber security regimes. Standards, rules, guidelines, practises, and ideas that ensure strong safety are the components included in cyber security frameworks. These may be broken down into four categories: policies, rules, practises, and suggestions.

Some of the Cyber security frameworks available aim to assist organizations in risk reduction and also coordination and communication with its partners (Boneh & Shoup, 2020); (Smail et al., 2022). Most cybersecurity frameworks are constructed with multiple elements that are responsible for different purposes. But the most basic component is the one in charge of standardising the activity of tracing and defending against cyber threats and strikes. It is the responsibility of the implementation tiers to manage cyber security using specific protocols. Thirdly, profiles play a vital role in identifying and putting into action effectual measures to

increase cyber security across the organisation (Forouzan & Mukhopadhyay, 2015). Although at first glance the frameworks seem to be quite distinct from one another, in reality they are all working toward the same goal. There is a degree of diversity across the various cyber security frameworks; this provides companies with the opportunity to make well-informed decisions based on considerations such as appropriateness and usefulness.

The seven cyber security frameworks that are utilised most often are SOC2, ISO 27001/27002 and NIST Cyber Security framework, FISMA, GDPR, HIPAA, and NERC CIP. The goal of these frameworks is to provide organisations with a road map for analysing, monitoring, and removing cyber security threats and this is done by establishing a consistent vocabulary and set of principles for security providers across different industrial segments. (Asaad R. & Saeed V., 2022). This is done so that organizations are equipped with an action plan and procedures to protect themselves against cyberattacks (Shackelford et al., 2014); (Sabillon et al., 2017), (Azmi et al., 2018).

There are three types of cyber security frameworks based on functions that are needed:

• **Control frameworks**: These give an overall strategy for the cybersecurity team of an organisation. They provide a basic set of security controls and assist in prioritising the implementation of such measures.

• **Program frameworks**: These frameworks help analyse the state of the organization's security programme and in the assessment of its degree of safety.

• **Risk frameworks**: Frameworks of this kind are used so that the procedures that are essential for risk assessment can be specified, and that the proper security measures and activities may be prioritised. This process helps in characterising, quantifying, and evaluating the threats to the organization's security.

A framework generally provides users with various advantages. To start with, it provides a comprehensive language and a systematic strategy to lowering the cyber security risk. It will also combine a variety of different protective responsibilities, which can then be tailored to the requirements of a specific organization. In addition, framework profiling enables businesses and other organisations to focus on the areas where may build whole new processes or make enhancements to the ones they may already have. These features along with the simple vocabulary renders it easier to have clear communication across the board and with consumers. The advantage of using frameworks is that it provides them with way the whole organisation handles the management of cyber security risks. The framework can thus be used as a tool for evaluation, during which the budget, the significance of the mission, and the risk appetite are evaluated (Donaldson et al., 2015); (Shackelford, Russell and Haut, 2015). Because, the cyber risk management framework integrates with the organization's risk management strategy, it is among most effective methods for preventing cyberattacks. Any organisation, regardless of its size or purpose, that does not implement any kind of cyber security policy stands the danger of suffering from different kinds of harm. Due to the absence of a comprehensive cyber security framework, a company is unable to determine which security programmes and firewalls are required to safeguard its data from being compromised by potentially hazardous online behaviour. The organisation does not have the resources required to either avoid cyber security attacks or react to those that have already occurred. Because of this, the organisation does not have the resources necessary to mount a defence against the threat. Companies are unable to develop a transparent command structure from the moment an attack is discovered if they do not have an established cyber security architecture (Radanliev et al., 2018); (Malatji, Von Solms and Marnewick, 2019); (Kim, Alfouzan and Kim, 2021).

Below are some of the comparative points on six important frameworks:

6.2 NIST

NIST focuses on measuring control maturity and aligning cybersecurity defences to organizational goals. Identify, protect, detect, respond, recover are the domains of NIST. The major advantage of NIST is that it is built on previous frameworks, it is also available for free and works with various compliance requirements. In its advanced second version, NIST's framework consist of a comprehensive set of best practices that an organization looking to improve their security posture can adopt. This includes detailed guidance on multiple security requirements like risk management, identity and access control, asset management, supply chain management, incident response planning, etc. One disadvantage of NIST is that it may represent known results. Also, with NIST it is difficult to determine action items.

6.3 ISO 27001

ISO 27001 focuses mainly on building security management programs consisting of the following domains: human resources, security policies, asset management, access control, and information security organization. The major pluses of ISO 27001 are that this framework is the most recognized international IT security framework and almost all of the compliance requirements are built based on this framework. ISO 27001 is an international standard framework that gives a very systematic approach not just risk assessment and control selection, but also implementation. Requirements for establishing an Information Security Management System (ISMS) is also included in the framework. Disadvantages of this framework being the high cost for the certification.

6.4 CIS

The focus of CIS is the protection and tracking of high-risk areas usually by using automated controls. The three categories of CIS Controls are: Basic, Foundational, and Organizational.

- The focus of **Basic Controls** is on the essential cybersecurity measures that should be implemented by all organizations like regular patching and antivirus protection.

- **Foundational Controls** are more advanced and additional measures that are required to be taken in addition to the fundamental security protocols like incorporating two-factor authentication and regular monitoring of log files for suspicious activity.

- **Organizational Controls** are specific to the needs of an organization's environment and are designed to provide additional protections like user awareness and training.

The advantages of this framework are its ease of use, clearly defined actionable items, and the framework being permanently updated. There are 20 controls included in the framework that cover most security areas like access control, asset management, and incident response. A group of IT experts are responsible for formulating the actionable best practices for cyber defence and these are done using the information gathered from actual attacks and their effective defences. The major advantage of CIS Controls is that it provides specific guidance and a clear path for organizations so that they can achieve the goals and objectives described not just by the policy frameworks but also by multiple legal and regulatory bodies. While the disadvantage is that the framework is not very comprehensive.

6.5 SOC2

The SOC or Service Organization Control framework is basically an auditing standard and is employed by third-party auditors to assess an organization’s systems and services for security, availability, processing integrity, confidentiality, and privacy. SOC2 is among the most prevalent standards specifically designed for cloud service providers.

An organization must provide detailed documentation on their internal processes and procedures related to security, availability, processing integrity, confidentiality, and privacy to meet the SOC standards. These SOC-compliant documents must include detailed policies on all the security related activities like access control measures, data encryption protocols, incident response plans, and more. This also requires the organizations to provide evidence of the effectiveness of their controls like audit logs or penetration test results. This helps to make sure that the security measures implemented are functioning correctly and can protect their data from cyber threats. The main disadvantage of SOC2 is that its implementation can be very time consuming and resource intensive. Also, since SOC 2 framework is intended to be scalable and flexible to accommodate the needs of different types of organizations, it may not cover all relevant controls for every organization.

6.6 CMMI

CMMI focuses on measuring software engineering process capabilities. CMMI domains include Product and services development, Service establishment, management, and Product and service acquisition. The advantages of CMMI CSF are that this framework is suitable for large software development companies and is improved continuously. The disadvantages are - focus is mainly on software development, so it is not very much suited for other organizations and it needs a well-defined role to work with.

6.7 COBIT 5

The focus of COBIT 5 is connecting business and IT goals together, setting up responsibilities, and measuring control maturity. Its domains include control objectives, description of the process, maturity models, and management guidelines. It offers best practices for governance along with risk management and security.

There are five categories in this framework: Plan & Organize, Acquire & Implement, Deliver & Support, Monitor & Evaluate, and Manage & Assess. Each of these categories contain specific processes and activities that help the organization in the effective management of its IT resources. Detailed data security and protection guidelines covering access control, user authentication, encryption, incident response, and audit logging areas are contained in COBIT. These guidelines provide a comprehensive set of measures that can be employed by organizations to protect their systems from cyber threats. The advantages of COBIT are that it works with many compliance requirements and the focus on IT governance. The major disadvantage of this framework is that it lacks cybersecurity components.

6.8 Conclusion

As can be seen from the above study of various frameworks, these are very generic and fail to tackle the specific requirements of education sector. There are many controls that are not necessary for the institutions and will become a burden to implement. Below is a summary of comparison between a few frameworks. As can be seen, there are way too many controls and activities. These are generic and can be adopted to any type of businesses. The study focusses on tailoring these to educational sector with minimum number of controls for ease of implementation.

Enterprise Cybersecurity		(ICS)^2 Common Body of		ISO 27001/27002 Version 2013		NIST SP899-53		Council on CyberSecurity	
11 Functional Areas		10 Security Domains		114 Controls in 14 Domains		224 Controls in 18 Families		20 Controls and 182 Control Activities	
1	System Administration	1	Access Control	1	Information Security Policies	1	Access Control	1	Inventory of Devices
2	Network Security	2	Telecommunications and Network Security	2	Organization of Information Security	2	Awareness and Training	2	Inventory of Software
3	Application Security	3	Information Security Governance and Risk Management	3	Human Resource Security	3	Audit and Accountability	3	Secure Configuration for Computers
4	Endpoint, Server and Device Security	4	Software Development	4	Asset Management	4	Security Accessment and Authorisation	4	Continuous Vulnerability Assessment and Remediation
5	Authentication, and Access Management	5	Cryptography	5	Access Control	5	Configuration Management	5	Malware Defenses
6	Data Protection and Cryptography	6	Security Architecture and Design	6	Cryptography	6	Contingency Planning	6	Application Software Security
7	Monitoring, Vulnerability, and Patch Management	7	Security Operations	7	Physical and Environmental Security	7	Identification and Authentication	7	Wireless Device Control
8	High Availability, Disaster Recovery, and Physical	8	Bussiness Continuity and Disaster Recovery Planning	8	Operations Security	8	Incident Response	8	Data Recorvery Capability
9	Incident Response	9	Legal, Regulations, Investigations and Compliance	9	Communications Security	9	Maintenance	9	Security Skills Assessment and Training
10	Asset Management and Supply Chain	10	Physical (Environmental) Security	10	Systems Acquisition, Development and Maintenance	10	Media Protection	10	Security Configurations for Network Devices
11	Policy, Audit, E-discovery, and Training			11	Supplier Relationship	11	Physical and Environmental Protection	11	Network Ports, Protocols, and Services
				12	Information Security Incident Management	12	Planning	12	Control of Administrative Privilages
				13	Information Security Aspect of Business Continuity Management	13	Personal Security	13	Boundry Defense
				14	Compliance	14	Risk Assessment	14	Security Audit Logs
						15	System and Services Acquisition	15	Need to Know Access Control
						16	System and Communications Protection	16	Account Monitoring and Control
						17	System and Information Integrity	17	Data Loss Prevention
						18	Program Management	18	Incident Response Capability
								19	Secure Network Engineering
								20	Penetration Testing and Red Team Excercises

Table 6.1: Summary of comparison of cybersecurity frameworks

The problem we want to solve here are:

- Compliance with multiple frameworks like ISO 27001, NIST, SOC 2 etc.
- Multiple audits are burdensome on the team:
    - 1000s of audit artifacts
    - Framework changes all the time
- Anxiety that something is missing.
- Audit/Compliance driving the process.
- Policies morph into compliance documents instead of useful guidance

Solution is to create a simple, easy to implement framework that is tailored to education sector with minimum controls that is emphasized on technology. This will be:

- A single framework strategy
- Reduces effort of compliance
- Saves team’s time and effort as well as money.
- Risk drives compliance and policies
- Policies represents real-world processes customized to the institutions’ operations.

CHAPTER VII

EDUSEC CONTROLS FRAMEWORK

7.1 EduSec Controls Framework Overview

Before a cyber-attack can take place, companies and organisations need to establish the best possible frameworks to keep track of, manage, and eliminate any threats to their online safety. Implementing and adhering to a cyber-security framework is the most effective technique for guaranteeing that users are protected in an online setting (M. I. Alshar'e, Sulaiman, Mokhtar, & MohdZin, 2014); (M. Alshar'e et al., 2022). Because it contains all the essential processes and instruments, this structure is an excellent choice for protecting the organization's resources. A framework is like a structure of beams that holds up a building but in the realm of ideas, it holds the system of data and how it is organized (Panda & Bower, 2020). The aim of the framework is to secure the data and information from criminals and hackers by removing its vulnerabilities and also researching its weak points and making it more difficult to access and difficult to take advantage of (Kahyaoglu & Caliyurt, 2018).

The proposed EduSec framework is an automated intelligent execution model that is based on a simple approach to guide educational institutes and its stakeholders like teachers, students, and the research community on how they can use the existing cybersecurity practices, what additional cybersecurity activities are needed to address the specificities of educational sector. It spans the five phases of the National Institute of Standards and Technology (NIST) cybersecurity framework and follows the CIA Triad's priorities. The framework involves implementation of multiple layers of security controls placed throughout an information technology system. To protect against the increasing volume and sophistication of cyberattacks such as ransomware, educational institutions need elevated security. Most of the institutions still rely on traditional protections like antivirus, which offers only a single layer of protection using signature matching and protects only against known threats. With EduSec, institutes get

multi-layered protection, detection, and response, spanning the five functions of the NIST cybersecurity framework—identify, protect, detect, respond, and recover—to protect and remediate against known and unknown threats. Below are the capabilities of this framework in detail:

Identify

- Identification of risk is the key to secure the system. This helps prioritize and focus on the vulnerabilities that pose the most urgent and highest risk to the organization. Hence it is important to identify, discover, prioritise, and remediate any software or hardware misconfigurations and vulnerabilities, so that a secure foundation for IT environment can be built proactively.

Protect

- Attack surface reduction is one of the ways to minimize the attack probability i.e., limiting or securing the devices and applications that are vulnerable to cyberattacks across the organization, leaving bad elements with fewer ways to perform attacks.
- Next-generation anti-malware and antivirus tools help prevent and protect against threats to the on-prim devices and the data in the cloud.

Detect and Respond

- Behaviour-based detection and alerts to identify persistent threats and removing them from the environment can be achieved through endpoint detection and response systems.

Recover

- It is important to scale the security operations by examining alerts and taking immediate action to resolve attacks using Auto-investigation and remediation tools. By reducing alert volume and remediating threats, tasks can be prioritized and focus can be made on more sophisticated threats.

7.1.1 PPT focused EduSec Framework

EduSec Cyber Security Framework is primarily a Technology Solution, though successful security solution is possible only by integrating People, Process, and Technology.

