CYBER SECURITY CHALLENGES ON ACADEMIC INSTITUTIONS AND NEED FOR SECURITY FRAMEWORK TOWARDS INSTITUTIONAL SUSTAINABILITY GROWTH AND DEVELOPMENT

By

WALI MOHAMMAD DAR

Department of Computer Science, School of Technology, Islamic University of Science and Technology Awantipora (IUST), Pulwama, Jammu and Kashmir, India

ABSTRACT

The growing dependence on computer networks and internet based applications in all areas of human involvement (Health, Education, Transportation and energy) makes it a big challenge to treat Cyber security as a separate dimension. For the sustainable development and existence of Academic Institutions, a secure and comprehensive framework is the need of the hour to ensure the sustainability and existence in the digital world. Cyber security consists of 'cyber space' which is a collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment, organization and user's assets. Cyber security endeavors to ensure the attainment and maintenance of the security properties of the organization and user's assets. Therefore strong initiatives like implementation of security policies and strategic framework of procedures/plans to secure the future of Institutions are enforced. In the present era, digital information is at the core of almost all of a university activities and the safety and security of this information is vital for growth and development. This paper discusses the Security Framework as a means to protect information and technology resources, throughout the University.

Keywords: Comprehensive Framework, Digital Information, Computer Networks, Academic Institutions.

INTRODUCTION

Digital Technology has effected virtually every aspect of life today. Social interaction, health care, Economic decision making, political doctrine ,digital connectivity permeates it all, and the dependence on this connectivity is growing swiftly. Greater reliance on a networked resource naturally makes us more interdependent. As this new, shared digital space evolves, the immediate need is to develop a common set of activities in the form of Framework to address systemic risks, and to define not only the management strategies and responsibilities of all the participants in collaboration with local as well as national institutions, but like Universities [1] and highly developed academic leaders to address the problems and threats imposed by the sophistication and exponential growth of Internet today in the Cyber Ecosystem. The obligations will encompass several key issues in the Cyber Dimension from privacy norms to internal governance policy but the collective ability to manage cyber risks in this shared digital environment is fundamental, as it forms the crux of the Cyber security. Higher Educational Institutions get their required data for the purpose related to their concerned core area, like information about students, staff or Finances. This data might be considered very sensitive by the law and the providers of data or where it informs decision making, such as marketing and recruitment data or, potentially, analytics from virtual learning environments. As the importance of digital information has grown, so has the need to ensure that data is protected from potential corruption, destruction or theft. However, in the case of large, complex organizations like universities, different types of activity may involve different types of risks, management priorities, and associated security measures.

1. Challenges

Academic Institutions are facing various challenges and threats of complex and varied nature. These challenges impose threat to the very existence of these Institutions and its infrastructure, such as through distributed denial of service attacks that may directly or indirectly target an institution's network. It's important to note that there is no one-size-fits-all solution for cyber security, and the government cannot provide comprehensive, prescriptive guidelines for all entities across industries. So while the Framework offers worthwhile standards for improving cyber security, it does not fully address several critical areas.

1.1 Difficulty Identifying Motives

Distinguishing between different types of cyber-threats [9] is challenging because the motives and behavior of individuals in this realm is difficult to identify and monitor.

1.2 Lack of Central Authority

Since Cyber Space (Internet) is partially regulated, there is no central authority policing cyberspace. There is Exploitation of Vulnerabilities and Loopholes between Universities, and Lack of Collaborations among State and National Institutions. With the spread of networks of hijacked computers over different countries, criminals can launch cyber attacks using a decentralized model based on peer-to-peer arrangements. This makes it increasingly difficult for any single national or regional legal framework to deal adequately with the problem. Cyber criminals are shifting operations to countries where appropriate and enforceable laws are not yet in place. Also the framework policies are not implemented due to lack of infrastructure. This allows them to launch attacks on victims with almost complete impunity, even in those countries which do have effective policies in place [11].

1.3 Issues in Cyberspace:

While many countries have adopted or are working on legislation in order to combat cyber crime and other misuse of IT, these laws are drawn up to be enforceable in well-defined geographical boundaries which are either national or regional. Additionally, there is an absence of a common understanding on the applicable international rules for state behavior in this domain. Even if all countries introduced legislation, cyber criminals cannot be easily extradited between the country where the cybercrime was instigated and the country where it was committed, unless these legal frameworks are inter-operable. This is far from the situation today. On the contractual front, jurisdiction and formation of e-contracts are two key issues on which traditional legal principles have been largely applied by Courts worldwide. There is a now a general consensus that in the e-world, electronic signatures and electronic documents are equally legally valid as the hand-written signatures or hard copy paper documents.

1.4 Global Connectivity and Vulnerable technologies:

Many of the tools in cyberspace can be used for both legitimate and malicious purposes. States and non state actors are carrying out increasingly sophisticated exploitations of vulnerabilities in Information and Communication Technology. Lack of central