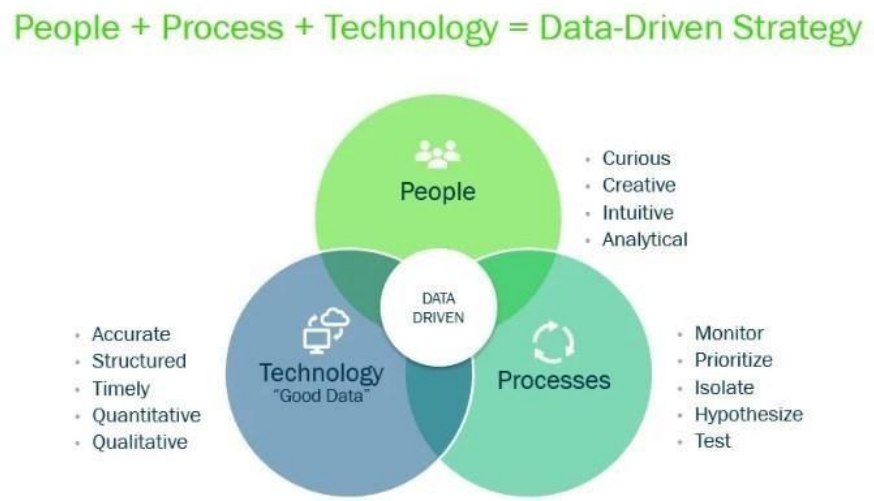

Figure 7.1: PPT Framework (www.linkedin.com, n.d.)

When designing the system, we need to carefully consider who are the users since it is people who make things happen by leveraging technology. Emphasis is on training and enabling the people to execute their roles in the security process effectively.

Process focuses on how to make things happen. Processes ensure efficiency by ensuring tasks are done optimally. EduSec framework recommends well defined processes for each step of the cybersecurity implementation journey.

With the current advancement in technology, it is this aspect that can be leveraged to make the framework efficient and easy to use. The investment in technology may be expensive, but the returns will be realized with data-driven decisions. EduSec Framework focuses on automation of each step in the security process. The technology that is employed are critical component of the framework. A variety of tools can be used to automate and monitor each activity related to attack, security breach and respond proactively.

7.1.2 EduSec is a 10 Point Framework for Security Controls:

The focus of EduSec framework is the protection and tracking of the IT systems in a layered approach using automated controls. It covers the following domains:

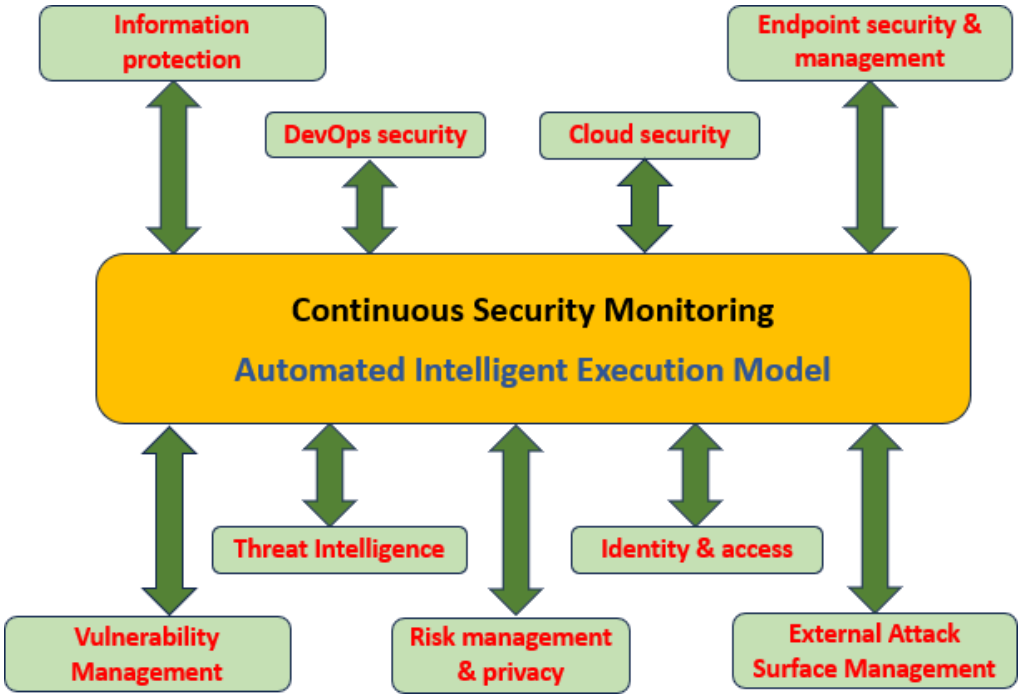

Figure 7.2: EduSec Framework with 10 Point Security Controls

1. Endpoint security & management
2. Cloud security
3. External Attack Surface Management

4. Vulnerability Management
5. Threat Intelligence
6. Information protection
7. Risk management & privacy
8. Identity & access
9. DevOps security
10. Security Continuous Monitoring

7.2 Endpoint Security & Management

The more endpoint devices connected to the institute's network, the more avenues' cybercriminals have to infiltrate that network. So, it is important to identify and secure all the endpoint devises including staff and students' personal devices using endpoint security management system. This is a software approach, normally centralized, to enable network administrators to identify and manage end users' device access within the institute's network.

Figure 7.3: Endpoint Security management (Anon, 2020)

Examples of endpoint security management include, but are not limited to:

- Managed antivirus software
- Web filtering

- Application/patch management
- Network access control
- Virtual private network (VPN) software
- Data and email encryption

Access permissions are set by the administrators according to the institute's security policy so that outsiders like guests, contractors, vendors and friends and family of staff and students have limited network access. Access can be set based on "need to know" so that users will only have access to areas of the network that is essential to fulfil their job responsibilities. This way, regardless of the number of devices connecting to the network, safety from security threats can be ensured. Administrators can control security for the endpoints using policy settings that depend on the type of protection or access a student or staff require and this can be achieved through endpoint security applications. Always ensuring that every device which connects to the network uses up-to-date antivirus software with latest patches and updates and block access to malicious websites is a very good example of end point security.

7.3 Cloud Security

These days most organizations use cloud for their data and application needs. Cloud Security protects this information stored in a digital environment. Various service providers like AWS, Azure, Google, etc., may be used to verify security against multiple threats in the cloud.

Cloud security is a responsibility shared between the cloud service provider and consumer. In a shared responsibility model, there are three categories of responsibilities – those that are provider's, those that are the customers, and those that change depending on the model.

The provider's responsibilities are related to the protecting the infrastructure and controlling its access along with patching and configuration of the network. The customer's responsibilities include managing users and controlling their access to the cloud, encryption of data in the

cloud, safeguarding of cloud accounts, and managing the security compliance. The third category of responsibilities vary based on cloud platform being used such as Infrastructure as a Service (IaaS), Platform as a Service (PaaS), or Software as a Service (SaaS).

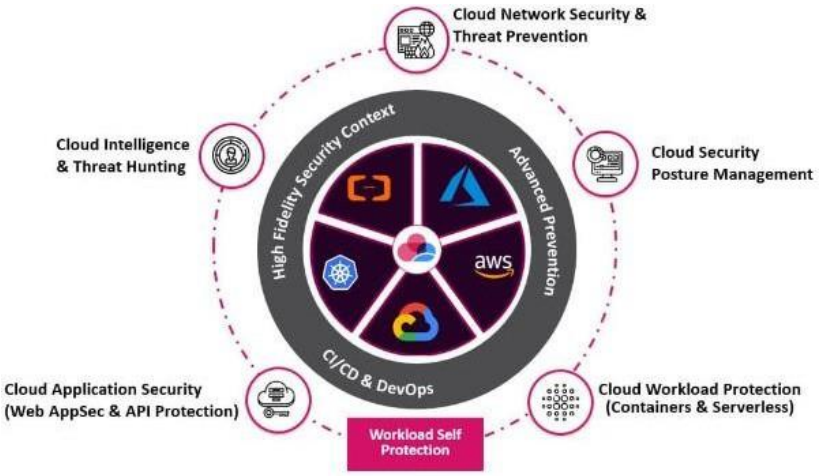

Figure 7.4: Cloud Security (Check Point)

In this framework, a Cloud security platform that integrates seamlessly with the providers' security services is recommended. This ensures that cloud users align with Shared Responsibility Model and maintain Zero Trust policies across all security requirements like access control, virtual server compliance, data protection, and threat intelligence.

7.4 External Attack Surface Management

7.4.1 External attack surface management

The process of identifying, analysing vulnerabilities and mitigating risks associated with an organization's external-facing digital assets, like websites, applications, and network infrastructure is called External attack surface management or EASM. This requires continuous monitoring of the exposed attack surface for breaches and unauthorised access to ensure security. To understand and manage all the ways an attacker might get into the organization's network is the best way to protect it.

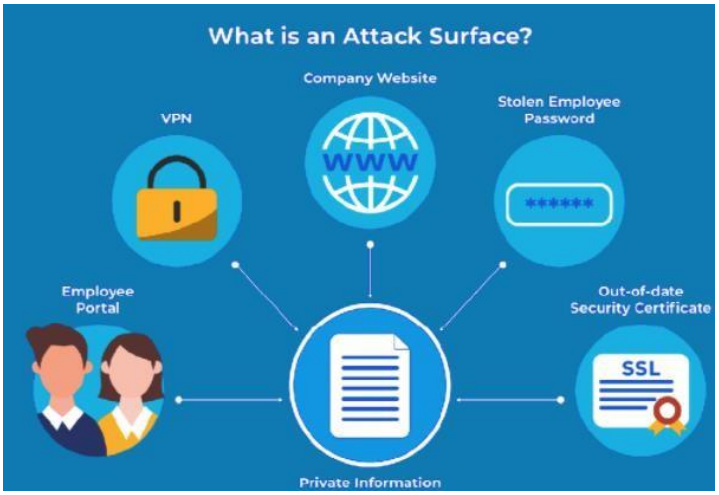

Figure 7.5 External Attack Surface (Acanerler, 2021).

An organization's entire internet-facing digital assets that are vulnerable to cyber-attack is called the External Attack Surface or Digital Attack Surface. Some such assets are servers, operating systems, domain names, SSL certificates, IoT and security devices, IP blocks. These can either be located on-prim or in the cloud or can also be housed by a third-party vendor.

Threat actors can access any of these assets, therefore, the best way to protect the organization is to understand and manage all the different ways a hacker can reach the organization. The attack surface cannot be fully protected until all the assets the attackers are exposed to are secured and this can be achieved by adopting an outside-in and an external attack surface management perspective.

7.4.2 Key Elements for External Attack Surface Management and Protection

1. **Digital footprint discovery:** The first step for external attack surface management is to identify all the organization's assets that are exposed to the internet like websites, IPs, domains, SSL certificates, and cloud services. Organizations can have many assets that they have forgotten or are not aware of, as well as assets that they know and manage. Any asset that is forgotten or not configured for security is a risk.

2. **Asset inventory and classification:** It is important to understand the owner of the asset and how it is networked. It is essential to create an accurately classified inventory so that the people responsible have quick access to the assets they manage.
3. **Evaluation:** Once all the assets in the IT ecosystem are identified and classified, it is crucial to evaluate them for risks. Attackers just need a single opportunity, so it is important to identify misconfigured assets, network architecture flaws, data vulnerabilities, authentication and encryption weaknesses, or any other risk, including common vulnerabilities and exposures (CVE). These vulnerabilities on the external attack surface can be detected using multiple security testing techniques and then the results correlated to identify attack vectors that threat actors can use.
4. **Prioritization:** Prioritizing risks on the external attack surface ensures that focus is where should be. Due to the volume of security issues and alerts organizations face it is nearly impossible to manage without prioritization. The goal is to increase the productivity of the team by reducing false positives. Correcting risks such as misconfigurations, open ports, and unpatched vulnerabilities in an order of urgency, severity, and risk is vital to achieving this goal.
5. **Continuous security monitoring/Fixing:** The assets of organizations are constantly changing, increasing in number, and being updated every day. It is difficult to keep track of updated assets as the digital asset inventory grows. Along with this, the 3rd party applications running on assets may introduce security vulnerabilities that can be easily exploited. Therefore, it is critical to ensure continuous 24/7 monitoring of digital assets for all vulnerabilities and misconfigurations including the newly discovered ones.

It is important to make remediation functional for external attack surface management as refinement is very critical to attack surface protection.

7.5 Vulnerability Management

Vulnerability management is an important part of an overall security program and is often automated, continuous, and proactive process that helps keep the IT systems safe from cyber-attacks and data breaches. The four steps of vulnerability management are:

1. Identifying vulnerabilities.
2. Evaluating and prioritizing vulnerabilities.
3. Reporting vulnerabilities.
4. Remediating the identified vulnerabilities.

Figure 7.6: Vulnerability Management Process (Chaitra S, 2022)

7.5.1 Identifying Vulnerabilities:

- Vulnerability scanners can be employed to identify the devices that are prone to risk in an organization's network.
- With the help of a vulnerability database that contains publicly known vulnerabilities, vulnerability scanners can associate known vulnerabilities to scanned devices.
- This information helps to maintain up-to-date vulnerability data and can be used to create reports for the stakeholders.

7.5.2 Evaluating and Prioritizing Vulnerabilities:

- Once the identification of vulnerabilities is completed, they must be evaluated as per their severity level.
- Prioritization of vulnerabilities based on CVSS (common vulnerability scoring system) can be done using vulnerability management solutions. CVSS scores the vulnerabilities between 1-10 based on their severity.
- There are two types of errors that may be seen while evaluating vulnerabilities:
    - Type 1 error: False positive where vulnerabilities are reported that don't actually exist.
    - Type 2 error: False negative where vulnerabilities are not reported even though they are present.

7.5.3 Reporting Vulnerabilities:

- Reporting the identified vulnerabilities and their risk to the organization can be done by the vulnerability scanning tools so that the stakeholders are aware. This also helps the people who are responsible to take remedial actions.

7.5.4 Remediating the Identified Vulnerabilities:

The next step after vulnerabilities is identified and prioritized, is to remediate them. Vulnerabilities can be treated in different ways:

- **Remediation:** This is the process of patching vulnerabilities before it becomes a security threat. Once the required patches are applied, it is advised to have another round of scans to ensure all the weaknesses are remediated.

- **Mitigation:** Mitigation is the means of reducing the impact of vulnerability being exploited which becomes vital when there is no proper patch available. It only acts as a temporary solution and does not eliminate vulnerabilities.
- **Acceptance:** No action is taken. When there are low-risk vulnerabilities, and the cost of fixing them is greater, sometimes it is decided not to take any action to fix them. But it is dangerous to avoid addressing known vulnerabilities. Therefore, this is choice that should be used only if there is no significant impact on the organization.

7.5.5 Tools for Vulnerability Management

There are many tools and solutions that help in threat and vulnerability management and prevent and address cyberthreats. These tools proactively look for weaknesses in the system by scanning and identifying assets and its vulnerabilities. They also provide remediation and mitigate suggestions for future security breaches and thus help an organization stay one step ahead of hackers.

7.5.6 Asset Discovery and Inventory

The organization's IT is responsible for tracking and maintaining records of IT assets including servers and other digital devices, software, and more across the organization's digital environment. This exercise can be extremely complex due to the volume of assets and their spread in different locations. This is where asset inventory management systems help provide visibility into all assets that an organization has along with its location, and usage.

7.5.7 Vulnerability Scanning

Vulnerability scanners are employed to look for common weaknesses or flaws by running a series of tests against systems and networks. These tests include attempting to exploit known

vulnerabilities, trying to gain access to restricted areas, or guessing default passwords for user accounts.

7.5.8 Patch Management

Patch management is essential to keep the computer systems up to date with the latest security patches. Most patch management solutions and tools come with the capability of not just automatically checking for updates but also notifying the user when new ones are available. Some of these tools also take care of deploying patches across multiple computers in an organization, so that large fleets of machines are kept secure.

7.5.9 Configuration Management

Security Configuration Management (SCM) software or tool is used to make sure that all device configurations are secured, that any changes to the security settings of a device is properly tracked and approved, and that all systems are security policy compliant. Most SCM tools function as vulnerability management tools and also ensure security policy compliance.

7.6 Threat Intelligence

7.6.1 Cyber Threat Intelligence

Cyber threat intelligence (CTI) is a way of understanding and analysing threat data that can be later used to prevent or mitigate cyber-attacks. In a large organization with complex security infrastructure, it is challenging to have complete oversight of the network. In such cases CTI will help identify the risks and highlight potential threats and recommend remediation methods. There are 3 different levels on which this intelligence can be identified – strategic, operational, and tactical:

Tactical intelligence is conceived to defend against specific threats in real-time. Threat data is collected as and when the security incidents occur. The tool then informs how remediation is performed.

Operational intelligence takes an overview of potential threats. The collected data is used to gauge risk and provide alerts that can help the security team understand the scope of an attack and provide defence against it. This includes insights on how and where the attack occurred and how likely the attack is to happen in the future. This strengthens overall security posture by correcting remediation policies and helps in the configuration of tools to proactively take action against potential threats.

Strategic intelligence is a high-level overview of the organization's threat landscape. It uses intel data collections, historical observations, and research to identify geographic, political, and business trends and create long-term plans. This type of intelligence will present broad trends and help define a company's security posture.

7.6.2 The Cyber Threat Intelligence Lifecycle

Cyber threat intelligence is a closed loop consisting of six phases. It can be used to analyse a range of threats and ensure that the analysis is correctly aligned with risk management and business objectives.

Figure 7.7: Cyber Threat Intelligence Lifecycle (Cymune)

Direction: The first step is to plan the goals of collecting threat intelligence, and the information that should be collected based on the requirements of key stakeholders in the shortest possible time frame. This helps define objectives and establish the goal of threat intelligence.

Collection: This can include collecting both digital and physical evidence depending on the kind of incident. These may be IP addresses, audit logs, CCTV footage and also physical devices depending on the sort of the attack. This means the data will be in huge amounts sometimes in terabytes, and hence will need good planning, storage, and processing capabilities.

Processing: Once data is collected, the next step is to process the raw data into more organized and decipherable forms. This involves decoding the information, grouping, and organizing the data, tagging information that fits a specific context or source.

Analysis: Analysis involves summarising the collected data, interpreting the data using analytical and logical methods to determine patterns, relationships, and/or trends. It may also include further analysis of any contradictory information for comparison and clearer understanding of the events as they unfolded. Once patterns and other evidence emerge, it may require even further analysis. This is one of the most time-consuming stages of the cycle and will need human analyst to lead, though it can be aided by tools.

Dissemination: In this stage the reports generated from the analysis stage is shared with the key decision makers and stakeholders so that appropriate action can be taken.

Feedback: The cycle is only effective if there is continuous improvement, and this can only be achieved through feedback. Action is taken on the basis of the feedback from all the previous

stage in the cycle. Actions may include implementation of a new security feature, retaliation, or it could be adding more data to the cycle for recanalization.

7.7 Information Protection

7.7.1 Information Protection

Protection of data and information systems from unauthorised access and use, disclosure, modification, disruption, or destruction is referred as Information protection or Information security. This is very important and will provide:

- **Confidentiality:** Confidentiality means protecting data from access and disclosure by unauthorised persons. It includes protection of personal privacy and proprietary information.
- **Integrity**: Integrity refers to guarding the data against illegal information modification or destruction. It includes ensuring information authenticity and non-repudiation.
- **Availability:** Availability means ensuring information is available for use in a timely and reliable manner.

Information protection employs different means including security solutions like encryption, and other technologies, and also policies and processes, to secure information.

7.7.2 Components of Information Security Policy

The scope of a security policy can be very broad and includes everything related to IT security along with the security of related physical assets. Some important considerations when an information security policy is developed are listed below:

1. **Purpose:** The purpose of the policy should be to define an overall methodology to information security like security requirements, standards, and best practices. It will involve detecting and averting information security breach, upholding ethical and legal responsibilities and applicable governance.
2. **Audience:** This includes understanding to whom the policy applies and would also specify which audiences are out of the scope of the policy.
3. **Information Security Objectives:**It is essential to have well-defined objectives for strategy that is agreed upon by the team. The three most important objectives are:

   Confidentiality —Authentication and access control is used in such a way that only authorized persons will be able to access information assets.

   Integrity — IT systems can be kept operational only if the critical data contained within is unharmed, accurate and complete, and.

   Availability — Data is available for the users when needed.

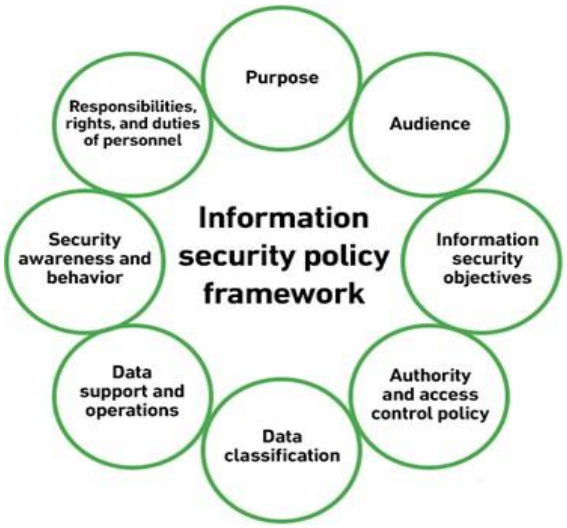

Figure 7.8: Information Security Policy Framework (Exabeam)

4. **Authority and Access Control Policy**

- **Hierarchical Pattern** —The policy should clearly define the level of authority over data and IT systems for every role in the organization.
- **Network Security Policy** — This policy should ensure approval and enforcing of critical patching and other threat mitigation policies. It also includes clear access control policies like passwords, biometrics, ID cards, or tokens and monitoring and recording login attempts of all systems.

5. **Data Classification**

The data classification policy should classify data into categories based on level of sensitivity, the risks. This will help in understanding which systems and operations touch the most sensitive and controlled data, so that security controls can be properly designed. It also ensures proper access control for sensitive data and avoids needless security measures for unimportant data.

6. **Data Support and Operations**

- **Data Protection Regulations** — It is important that sensitive data is protected according to organizational and industry compliance standards, best practices, and relevant regulations. At a minimum almost all security standards require, data encryption, anti-malware protection, and a firewall.
- **Data Backup** — All data including those in motion and at rest should be encrypted and backed-up according to industry best practices. Also, this backed-up data should be securely stored.
- **Movement of Data** — Data should be transferred only via secure protocols and any data that is transmitted over the public network should be encrypted.

7. **Security Awareness and Behaviour**

IT security policies should be available to all the staff and other stakeholders. Training sessions should be conducted regularly to inform staff and students regarding security procedures and mechanisms, including data and access protection measure and sensitive data classification.

Social Engineering — All students and staff should be made aware of social engineering attacks such as phishing emails or informational requests via phone calls so that they are capable of noticing, preventing, and reporting these kinds of attacks.

Clean Desk Policy — It is important to clear the desk and printer areas so that documents do not fall into the wrong hands. Sensitive document should be shredded, and laptops and desktops should be locked when not in use.

Internet Usage Policy helps to restrict usage of internet using firewalls, blocking of websites that are against organization policy of usage, etc.

8. Encryption Policy

Encryption is encoding of data in such a way that it is not accessible to unauthorized people. This is done to protect not just the stored data but also data that is in transit between locations to ensure privacy of sensitive and proprietary data. Organizations require an encryption policy to define which media and devices require encryption and when it is mandatory. It should also clearly define the minimum standard that is applicable to the encryption software chosen.

9. Data Backup Policy

A data backup policy is an integral component of overall data protection, business continuity, and disaster recovery strategy and defines rules and measures for creating backup copies of data. This policy will identify information that should be backed up and determines the frequency of backups for both full and incremental backups. It also defines a storage location for the backup data and roles and responsibilities of the IT team with respect to backup process.

10. Responsibilities and Duties

Key roles and responsibilities of Institutional Information and IT Resources in regard to data protection should be clearly defined in the security policy. Responsibilities range in scope from the safeguard of one's own password to user access reviews, education change management, incident management, implementation of security controls administration, as well as periodic updates of the security policy.

11. System Hardening Benchmarks

The information security policy should reference which security benchmarks and best practices the organization should use to strengthen the systems, network, and infrastructure. It involves implementing controls using tools and techniques to reduce threats. The policy should align with hardening guidelines like CIS and NIST to ensure protecting the infrastructure and systems as well as implementing continuous monitoring.

12. References to Regulations and Compliance Standards

The information security policy should reference regulations and compliance standards that impact the organization. It should consider the Information Technology Act, the SPDI Rules for Reasonable Security Practices, the National Cyber Security Policy and the IT rules which help meet the security practices under Indian jurisdiction.

7.8 Risk Management & Privacy

7.8.1 Privacy Risk

EduSec Framework leverages the ISO Privacy Framework to help institutes protect data privacy and minimize the potential loss of control over personal information. PII or personally

identifiable information is that information about a person which can be used to distinguish or trace an individual's identity, like name, national identification number, date and place of birth, biometric records, etc. It also includes any other information that is linked to a person like health, educational, employment, and financial records. EduSec framework uses ISO framework as a guide in implementing Privacy Risk Management as shown below.

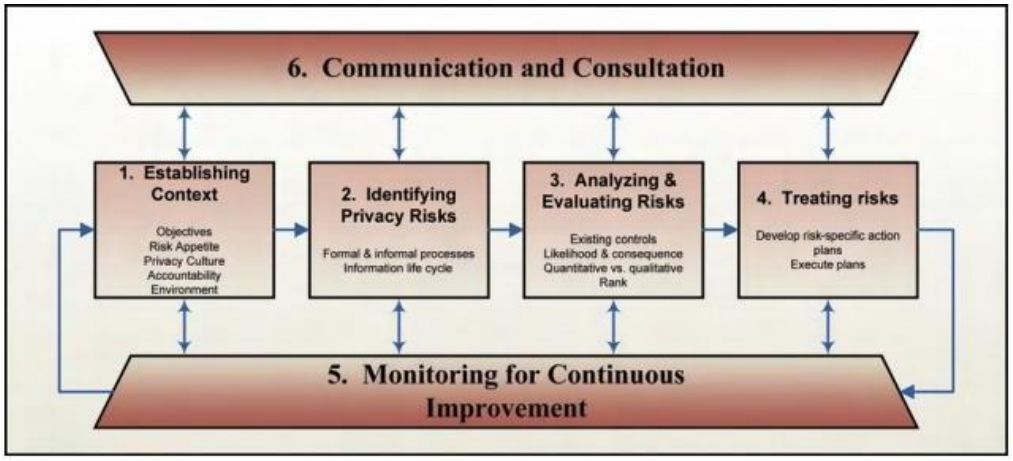

Figure 7.9: Privacy Risk Management Framework (Information and Privacy Commissioner, 2010)

7.8.2 Establishing Context

Establishing context and setting the scope is the prerequisite for privacy risk management. It is important to understand both external and internal contexts that affect privacy as management of PI or personal information and corresponding risks is within the purview of the institute's broad strategic risk management environment. External context may include consideration of social, legal, technological, competitive environment. PI should be managed through documented operating practices, roles, and responsibilities.

7.8.3 Identifying Privacy Risks

It is critical to identify of potential privacy risks so that they may be eliminated or, at least, mitigated to effectively protect personal information. Privacy risks are mainly operational risks that cause direct or indirect loss due to inadequate or failed internal processes and systems. While identifying privacy risks it is also important to consider institute's outsourced service providers, as they are often overlooked. Institutes can leverage Privacy audits and Privacy Impact Assessment processes to identify privacy risks. In addition, they can also engage any of the below techniques depending on their requirements:

- Developing a Culture of Privacy Protection
- Listening to Feedback from Employees and Business Partners
- Examining the Key Business Processes
- Reviewing Third Party Processes
- Performing Self-Assessments and audits
- Establishing Privacy Committees
- Analysing & Evaluating Risks

Though it is important to identify each of the risks faced by the institute, it must be acknowledged that very few institutes will own resources necessary to manage all of them effectively. Hence it is essential to do risk triage or ranking or all the identified risks according to the organization's policies. Separating them as minor which will possibly be acceptable risks and major ones that needs mitigation is required. Analysis and evaluation of these risks may also yield insight into proper treatment strategies as all risks do not warrant the same degree of attention. Analysis of privacy risks and evaluating them to determine if they require active treatment or need only monitoring can be done using well-established risk management processes and tools. But all the identified risks should be plotted and monitored, even if they are trivial, since sometimes even the most inoffensive risk might become significant.

7.8.4 Treating Risks

Once privacy risks are identified and assessed, next step is to determine the ways of addressing or treating them. Proactive treatment strategies can be employed as a matter of policy that include the following:

- Limiting collection, use, disclosure, and retention of personal information should be practiced, ensuring compliance with privacy laws, following Fair Information Practices, and Industry best practices.
- A good top-down / bottom-up privacy culture should be fostered in the organizations by establishing oversight and accountability.
- Establish a privacy policy and practices to clarify all personal information management requirements.
- Establishing complaint and feedback mechanisms to address privacy concerns.
- Privacy should be incorporated as part of ongoing quality assurance activity and protection performance should be monitored through audits so that gaps are identified and any enhancements needed are added.
- Appropriate escalation mechanism should be established to ensure proper management in case of a major privacy incident by developing good response protocols.
- Vulnerabilities should be identified using Performing Privacy Impact Assessments and Information Life Cycle Audits.
- Advanced encryption techniques should be used to ensure that personal information is suitably secured.
- Regular trainings should be providing for awareness and employee communications and debrief discussions should follow any privacy incident.

- Regular review of privacy incidents and analysis should be conducted so that insights from the analysis can be incorporated to enhance processes and systems.

Focusing on prevention is the best and the most effective strategy to address privacy risk. Using the most appropriate and practical techniques from among the listed ones, an effective strategy to mitigate privacy risk should be established.

7.8.5 Monitoring for Continuous Improvement

Monitoring is among most essential steps in the Security management process. Monitoring is required to determine if the chosen strategy is effective and has achieved desired results. Privacy risks continuously evolve with time, and monitoring will reveal the necessity of introducing new strategies and will also satisfy legal and public expectations.

Monitoring, collecting data and established trends in privacy incidents and complaints will help enhance the organization's privacy protection efforts and process improvements where needed. Monitoring along with early warnings is also good governance and will ensure protection and enhance value for the organization.

7.8.6 Communication and Consultation

It is very essential to have ongoing communication with both internal and external stakeholders in managing privacy risk. Communication policy should establish methods to communicate changes in privacy policy with all stakeholders, providing needed reports to management and Board on effectiveness of privacy measures, establishing a good response plan for communicating in the event of a privacy breach, and creating a feedback mechanism for privacy issues.

7.9 Identity and Access Management

Identity and access management (IAM) system ensures that the right people and right job roles in the institutes can access the tools and systems that they need to perform their jobs. This system will enable the administrator to manage all apps without logging into each app individually.

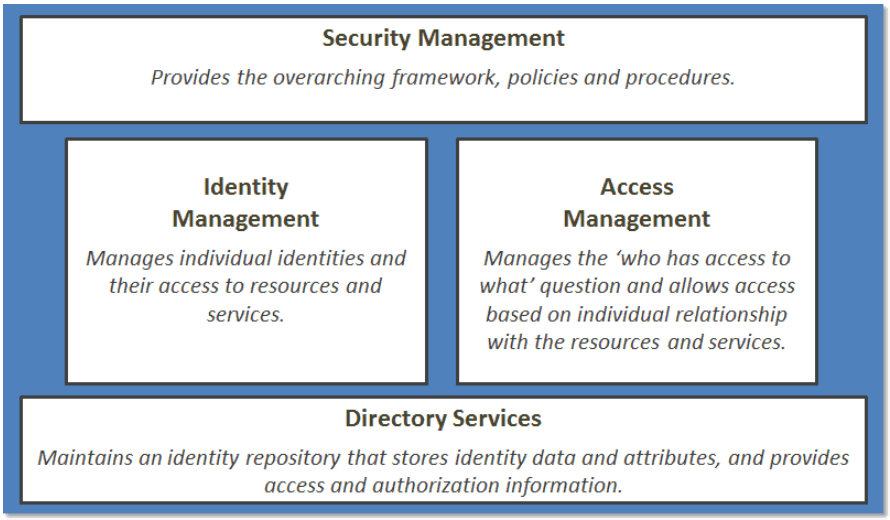

Figure 7.10: Identity and Access Management (www.interfacett.com, n.d.)

Identity and Access Management (IAM) solution should be implemented using zero-trust principles like least privilege access and identity-based security policies.

7.9.1 Central Identity Management

A centralized management of identities will help simplify the management of access to resources at the identity level which is the key principle of zero trust policy. This includes synchronizing IAM with other user directories or migrating users from other systems.

7.9.2 Secure Access

It is essential to confirm the identities of users as securing at the identity level is the key, which means implementation of multi-factor authentication or a combination of MFA and adaptive authentication which will consider context of login attempt like location, device, time, etc.

7.9.3 Policy-Based Control

Authorization or privilege should be limited to perform required tasks only and no more privilege than necessary should be given to the user. This can be achieved by IAM using job role-based access control. This way, centrally managed identity solution policies can ensure that resources are secure irrespective of the location of access.

7.9.4 Zero-Trust Policy

Users' identity and access points should be constantly monitored and secured by IAM solution as part of the zero-trust policy. Historically, the process was that, once a person was in, access is given always. But zero-trust policy ensures each user is constantly identified and their access managed.

7.9.5 Secured Privileged Accounts

All users do not need access to everything, so user accounts are created with different levels of access. Accounts with privileged access to sensitive information can be provided with additional tier of security and support that suits their status.

7.9.6 Training and Support

Training users including administrators is an integral part of implementing IAM. This will ensure effective implementation of access control.

7.10 DevOps Security

DevSecOps or DevOps security combines the three phases: Development, Operations, Security and focuses on application development and development operations (DevOps). DevOps security help bridge the gap between the organization's software development and IT operations by eliminating the barriers and establishing fast communication and collaboration.

The philosophy of DevOps security is to cover the developers' code and its subsequent need to work well in its implemented environment.

Figure 7.11: DevOps Security (Gallagher P, 2023)

DevOps works well in terms of vigilance and evolution, and these are essential to the success of security in any software development. But to bring this in practice requires active and well-aligned action plan. It is also essential for the developers to learn to elevate security concerns and making them part the development process. Awareness on security best practices should be part of DevOps training along with certifications schemes.

Below are some of the practices to ensure proper consideration is given to security:

- Security should be treated as a continuous priority.
- Build awareness on changing digital landscape and latest in security threats.
- Encourage communication and collaboration between teams.
- Smart automation to increase efficiency and reliability by replacing manual processes.
- Continuous improvement to manage security threats that are continuously evolving.
- Act quickly as undiagnosed issues can increase in scale over time.
- Tool and access security using privileged access management.

7.11 Continuous Security Monitoring

The practice of continuously assessing an organization's security posture to identify risks or vulnerabilities real-time is called CSM or Continuous security monitoring. It is a proactive approach to help organizations detect and respond to security threats even before they cause any real damage (www.jit.io, n.d.). CSM augments other security practices like vulnerability management and incident response and helps reduce their overall security risk in the organization. There are many Continuous Security Monitoring tools that aid administrators in real-time to identify and respond to security threats.

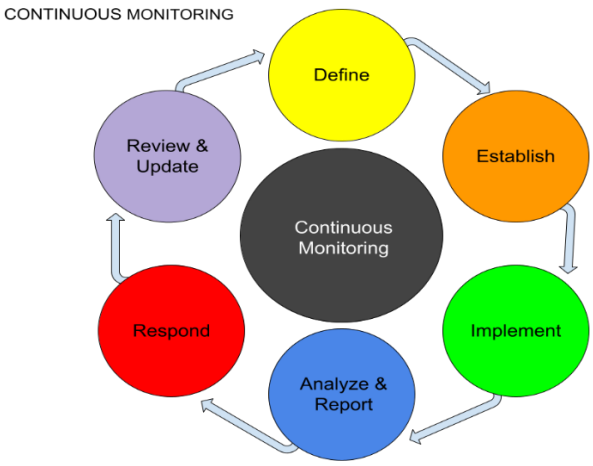

Figure 7.12: Continuous Security Monitoring Process (Ruck, 2021)

Data collection can be done from sources like network traffic, user activity and system event logs by CSM tools to analyse for signs of suspicious or unusual activity. CSM tools are equipped to generate alert if a potential security threat is detected so that appropriate action can be taken without delay. It is important to keep the CSM tools up to date with latest security intelligence and they must also integrate with other security tools to be effective.

7.11.1 Types of Continuous Monitoring

An integral part of any organization's security program, Continuous monitoring process, monitors and assesses security controls on an ongoing basis so that issues can be resolved without any delay. The three types of continuous monitoring are:

Infrastructure Monitoring: Monitoring the physical components of an IT system, like storage, and networking equipment and servers. Helps identify problems with the hardware.

Application Monitoring: Monitoring the software components of an IT system which includes the database and the application code or software. Helps in identifying problems like slow performance or memory leaks.

Network Monitoring: Monitoring the network traffic of the system that includes devices like routers, switches, and other networking equipment. Helps in identifying problems like high latency or packet loss.

7.12 Conclusion

Finally, education institutions do not entirely get to pick and choose their compliance standards because of various constraints and budgetary limitations they face. However, when adopting a general framework, EduSec is best suited for its simplicity, ease of implantation, limited number of controls and subsequently lesser measures for audit compliance. Securing student information is a legal obligation for colleges and universities. In today's digital world, nobody likes to work with organizations that cannot protect their information. Heavy fines and penalties can drain away financial resources and often create a cascading effect that no institution would like to endure. Therefore, it is strongly recommended that these institutes assess the gaps in their current cybersecurity posture and immediately begin to design and implement plans in order to close those gaps using the EduSec framework as a model.

In the next chapter, a detailed implementation plan is recommended as a successful Cybersecurity strategy for the educational institutions.

CHAPTER VIII

EDUSEC CONTROLS FRAMEWORK IMPLEMENTATION

8.1 Overview of EduSec Implementation Process

A well-defined plan that is guided by best practices but is specific for the current requirement is essential to effectively protect the institute from both internal and external threats. This plan or strategy should establish a baseline for the institute's security program and allow for adaptation so that emerging threats and risks can be handled effectively.

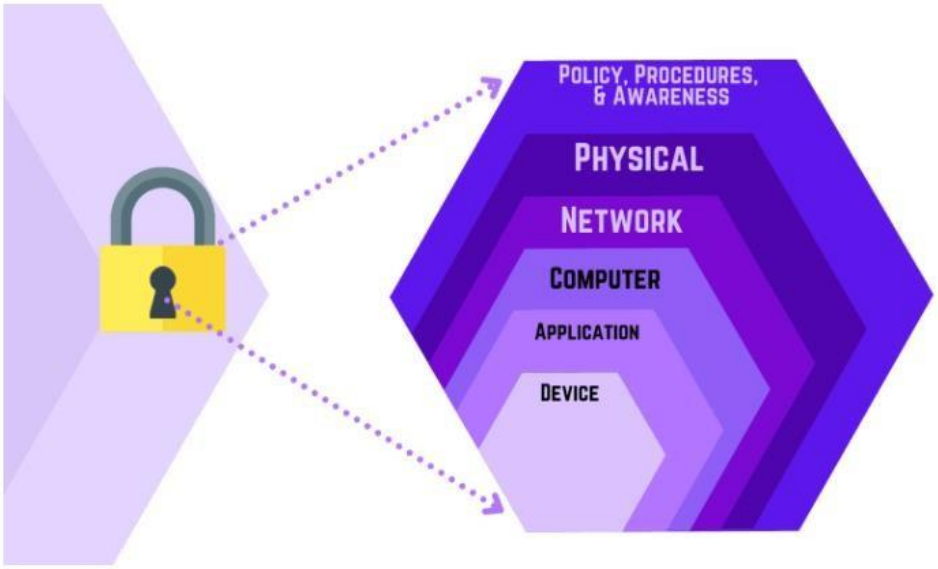

Figure 8.1: Layering of security defences (PurpleSec, n.d.).

The objective of adopting this strategy is layer the security defences with multiple tools to create defence in depth approach (PurpleSec, n.d.).

Figure 8.2: Security Policy enforcement using multiple tools (PurpleSec, n.d.)

The Education Sector Specific Cybersecurity Controls (EduSec) Framework implementation will be based on optimum cybersecurity controls for critical assets following CIA Triad priorities. The implementation process of EduSec framework can be done in seven easy steps, as indicated in Figure 8.3.

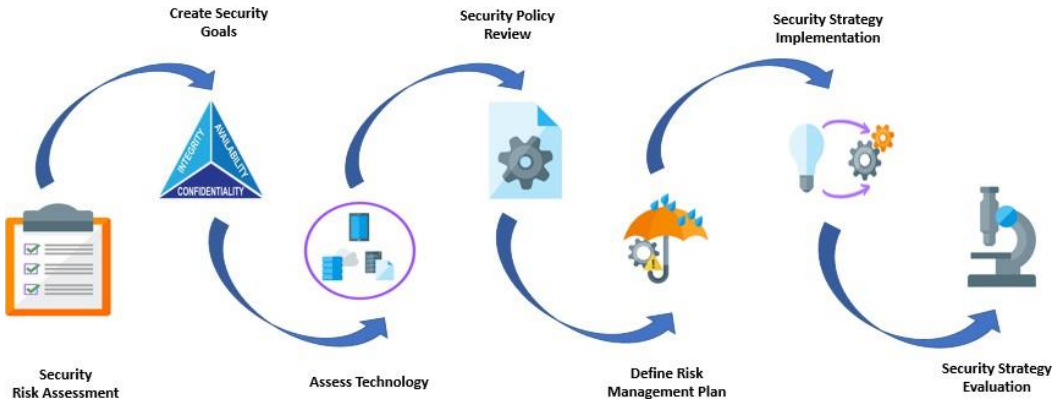

Figure 8.3: EduSec framework implementation steps

Each organization has its specific needs when it comes to cyber security. When it comes to implementing the cyber-security, one size fits all approach will not work. In this section, we

will walk through the eight recommended steps that can act as a model in developing and implementing a successful cybersecurity strategy for an educational institute.

8.2 Step 1: Security Risk Assessment

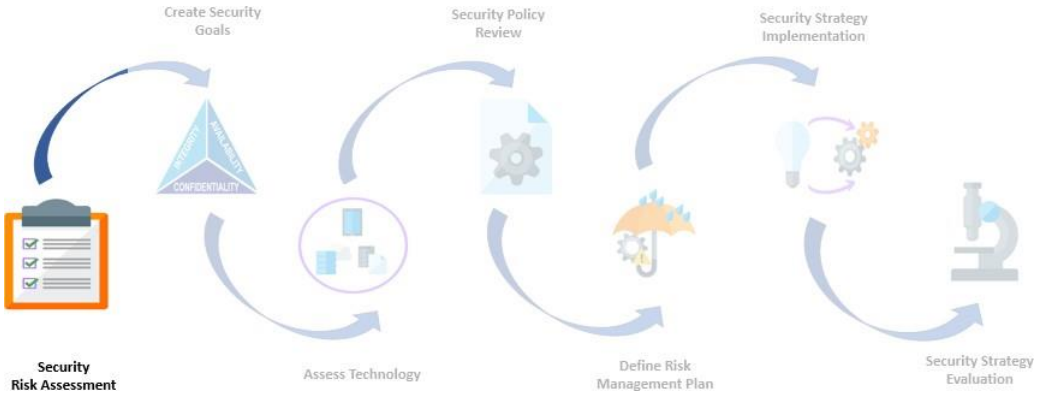

Figure 8.4: Step 1 – Conduct Security Risk Assessment

The very first step in the implementation is to conduct an IT enterprise security risk assessment and will require collaboration from multiple groups and data owners. This step is essential to assess, identify, and if required modify the overall security posture of the organization. This helps in obtaining management's commitment to the cybersecurity program so that funds and resource allocation is guaranteed. Not all assets belonging to the organization is critical and it will be a wasted effort if all the assets are given the same kind of security. Hence a thorough security risk assessment should be done to determine the value of all the different types of data generated and stored across the organization. This way prioritization of assets is possible and thus appropriate allocation technology resources. Identification of data sources is essential in accurately assessing the risk as well as the location of the data and the associated vulnerabilities.

Identification of Assets is done using the current asset tracking system to build a repository containing all assets like servers, workstations, laptops, operating systems, applications, institute owned mobile devices, etc.

Data Classifications should be done based on sensitivity of data and the risk associated.

- **Public** – data that is shared publicly for example, published research papers, website content. This information if breached may not have any negative impact.
- **Confidential** – data that should not be shared with the public such as ongoing research program information, student demographic information, etc. Non-Disclosure Agreement (NDA) or other protections may be required to prevent unauthorised access of such data or information.
- **Internal Use Only** – confidential data that should be maintained within the organization and should not be shared at all with outsiders.
- **Intellectual Property** – This is very critical to the institute. If this data is breached, it may damage the institute's reputation and impact its competitiveness.
- **Compliance Restricted Data** – This is the data that should be controlled and accessed according the compliance policies of the framework.

It is important to map assets with resources, location etc and create a comprehensive infrastructure topology. Below are some of the ways in which different categories of assets are mapped:

- **Software** – A repository for authorized corporate software is maintained.
- **Systems** –Central Management Database (CMDB) can be used for asset mapping back to a system or asset owner.
- **Users** – Users should be grouped based on role assignments, example Active Directory.
- **Identity** – Asset assignments should be regularly tracked to users based on their current role.

Identifying the Threat Landscape: This includes identifying all the vulnerabilities both identified and potential that represent danger to the institute. A complete analysis should be done including working with legal teams to identify 3rd party contracts, NDAs etc.

External vs internal infrastructure should be analysed to identify all egress and ingress points of the network.

Map where environments connect by ensuring network diagrams are up to date and available.

Prioritize Risks by performing impact analysis to identify critical systems and data owners. Risk register can help in identifying systems or assets that pose the greatest risk to the Confidentiality, Integrity, and Availability.

Reduce Business's Attack Surface by implementing network segmentation, conducting penetration testing and perform vulnerability management.

8.3 Step 2: Create Security Goals

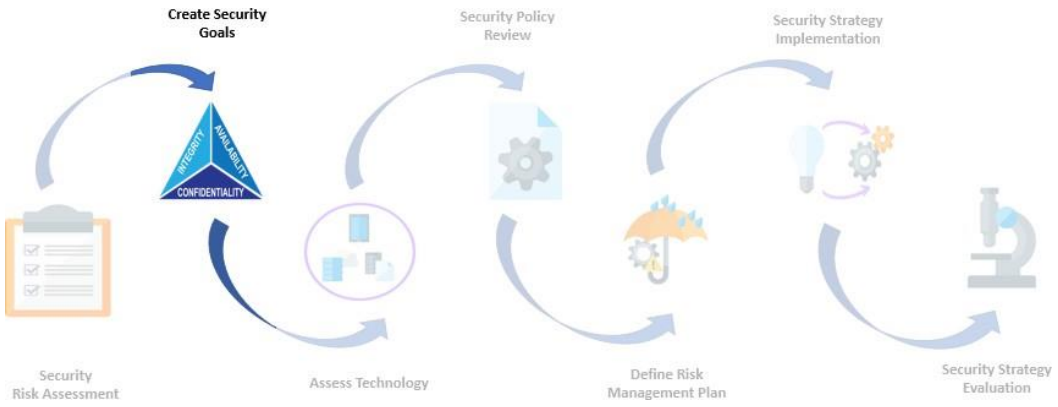

Figure 8.5: Step 2 – Create Security Goals

The most important factor in a cyber-security strategy is to ensure that it aligns with the overall goals and mission of the institute. Various areas that may help in creating the security goals are detailed in this section.

Determine Security Maturity

- Assess security program by reviewing the current posture, incident logs, and performance of various security management systems.
- Review the SLAs and KPIs to determine the status of the metrics.
- Measure the maturity of the institute's cybersecurity capabilities and benchmark the current state.

Understand the Organization's Risk Appetite

Cyber security should be prioritized on the basis of the output from a risk register and impact analysis.

Set Reasonable Expectations

It is necessary to have proper expectations that takes into account existing limitations of budget, resources, timelines, and ability to execute.

Handle Low Hanging Fruit Immediately

It is always efficient to manage tasks that are simple and easily attainable. If executed properly, this will give confidence to continue and to achieve strategic goals as challenges become more and more difficult.

8.4 Step 3: Assess Existing Technology

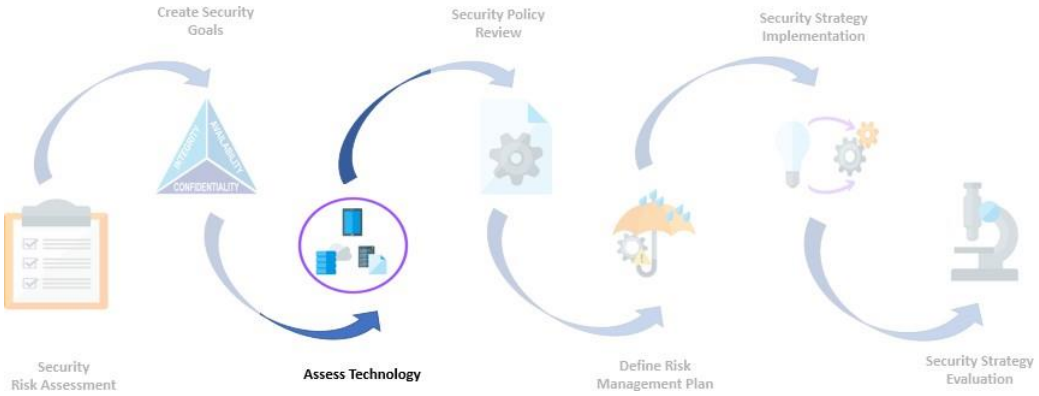

Figure 8.6: Step 3 – Assess Existing Technology

Understanding what technology to use and where is another important consideration while implementing a cyber-security program. Once assets are identified and prioritized, the next step is to determine if these systems are equipped in terms security requirements, understand if they function as per security best practices. Below points will help in this step:

Current technology landscape: Current state of the asset Operating Systems need to be identified and risks understood. There may be End-of-Life technology, in which case patches, bug fixes and security upgrades will automatically stop resulting in security risk.

Resource availability to manage the systems/platforms: As discussed in detail in Step 2 of the plan it is crucial to have the expertise to support technical platforms. Trained resources will be needed not only to patch these systems, but also to mitigate the threat in the event of a zero-day attack as well as recover from an incident.

Assess for Technology Bloats: Technical bloats like poorly written code, unapproved installation will create risks and need to be assessed and managed.

Data flow diagrams: It is essential to have detailed documentation on how data flows in and out of the system using a particular technology to identifying security weaknesses. Security should be engaged during the complete lifecycle of application development.

8.5 Step 4: Security Policy Review

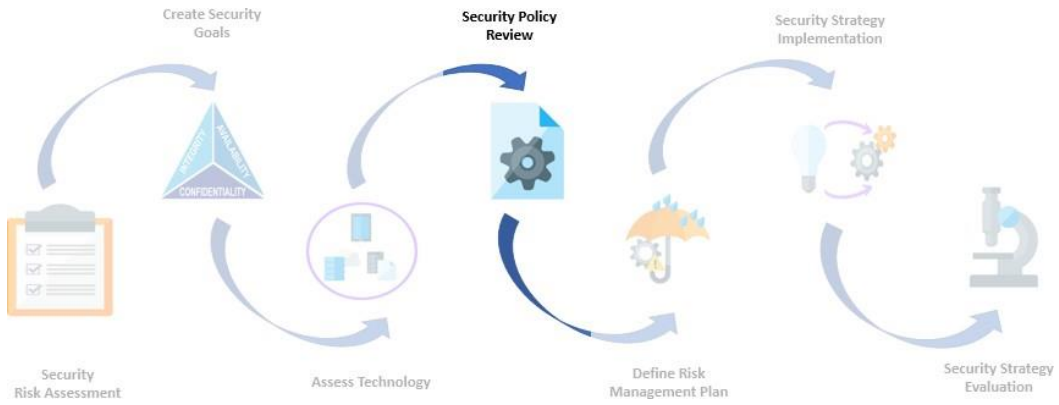

Figure 8.7: Step 4 - Security Policy Review

The objective of a security policy is to address and mitigate security threats and implement clear cyber-security strategies and procedures. It is necessary to keep security policies up to date so that they are equipped to address emerging threats. Policies should be reviewed regularly by experts to keep it effective. Steps below will help in the review process:

Current policy review: Current policies should be regularly reviewed to ensure they align with the overall business model.

Effectiveness of Policies Enforcement: The policies should be written such that they are enforceable. Every person in the organization should be trained and made aware of the security

policies and accountable for how he/she adheres to the security policies. The policies should be mapped to security controls so that effective monitoring, logging is possible.

8.6 Step 6: Define a Risk Management Plan

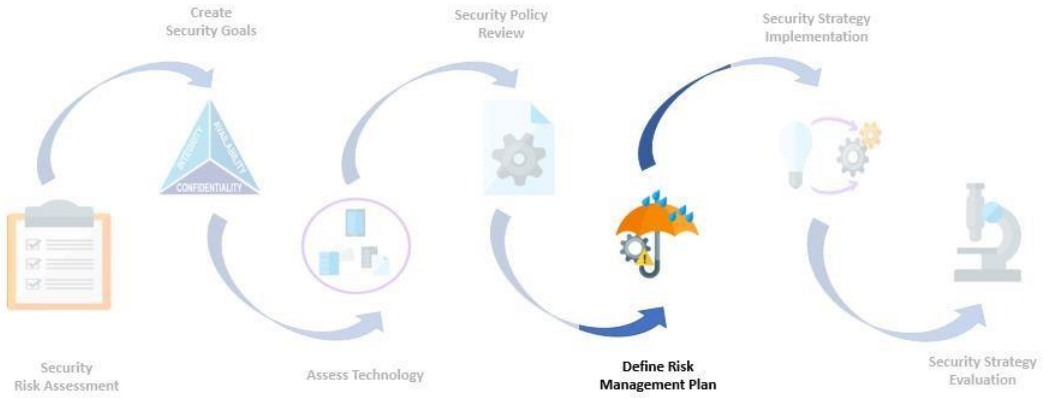

Figure 8.8: Step 5 - Define a Risk Management Plan

This next step in implementing cyber-security strategy is to create or define a good risk management plan that provides an effective analysis of all potential risks to the institute. Some of the best practice policies that can be incorporated into the risk management plan is listed below:

- **Data Privacy Policy** to provide governance on handling of institute's data and how it can be secured properly.
- **Retention Policy** that describes storage strategy for various types of data.
- **Data Protection Policy** that describes how personal data of its employees, students, vendors, and other third parties should be handled.
- **Incident Response Plan** to detail the procedures that must be followed so that in the event of security incident, a quick, effective and orderly response is ensured.

8.7 Step 6: Security Strategy Implementation

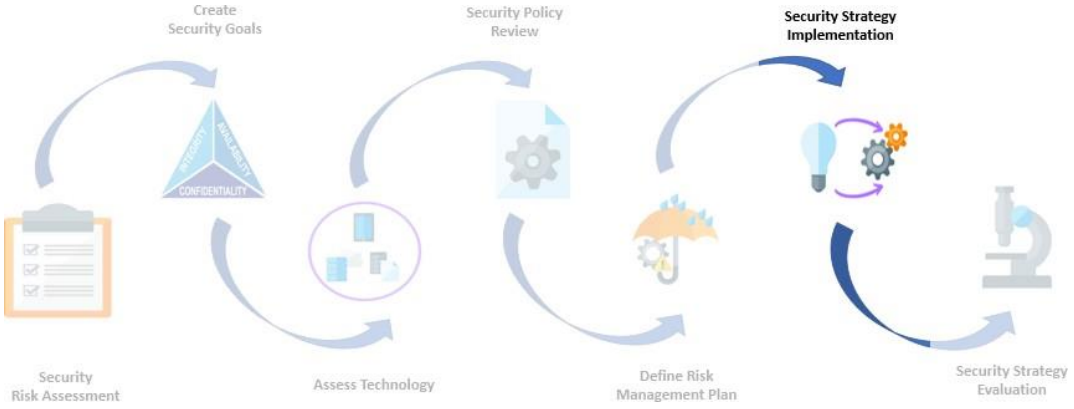

Figure 8.9: Step 6 - Security Strategy Implementation

This is the stage at which assessments are almost complete along with policy plans. Prioritization of remediation efforts is the next step along with assigning tasks to proper teams.

Assign remediation items by priority to internal teams along with providing leadership through Project Management office if available and plan the efforts.

Set realistic remediation goals and deadlines: It is better to set a reasonable time frame and exceed expectations than having too aggressive and unrealistic deadlines.

8.8 Step 7: Security Strategy Evaluation

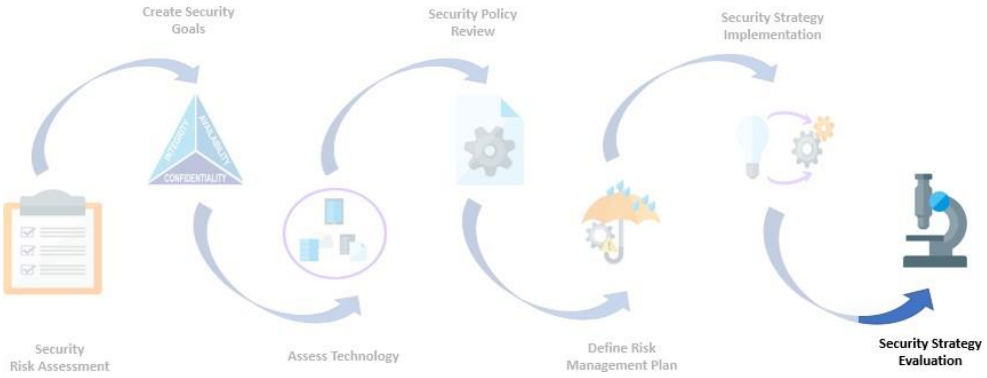

Figure 8.10: Step 7 - Security Strategy Evaluation

No strategy works efficiently without continuous monitoring and enhancements. It is important to have an ongoing support plan that will regularly monitor and test the security strategy to

ensure goals align with the threat landscape. Some key points to consider while maintaining a continuous and comprehensive oversight are:

Project Sponsor should be identified that guarantees resources availability and support for the project and is accountable for its success.

Conduct Annual Risk Assessment to ensure the security goals closely align with the organization's overall goals. Because the threat landscape keeps changing, the strategy must be revisited and revised, so that any gaps are addressed on a timely basis.

Obtain Feedback from Internal and External Stakeholder so that it will help justify security budgets, processes, and overall organization strategies. When stakeholders are aware of the security strategy and related processes and tasks, they will accept and appreciate the actions taken and even support them.

CHAPTER IX

SUMMARY, IMPLICATIONS, AND RECOMMENDATIONS

9.1 Summary

It is astonishing to see that though educational institutions are increasingly becoming victims of cyber-attacks, they are not showing enough attention in resolving the ground-level cybersecurity issues. The study showed that the educational institutes lack the resources needed to establish and maintain a strong cybersecurity program; they are lost in finding the right framework suited for their operational needs; existing frameworks are costly and complex to implement; other organizational priorities take precedence over cybersecurity, and institutes require the simple roadmap to assist them in achieving their security goals.

9.2 Research Implications

To start with it may be preferable to at least have a minimum of cybersecurity measures recommended in this study instead of not having any cybersecurity controls. This will at the very least ensure protection of the institute’s primary data and continuing to improve their cybersecurity maturity. Top management’s consideration on overall organization interests should be one of the key inputs while developing and implementing cybersecurity measures. All the available cybersecurity standards or frameworks generally have a comprehensive landscape of controls. These controls meet the standard's or framework's desired expectations. The new framework recommended as the solution, is a paradigm shift in the institute’s cybersecurity journey as it provides a sector specific security posture.

Most cybersecurity standards and frameworks are generic in nature and include a large set of measures that needs to be adopted by an organization, irrespective of its domain, size, staff strength. Most of the times only a few controls may be sufficient for institutes with a such specialized business domain. Too many controls and measures may prevent them from

implementing any of the existing standards or frameworks. Too many institutes have not even taken the first step toward implementing cybersecurity, thus making them vulnerable to growing cyber-attacks. There are a number of institutes that are even unaware of actually undergone an attack. The institutes need good motivation and encouragement to accept cybersecurity and implement it to an acceptable level. It is important that the management sees the link between good cybersecurity investment and optimal data and information protection for their organizational goals while mitigating cyber risks.

9.3 Recommendations

The research revealed that the security posture in the educational institutions is inadequate and needs to step up to manage the current risks. The EduSec cybersecurity framework, which was created for the benefit of the education sector with simplified controls and implementation steps is recommended for educational institutes to improve their cybersecurity posture.

This framework emphasizes on usage of technology and tools that can be leveraged fully to identify and mitigate the cyber-attacks automatically based on the IOA and IOC by continuously monitoring the activities in the network. The integration of all security tools, seamless collaboration and automation with continuous monitoring for unusual activities is the main focus of this framework.

Automated intelligent execution model with appropriate tools recommended to identify and mitigate the vulnerabilities and attack proactively by checking every step involving the execution and operation of activities in the network.

9.4 Future Work

The study has so far mostly concentrated on higher educational institutes. Further work encompassing other educational institutes like schools and private training and coaching

institutes can help modify this framework to suit these types of institutes. There is also a need to include artificial intelligence mechanisms that can analyse risk through behavioural data, accelerate alert investigations and save valuable time in detecting and remediating issues. This will be considered for future work.

9.5 Conclusion

Education sector has changed the way they conduct day to day business with the increase in demand for E-leaning. They have become more and more pro-active in building or finding new services that can enable students to study in a virtual environment. The Higher Education IT departments are constantly challenged with the increase in demand for e-learning flexibility, mobility, and empowerment. It is increasingly harder for them to maintain control over how data is stored, used, and shared inside and outside the virtual class. There is a requirement to build secure, standardised, highly available e-learning environments, as well as centralised application management so that users' needs are met with new and advanced services.

There is truly a need for at least minimum and stepwise cybersecurity implementation recommendations for educational institutions to overcome the risk of getting hacked. There are few schools of practical thought to overcome existing problems faced by educational institutions with ease of solution. Instead of "no" or "random" cybersecurity controls implemented, educational institutions can prioritize the implementation of controls based on perceived threat. Further, along with the minimum cybersecurity controls to provide Defence in Depth (DiD) for the educational institution, mapping the CIA prioritization with the cybersecurity controls can help educational institutions to get a good cybersecurity posture for safeguarding their organization.

APPENDIX A

Survey Cover Letter

Below is the questionnaire that was used to collect information from educational institutions regarding their current state of cyber security. The main focus of the questionnaire was to understand the current security controls in place and the problems or challenges that are being faced by the institutes in implementing cyber security.

Questionnaire

Sl.no	Questions
1	How old is the Institute?
2	Has institute adopted any standards or frameworks?
3	Does institute use any security controls?
4	What are the Physical security controls used in the institute?
5	What Technical Security controls are implemented in the institute?
6	Does the institute have any Administrative controls implemented?
7	What is the frequency of Security awareness trainings for the staff?
8	Is there any appropriate mechanisms for staff to be able to report suspicious emails quickly and effectively?
9	Does the staff and students understand the risks of using public WiFi?
10	Does organisation have manpower with Cybersecurity knowledge to identify the risks and threats?
11	What is the schedule to take backup of data?
12	Is backup data encrypted?
13	Is data classified by sensitivity and risk?
14	Did institute come under any cyber-attack?
15	Is network traffic monitoring done on daily basis through NOC/SOC for any malicious traffic?
16	What is the biggest challenge faced by the institute while deciding and/or implementing Cybersecurity Controls?
17	Is there any security roadmap, and regular review in overall IT roadmap strategy?
18	Is IT security operations outsourced ?
19	Is there any provision to handle Data privacy and Protection?
20	What are objectives that the institute wants to achieve by implementing security standards or framework?

APPENDIX B

Background Information about Survey Participants

Institute Code	Category	Segment	Age
IN001	Engineering/Technical college	Government	0-5 years
IN002	Multi-disciplinary University	Aided	5-10 years
IN003	Multi-disciplinary College	Private	10-20 years
IN004	Management Institute	Government	above 20 years
IN005	Medical College	Private	0-5 years
IN006	Engineering/Technical college	Private	0-5 years
IN007	Multi-disciplinary College	Government	5-10 years
IN008	Multi-disciplinary College	Government	5-10 years
IN009	Multi-disciplinary College	Government	10-20 years
IN010	Engineering/Technical college	Government	10-20 years
IN011	Engineering/Technical college	Private	above 20 years
IN012	Engineering/Technical college	Private	above 20 years
IN013	Engineering/Technical college	Private	5-10 years
IN014	Engineering/Technical college	Private	5-10 years
IN015	Medical College	Private	5-10 years
IN016	Multi-disciplinary University	Private	5-10 years
IN017	Multi-disciplinary University	Private	5-10 years
IN018	Multi-disciplinary University	Private	10-20 years
IN019	Multi-disciplinary University	Government	10-20 years
IN020	Multi-disciplinary University	Private	10-20 years
IN021	Multi-disciplinary University	Private	0-5 years
IN022	Multi-disciplinary University	Private	0-5 years
IN023	Multi-disciplinary University	Government	above 20 years
IN024	Medical College	Government	above 20 years
IN025	Medical College	Government	above 20 years
IN026	Medical College	Private	above 20 years

IN027	Engineering/Technical college	Private	0-5 years
IN028	Management Institute	Private	0-5 years
IN029	Management Institute	Private	0-5 years
IN030	Management Institute	Private	0-5 years
IN031	Management Institute	Private	0-5 years
IN032	Management Institute	Private	5-10 years
IN033	Management Institute	Private	5-10 years
IN034	Management Institute	Private	5-10 years
IN035	Management Institute	Private	5-10 years
IN036	Engineering/Technical college	Private	5-10 years
IN037	Engineering/Technical college	Private	5-10 years
IN038	Engineering/Technical college	Private	5-10 years
IN039	Engineering/Technical college	Private	5-10 years
IN040	Engineering/Technical college	Aided	5-10 years
IN041	Medical College	Aided	10-20 years
IN042	Medical College	Aided	10-20 years
IN043	Medical College	Aided	0-5 years
IN044	Medical College	Aided	0-5 years
IN045	Medical College	Aided	5-10 years
IN046	Medical College	Aided	5-10 years
IN047	Medical College	Aided	5-10 years
IN048	Multi-disciplinary University	Aided	5-10 years
IN049	Multi-disciplinary University	Aided	5-10 years
IN050	Multi-disciplinary University	Aided	5-10 years
IN051	Multi-disciplinary University	Private	5-10 years
IN052	Multi-disciplinary University	Private	5-10 years
IN053	Engineering/Technical college	Government	5-10 years
IN054	Engineering/Technical college	Government	5-10 years
IN055	Engineering/Technical college	Private	10-20 years
IN056	Engineering/Technical college	Government	10-20 years
IN057	Engineering/Technical college	Government	10-20 years

IN058	Multi-disciplinary College	Private	10-20 years
IN059	Management Institute	Government	10-20 years
IN060	Management Institute	Government	10-20 years
IN061	Management Institute	Government	above 20 years
IN062	Management Institute	Aided	above 20 years
IN063	Management Institute	Aided	above 20 years
IN064	Management Institute	Aided	0-5 years
IN065	Multi-disciplinary College	Aided	0-5 years
IN066	Multi-disciplinary College	Aided	0-5 years
IN067	Multi-disciplinary College	Aided	10-20 years
IN068	Multi-disciplinary College	Aided	above 20 years
IN069	Multi-disciplinary College	Private	5-10 years
IN070	Multi-disciplinary University	Government	0-5 years
IN071	Multi-disciplinary University	Aided	5-10 years
IN072	Multi-disciplinary University	Aided	above 20 years
IN073	Multi-disciplinary University	Aided	10-20 years
IN074	Multi-disciplinary University	Aided	5-10 years
IN075	Multi-disciplinary University	Aided	0-5 years
IN076	Engineering/Technical college	Government	0-5 years
IN077	Multi-disciplinary University	Aided	5-10 years
IN078	Multi-disciplinary College	Private	10-20 years
IN079	Management Institute	Government	above 20 years
IN080	Medical College	Private	0-5 years
IN081	Engineering/Technical college	Private	0-5 years
IN082	Multi-disciplinary College	Government	5-10 years
IN083	Multi-disciplinary College	Government	5-10 years
IN084	Multi-disciplinary College	Government	10-20 years
IN085	Engineering/Technical college	Government	10-20 years
IN086	Engineering/Technical college	Private	above 20 years
IN087	Engineering/Technical college	Private	above 20 years
IN088	Engineering/Technical college	Private	5-10 years

IN089	Engineering/Technical college	Private	5-10 years
IN090	Medical College	Private	5-10 years
IN091	Multi-disciplinary University	Private	5-10 years
IN092	Multi-disciplinary University	Private	5-10 years
IN093	Multi-disciplinary University	Private	10-20 years
IN094	Multi-disciplinary University	Government	10-20 years
IN095	Multi-disciplinary University	Private	10-20 years
IN096	Multi-disciplinary University	Private	0-5 years
IN097	Multi-disciplinary University	Private	0-5 years
IN098	Multi-disciplinary University	Government	above 20 years
IN099	Medical College	Government	above 20 years
IN100	Medical College	Government	above 20 years
IN101	Medical College	Private	above 20 years
IN102	Engineering/Technical college	Private	0-5 years
IN103	Management Institute	Private	0-5 years
IN104	Management Institute	Private	0-5 years
IN105	Management Institute	Private	0-5 years
IN106	Management Institute	Private	0-5 years
IN107	Management Institute	Private	5-10 years
IN108	Management Institute	Private	5-10 years
IN109	Management Institute	Private	5-10 years
IN110	Management Institute	Private	5-10 years
IN111	Engineering/Technical college	Private	5-10 years
IN112	Engineering/Technical college	Private	5-10 years
IN113	Engineering/Technical college	Private	5-10 years
IN114	Engineering/Technical college	Private	5-10 years
IN115	Engineering/Technical college	Aided	5-10 years
IN116	Medical College	Aided	10-20 years
IN117	Medical College	Aided	10-20 years
IN118	Medical College	Aided	0-5 years
IN119	Medical College	Aided	0-5 years

IN120	Medical College	Aided	5-10 years
IN121	Medical College	Aided	5-10 years
IN122	Medical College	Aided	5-10 years
IN123	Multi-disciplinary University	Aided	5-10 years
IN124	Multi-disciplinary University	Aided	5-10 years
IN125	Multi-disciplinary University	Aided	5-10 years
IN126	Multi-disciplinary University	Private	5-10 years
IN127	Multi-disciplinary University	Private	5-10 years
IN128	Engineering/Technical college	Government	5-10 years
IN129	Engineering/Technical college	Government	5-10 years
IN130	Engineering/Technical college	Private	10-20 years
IN131	Engineering/Technical college	Government	10-20 years
IN132	Engineering/Technical college	Government	10-20 years
IN133	Multi-disciplinary College	Private	10-20 years
IN134	Management Institute	Government	10-20 years
IN135	Management Institute	Government	10-20 years
IN136	Management Institute	Government	above 20 years
IN137	Management Institute	Aided	above 20 years
IN138	Management Institute	Aided	above 20 years
IN139	Management Institute	Aided	0-5 years
IN140	Multi-disciplinary College	Aided	0-5 years
IN141	Multi-disciplinary College	Aided	0-5 years
IN142	Multi-disciplinary College	Aided	10-20 years
IN143	Multi-disciplinary College	Aided	above 20 years
IN144	Multi-disciplinary College	Private	5-10 years
IN145	Multi-disciplinary University	Government	0-5 years
IN146	Multi-disciplinary University	Aided	5-10 years
IN147	Multi-disciplinary University	Aided	above 20 years
IN148	Multi-disciplinary University	Aided	10-20 years
IN149	Multi-disciplinary University	Aided	5-10 years
IN150	Multi-disciplinary University	Aided	0-5 years

APPENDIX C

Information Gathered from the Interviews

The following are the high-level inputs (samples) received from top management, such as directors, IT heads, and Computer Centre heads of the Educational Institutes when asked about the problems faced while choosing and implementing cyber security controls. Their input was also sought regarding how they are currently handling data privacy and safety in their organization and their expectation from security standards or framework. In this qualitative analysis, institutes participating were from all over India, and mostly Private or Semi-private. 50 institutions participated in the interview process.

Summary of Interview data

Problems faced while choosing and implementing cyber security controls	
Huge cost involved in implementing standard Cybersecurity controls.	46
Difficult to decide the controls that suit the institute's requirements	33
Lack of skilled resources to implement and maintain	33
Other businesses take priority	31
No clear roadmap to invest in the cybersecurity program	31
Available cybersecurity standards or frameworks take very long to implement and realise gains	42

Is there any mechanism to handle DATA privacy and Protection?	
Backups and Encryption	24
Access control and Authentication	50
More sophisticated controls	8

What is the expectation from security standards or framework	
Simple to understand and implement	38
Less number of controls and hence less measures for audits	30
Should be within budget	46
Step-by-step implementation with Intermittent milestones so that stakeholders can visualize success at regular intervals	28
Less time for implementation	32

BIBLIOGRAPHY

1. Acanerler, A. (2021). What is External Attack Surface Management? [online] *SOCRadar® Cyber Intelligence Inc.* Available at: https://socradar.io/what-is-external-attack-surface-management/.
2. Ajijola, A., Zavarsky, P. and Ruhl, R. (2014) 'A review and comparative evaluation of forensics guidelines of NIST SP 800-101 rev.1:2014 and ISO/IEC 27037:2012', *World Congress on Internet Security (WorldCIS-2014)* [Preprint]. doi:10.1109/worldcis.2014.7028169.
3. Albrechtsen, E. (2007) 'A qualitative study of users' view on information security', *Computers & Security*, 26(4), pp. 276–289. doi:10.1016/j.cose.2006.11.004.
4. Aliyu, A. *et al.* (2020) 'A holistic cybersecurity maturity assessment framework for higher education institutions in the United Kingdom', *Applied Sciences*, 10(10), p. 3660. doi:10.3390/app10103660.
5. Aloul, F.A. (2012) 'The need for effective information security awareness', *Journal of Advances in Information Technology*, 3(3). doi:10.4304/jait.3.3.176-183.
6. Alshar'e, M. (2023) 'Cyber Security Framework Selection: COMPARISION of NIST and ISO27001', *Applied computing Journal*, pp. 245–255. doi:10.52098/acj.202364.
7. Amin, Z. (2017) 'A practical road map for assessing cyber risk', *Journal of Risk Research*, 22(1), pp. 32–43. doi:10.1080/13669877.2017.1351467. [CrossRef]
8. Anghel, M.; Racautanu, A. (2019). A note on different types of ransomware attacks. Cryptol. *Eprint Arch. 2019, 605.*
9. Backup and disaster recovery solutions (2023) *Sentry IT Solutions.* Available at: https://sentrytechsolutions.com/it-support/managed-security-services/endpoint-security/ (Accessed: 05 February 2024).

10. Arora, B. (2016). Exploring and analyzing Internet crimes and their behaviours. *Perspectives in Science*, [online] 8, pp.540–542. doi:https://doi.org/10.1016/j.pisc.2016.06.014.
11. Asaad, R. R., & Saeed, V. A. (2022). A Cyber Security Threats, Vulnerability, Challenges and Proposed Solution. *Applied computing Journal*, 227-244
12. Atoum, I., Otoom, A., & Ali, A. (2014). A holistic cyber security implementation framework. *Information Management & Computer Security*, 22. https://doi.org/10.1108/IMCS-02-2013-0014
13. Bay, M. (2016). WHAT IS CYBERSECURITY? In search of an encompassing definition for the post-Snowden era. *French Journal for Media Research*. 6/2016.
14. Beckers, K., Heisel, M., Solhaug, B., Stølen, K. (2014). ISMS-CORAS: A Structured Method for Establishing an ISO 27001 Compliant Information Security Management System. In: Heisel, M., Joosen, W., Lopez, J., Martinelli, F. (eds) Engineering Secure Future Internet Services and Systems. *Lecture Notes in Computer Science, vol 8431*. Springer, Cham. https://doi.org/10.1007/978-3-319-07452-8_13
15. Bian, L., Chen, J., Soni, M., Bhola, J., Kumar, H. and Jawarneh, M. (2022) Research on computer 3D image encryption processing based on the nonlinear algorithm. *Nonlinear Engineering, Vol. 11 (Issue 1)*, pp. 664-671. https://doi.org/10.1515/nleng-2022-0232
16. Boneh, D., & Shoup, V. (2020). toc.cryptobook.us. (n.d.). A Graduate Course in Applied Cryptography. [online] Available at: https://toc.cryptobook.us/.
17. Borgman, C. L. (2018). Open data, grey data, and stewardship: Universities at the privacy frontier. *Berkeley Technology Law Journal*, 33(2), 365-412.

18. Bykov, V. Yu., Burov, O. Yu., and Dementievska, N. P (2019). Cybersecurity in Digital Educational Environment. Information Technologies and Learning Tools, 70(2), 313-331
19. Carlton MP, Wyrick P, Frederique N, Lopez B (2017) States' roles in keeping schools safe: opportunities and challenges for state school safety centers and other actors. *National Institute of Justice Report.* National Institute of Justice
20. Carr, M., 2016. Public–private partnerships in national cyber-security strategies. *International Affairs*, 92(1), pp.43-62.
21. Chapman, J., 2019. How Safe is Your Data?: Cyber-security in Higher Education (Vol. 12, pp. 1-6). Oxford, UK: Higher Education Policy Institute.
22. Chawki, M. and Abdel Wahab, M.S. (2006). Identity theft in cyberspace: Issues and solutions. *Lex Electronica*, 11, p.1.
23. Check Point Software. (n.d.). What is Cloud Security? Understand The 6 Pillars. [online] Available at: https://www.checkpoint.com/cyber-hub/cloud-security/what-is-cloud-security/.
24. CIS. (2018). CIS ControlsTM. [online] Available at: https://www.cisecurity.org/controls/.
25. Convocar, J.M. (n.d.). How Fast Can a Full Suite of Cybersecurity be Implemented? [online] www.itsasap.com. Available at: https://www.itsasap.com/blog/implementing-cybersecurity-program [Accessed 24 Nov. 2023].
26. Dahlstrom, E. and Bichsel, J., 2014. ECAR Study of Undergraduate Students and Information Technology, 2014. Educause.

27. Daras, N.J., 2017. On the mathematical definition of cyberspace. In 4th International Conference on Operational Planning, Technological Innovations and Mathematical Applications (OPTIMA), Hellenic Army Academy, Vari Attikis, Greece.
28. Data Communication and Computer Network. (2022). Types of Cyber Attack. [online] Available at: https://dcandcn.blogspot.com/2020/04/types-of-cyber-attack.html [Accessed 13 Aug. 2023].
29. discover.strongdm.com. (n.d.). What is DevOps Security? Challenges and Best Practices | strongDM. [online] Available at: https://www.strongdm.com/blog/devops-security.
30. Disterer, G. (2013). ISO/IEC 27000, 27001 and 27002 for Information Security Management. *Journal of Information Security*, [online] 04(02), pp.92–100. doi:https://doi.org/10.4236/jis.2013.42011.
31. Donaldson, S.E., Siegel, S.G., Williams, C.K. and Aslam, A. (2015). Cybersecurity Frameworks. *Enterprise Cybersecurity*, pp.297–309. doi:https://doi.org/10.1007/978-1-4302-6083-7_17.
32. EDUCAUSE Review. (n.d.). Three Insights for Presidents and CIOs. [online] Available at: https://er.educause.edu/articles/2010/6/three-insights-for-presidents-and-cios [Accessed 24 Nov. 2023].
33. Eerikson, H., Keller, M., Orlandi, C., Pullonen, P., Puura, J. and Simkin, M. (n.d.). Use Your Brain! Arithmetic 3PC for Any Modulus with Active Security Work done while at Cybernetica AS. [online] doi:https://doi.org/10.4230/LIPIcs.ITC.2020.5.
34. Elham Rajabian Noghondar, Konrad Marfurt and Bernhard, H. (2012). The Human Aspect in Data Leakage Prevention in Academia. *Springer eBooks*, pp.137–146. doi:https://doi.org/10.1007/978-3-658-00333-3_14.

35. Eloff, J.H.P. and Eloff, M.M. (2005). Information security architecture. *Computer Fraud & Security*, 2005(11), pp.10–16. doi:https://doi.org/10.1016/s1361-3723(05)70275-x.

36. Etal (2022*). Check Point Research: Education sector experiencing more than double monthly attacks, compared to other industries. [online] Check Point Software*. Available at: https://blog.checkpoint.com/2022/08/09/check-point-research-education-sector-experiencing-more-than-double-monthly-attacks-compared-to-other-industries/.

37. Evans, M., He, Y., Maglaras, L. and Janicke, H. (2019). HEART-IS: A novel technique for evaluating human error-related information security incidents. *Computers & Security*, 80, pp.74–89. doi:https://doi.org/10.1016/j.cose.2018.09.002.

38. Exabeam (2023). *The 12 Elements of an Information Security Policy - Exabeam. Exabeam.* [online] Available at: https://www.exabeam.com/explainers/information-security/the-12-elements-of-an-information-security-policy/.

39. Fiedelholtz, G. (2021). The Cyber Network Guide: Studies in Systems, Decision and Control Pre-incident Planning and Analysis; alternate title: The Cyber Network Guide: Studies in Systems, Decision and Control Incident Detection and Characterization. *mdsoar.org*. [online] doi:https://doi.org/10.13016/m2i0nc-5fev.

40. Fisch, E.A. and White, G.B. (2000) *Secure Computers and networks: Analysis, design, and implementation*. Boca Raton, FL: CRC Press.

41. Foster, A.L. (2004). *Insecure and Unaware An analysis of campus networks reveals gaps in security*. [online] https://www.chronicle.com/. Available at: https://www.chronicle.com/article/insecure-and-unaware/.

42. González-Martínez, J.A., Bote-Lorenzo, M.L., Gómez-Sánchez, E. and Cano-Parra, R. (2015). Cloud computing and education: A state-of-the-art survey. *Computers & Education*, 80, pp.132–151. doi:https://doi.org/10.1016/j.compedu.2014.08.017.
43. Groš, S. (2021). *A Critical View on CIS Controls.* [online] IEEE Xplore. doi:https://doi.org/10.23919/Con%E2%84%A152528.2021.9495982.
44. Harpreet, S. D. (2013). Cybercrime—a threat to persons, property, government and societies. *Int. J. Adv. Res. Comput. Sci. Softw. Eng. Res.*, 3(5 (May)).
45. Hina, S., & Dominic, P. D. D. (2018). Information security policies' compliance: a perspective for higher education institutions. *Journal of Computer Information Systems*.
46. ieeexplore.ieee.org. (n.d.). *Leverage intrusion detection system framework for cyber situational awareness system* | IEEE Conference Publication | IEEE Xplore. [online] Available at: https://ieeexplore.ieee.org/document/8267823 [Accessed 24 Nov. 2023].
47. Imperva (2021). *What is data classification?* | *best practices & data types* | imperva. [online] Learning Center. Available at: https://www.imperva.com/learn/data-security/data-classification/.
48. Jasper, S.E. (2016). U.S. Cyber Threat Intelligence Sharing Frameworks. *International Journal of Intelligence and Counter Intelligence*, 30(1), pp.53–65. doi:https://doi.org/10.1080/08850607.2016.1230701.
49. Jawarneh, M., Virmani, D., Kaliyaperumal, K., Phasinam, K., & Santosh, T. (2021). Towards Investigation of Various Security And Privacy Issues In Internet Of Things. *Design Engineering*, 1747–1758.
50. Johnson, H. (2007). Dialogue and the Construction of Knowledge in E-Learning: Exploring Students' Perceptions of Their Learning While Using Blackboard's Asynchronous Discussion Board. European *Journal of Open, Distance and E-learning*,

[online] 10(1). Available at: https://old.eurodl.org/?p=archives&year=2007&halfyear=1&article=251.

51. kahoward (2021). *Technical Communication & Cybersecurity. [online] Intercom*. Available at: https://www.stc.org/intercom/2021/07/technical-communication-cybersecurity/.
52. Kim, K., Alfouzan, F.A. and Kim, H. (2021). Cyber-Attack Scoring Model Based on the Offensive Cybersecurity Framework. *Applied Sciences*, 11(16), p.7738. doi:https://doi.org/10.3390/app11167738.
53. Khther, R.A. and Othman, M. (2013). Cobit Framework as a Guideline of Effective it Governance in Higher Education: A Review. *International Journal of Information Technology Convergence and Services*, [online] 3(1), pp.21–29. doi:https://doi.org/10.5121/ijitcs.2013.3102.
54. Krumay, B., Bernroider, E.W.N. and Walser, R. (2018). Evaluation of Cybersecurity Management Controls and Metrics of Critical Infrastructures: A Literature Review Considering the NIST Cybersecurity Framework. *Secure IT Systems*, 11252, pp.369–384. doi:https://doi.org/10.1007/978-3-030-03638-6_23.
55. Kwon, K.H. and Shakarian, J. (2018). Chapter 7 Black-Hat Hackers' Crisis Information Processing in the Darknet: A Case Study of Cyber Underground Market Shutdowns. *Studies in Media and Communications*, pp.113–135. doi:https://doi.org/10.1108/s2050-206020180000017007.
56. Lane, T. (2007). *Information security management in Australian universities : an exploratory analysis*. [online] eprints.qut.edu.au. Available at: https://eprints.qut.edu.au/16486/ [Accessed 24 Nov. 2023].
57. Lavrov, E., Tolbatov, A., Pasko, N. and Tolbatov, V. (2017). Cybersecurity of distributed information systems, the minimization of damage caused by errors of

operators during group activity. *2017 2nd International Conference on Advanced Information and Communication Technologies (AICT).* doi:https://doi.org/10.1109/aiact.2017.8020071.

58. Liu, C.-W., Huang, P. and Lucas, H. (2017). *IT Centralization, Security Outsourcing, and Cybersecurity Breaches: Evidence from the U.S. Higher Education. ICIS 2017 Proceedings*. [online] Available at: https://aisel.aisnet.org/icis2017/Security/Presentations/1/ [Accessed 10 Apr. 2022].
59. Lukehart, M. (2022). *2022 Cyber Attack Statistics, Data, and Trends | Parachute*. [online] Parachute. Available at: https://parachute.cloud/cyber-attack-statistics-data-and-trends/.
60. Mailloux, L.O., McEvilley, M.A., Khou, S. and Pecarina, J.M. (2016). Putting the 'Systems' in Security Engineering: *An Examination of NIST Special Publication* 800-160. IEEE Security & Privacy, 14(4), pp.76–80. doi:https://doi.org/10.1109/msp.2016.77.
61. Malatji, M., Von Solms, S. and Marnewick, A. (2019). Socio-technical systems cybersecurity framework. *Information and Computer Security*, 27(2), pp.233–272. doi:https://doi.org/10.1108/ics-03-2018-0031.
62. Mantha, B.R.K. and de Soto, B.G. (2019). Cyber security challenges and vulnerability assessment in the construction industry. *Proceedings of the Creative Construction Conference 2019.* [online] doi:https://doi.org/10.3311/ccc2019-005.
63. Merchan-Lima, J., Astudillo-Salinas, F., Tello-Oquendo, L., Sanchez, F., Lopez-Fonseca, G. and Quiroz, D. (2020). Information security management frameworks and strategies in higher education institutions: a systematic review. *Annals of Telecommunications*. doi:https://doi.org/10.1007/s12243-020-00783-2.

64. Mukhopadhyay, D. (n.d.*). Cryptography and Network Security*. [online] Available at: http://acl.digimat.in/nptel/courses/video/106105031/lec13.pdf [Accessed 13 Aug. 2023].

65. Mustafa, M., Alzubi, S. and Alshare, M. (2020). The Moderating Effect of Demographic Factors Acceptance Virtual Reality Learning in Developing Countries in the Middle East. *Communications in Computer and Information Science*, pp.12–23. doi:https://doi.org/10.1007/978-981-15-6634-9_2.

66. National Institute of Standards and Technology (2018). Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1. *Framework for Improving Critical Infrastructure Cybersecurity*, [online] 1.1(1.1). doi:https://doi.org/10.6028/nist.cswp.04162018.

67. Naumov, S. and Kabanov, I. (2016). Dynamic framework for assessing cyber security risks in a changing environment. *2016 International Conference on Information Science and Communications Technologies (ICISCT*). doi:https://doi.org/10.1109/icisct.2016.7777406.

68. Noble, H. and Heale, R. (2019). *Triangulation in Research. Evidence Based Nursing*, [online] 22(3), pp.67–68. doi:https://doi.org/10.1136/ebnurs-2019-103145.

69. Office, C. (2016*). National Cyber Security Strategy 2016 to 2021*. [online] GOV.UK. Available at: https://www.gov.uk/government/publications/national-cyber-security-strategy-2016-to-2021.

70. Ozier, W. (2010). Risk Analysis and Assessment: Risk Assessment Tasks. CRC Press eBooks, pp.2499–2506. doi:https://doi.org/10.1081/e-eia-120046889.

71. pages.checkpoint.com. (n.d.). Cyber-Attacks Trends: 2022 Mid-Year | Check Point Software. [online] Available at: https://pages.checkpoint.com/cyber-attack-2022-trends.html.

72. Petersen, R., Santos, D., Smith, M.C., Wetzel, K.A. and Witte, G. (2020). Workforce Framework for Cybersecurity (NICE Framework). [online] doi:https://doi.org/10.6028/nist.sp.800-181r1.

73. Pienta, D.A., Thatcher, J. and Johnston, A.C. (2018). A Taxonomy of Phishing: Attack Types Spanning Economic, Temporal, Breadth, and Target Boundaries. [online] *Semantic Scholar*. Available at: https://www.semanticscholar.org/paper/A-Taxonomy-of-Phishing%3A-Attack-Types-Spanning-and-Pienta-Thatcher/b6928c7c1ccf7d56c07138db1c0b3e0074c886e0 [Accessed 24 Nov. 2023].

74. Pipyros, K., Thraskias, C., Mitrou, L., Gritzalis, D. and Apostolopoulos, T. (2018). A new strategy for improving cyber-attacks evaluation in the context of Tallinn Manual. *Computers & Security*, 74, pp.371–383. doi:https://doi.org/10.1016/j.cose.2017.04.007.

75. potenzaglobalsolutions.com (2023). Cyber Threat Intelligence: Benefits and LifeCycle. [online*] Cymune*. Available at: https://www.cymune.com/cyber-threat [Accessed 13 Nov. 2023].

76. PurpleSec. (n.d.*). How To Plan & Develop An Effective Cyber Security Strategy*. [online] Available at: https://purplesec.us/learn/cyber-security-strategy.

77. P. Riquelme, I. and Román, S. (2014). Is the influence of privacy and security on online trust the same for all type of consumers? *Electronic Markets*, 24(2), pp.135–149. doi:https://doi.org/10.1007/s12525-013-0145-3.

78. Radanliev, P., de Roure, D., Nurse, J., Nicolescu, R., Huth, M., Cannady, S. and Montalvo, R. (2018). Integration of Cyber Security Frameworks, Models and Approaches for Building Design Principles for the Internet-of-Things in Industry 4.0. [online*] Social Science Research Network.* Available at:

https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3286131 [Accessed 24 Nov. 2023].

79. Ruck, D. (2021). Continuous Monitoring: What Is It and How Is it Impacting DevOps Today? [online] *Lightrun.* Available at: https://lightrun.com/continuous-monitoring-what-is-it-and-how-is-it-impacting-devops-today/.
80. Satori. (n.d.). Cybersecurity Frameworks. [online] Available at: https://satoricyber.com/data-protect-guide/cybersecurity-frameworks/.
81. Schneier, B. (1994). Description of a new variable-length key, 64-bit block cipher (Blowfish). *Fast Software Encryption*, pp.191–204. doi:https://doi.org/10.1007/3-540-58108-1_24.
82. Shackelford, S., Proia, A.A., Martell, B. and Craig, A. (2014). Toward a Global Cybersecurity Standard of Care? Exploring the Implications of the 2014 NIST Cybersecurity Framework on Shaping Reasonable National and International Cybersecurity Practices. [online] papers.ssrn.com. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2446631.
83. Shackelford, S., Russell, S. and Haut, J. (2015). Bottoms Up: A Comparison of Voluntary Cybersecurity Frameworks. [online] papers.ssrn.com. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2702039.
84. Shamma, B. (2018). Implementing CIS Critical Security Controls for Organizations on a Low-Budget. uh-ir.tdl.org. [online] Available at: https://uh-ir.tdl.org/items/e71dc058-dcee-4e56-ba03-37df3f31e7f3 [Accessed 25 Nov. 2023].
85. Sharma, S. (2022). Education sector hounded by cyberattacks in 2021. [online] CSO Online. Available at: https://www.csoonline.com/article/3647760/education-sector-hounded-by-cyberattacks-in-2021.html.

86. Shetty, S., McShane, M.K., Zhang, L., Kesan, J.P., Kamhoua, C., Kwiat, K. and Njilla, L. (2018). Reducing Informational Disadvantages to Improve Cyber Risk Management. [online] Social Science Research Network. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3121389 [Accessed 25 Nov. 2023].

87. Smail, B., Sanchez, Dr.D.T., Peconcillo Jr., Dr.L.B., De Vera, Dr.J.V., Horteza, Dr.A.D., Jawarneh, M. and Dr.Meenakshi (2022). Investigating different applications of Internet of Things towards identification of vulnerabilities, attacks and threats. International Journal of Next-Generation Computing. doi:https://doi.org/10.47164/ijngc.v13i3.841.

88. Smyth, G., 2017. Using data virtualisation to detect an insider breach. Computer Fraud & Security, 2017(8), pp.5-7.

89. Sree, C. (2022). *Vulnerability Management Process: It's More Than Just Detecting Vulnerabilities!* [online] SecPod Blog. Available at: https://www.secpod.com/blog/vulnerability-scanning-process-its-more-than-just-detecting-vulnerabilities/.

90. Stallings, W. and Hall, P. (2005). *Cryptography and Network Security Principles and Practices, Fourth Edition.* [online] Available at: http://www.inf.ufsc.br/~bosco/ensino/ine5680/material-cripto-seg/2014-1/Stallings/Stallings_Cryptography_and_Network_Security.pdf [Accessed 25 Nov. 2023].

91. Stealthlabs. (2021). *Cybersecurity in Education: 10 Important Facts and Statistics*. [online] Available at: https://www.stealthlabs.com/blog/cybersecurity-in-education-10-important-facts-and-statistics/.

92. Swanagan, M. (2020). *The 3 Types Of Security Controls (Expert Explains).* [online] PurpleSec. Available at: https://purplesec.us/security-controls/.

93. Thakur, K., Qiu, M., Gai, K. and Ali, M.L. (2015). *An Investigation on Cyber Security Threats and Security Models*. [online] IEEE Xplore. doi:https://doi.org/10.1109/CSCloud.2015.71.

94. Tso, L. (n.d.). *The Official Introduction to the ITIL Service Lifecycle*. [online] Available at: https://www.kornev-online.net/ITIL/The%20Official%20Introduction%20to%20the%20ITIL%20Service%20Lifecycle.pdf [Accessed 24 Nov. 2023].

95. Thomas, T., P Vijayaraghavan, A., & Emmanuel, S. (2020). Machine learning and cybersecurity. *In Machine Learning Approaches in Cyber Security Analytics (pp. 37-47). Springer, Singapore*.

96. von Solms, R. and van Niekerk, J. (2013). From information security to cyber security. *Computers & Security*, [online] 38, pp.97–102. doi:https://doi.org/10.1016/j.cose.2013.04.004.

97. Wirth, A. (2017). The Economics of Cybersecurity. *Biomedical Instrumentation & Technology*, 51(s6), pp.52–59. doi:https://doi.org/10.2345/0899-8205-51.s6.52.

98. www.6clicks.com. (n.d.). *Cyber Security Framework Comparisons*. [online] Available at: https://www.6clicks.com/resources/comparisons.

99. www.egnyte.com. (n.d.). *Cybersecurity Maturity Model Certification Framework*. [online] Available at: https://egnyte.com/guides/cmmc/cmmc-framework [Accessed 13 Nov. 2023].

100. www.ekransystem.com. (2020). *4 Steps to Ensuring Efficient Cybersecurity Monitoring in US Educational Institutions*. [online] Available at:

https://www.ekransystem.com/en/blog/security-monitoring-educational-organizations.

101. www.interfacett.com. (n.d.). *Access Management Control in IT is not just about the tools*! | Interface Technical Training. [online] Available at: https://www.interfacett.com/blogs/access-management-control-it-just-tools/ [Accessed 25 Nov. 2023].
102. www.iso27001security.com. (n.d.). ISO/IEC 27032 cybersecurity guideline. [online] Available at: http://www.iso27001security.com/html/27032.html.
103. www.jit.io. (n.d.). Read Jit Blog Post: Top 10 Continuous Security Monitoring (CSM) Tools for 2023 | Jit.io. [online] Available at: https://www.jit.io/blog/continuous-security-monitoring-csm-tools.
104. www.kaspersky.com. (2023). *Black hat, White hat, and Gray hat hackers – Definition and Explanation.* [online] Available at: https://www.kaspersky.com/resource-center/definitions/hacker-hat-types#:~:text=When%20a%20white%20hat%20hacker.
105. www.linkedin.com. (n.d.). *A Layered Approach to Cybersecurity: People, Processes, and Technology- Explored & Explained*. [online] Available at: https://www.linkedin.com/pulse/layered-approach-cybersecurity-people-processes-singh-casp-cisc-ces/.
106. www.linkedin.com. (n.d.). People, Process, Technology: The Framework for Workforce Management. [online] Available at: https://www.linkedin.com/pulse/people-process-technology-framework-workforce-jordi-vilanova/ [Accessed 25 Nov. 2023].
107. www.sans.org. (n.d.). *SANS Institute - CIS Critical Security Controls.* [online] Available at: https://www.sans.org/critical-security-controls.

108. www.securitymagazine.com. (n.d.). 92% of data breaches in Q1 2022 due to cyberattacks. [online] Available at: https://www.securitymagazine.com/articles/97431-92-of-data-breaches-in-q1-2022-due-to-cyberattacks.

109. www.stickmancyber.com. (n.d.). How to Get the Most from Your Cybersecurity Budget | *StickmanCyber*. [online] Available at: https://www.stickmancyber.com/cybersecurity-blog/how-to-get-the-absolute-most-from-your-cybersecurity-budget [Accessed 25 Nov. 2023].

110. www.theamegroup.com. (n.d.). Business Security Vulnerability Assessment | The AME Group. [online] Available at: https://www.theamegroup.com/business-security-vulnerability-assessment/ [Accessed 25 Nov. 2023].

111. www.verizon.com. (2020). Money makes the cyber-crime world go round - *Verizon Business 2020 Data Breach Investigations Report.* [online] Available at: https://www.verizon.com/about/news/verizon-2020-data-breach-investigations-report.

112. Yan, Z., Robertson, T., Yan, R., Park, S.Y., Bordoff, S., Chen, Q. and Sprissler, E. (2018). Finding the weakest links in the weakest link: How well do undergraduate students make cybersecurity judgment? *Computers in Human Behavior*, 84, pp.375–382. doi:https://doi.org/10.1016/j.chb.2018.02.019.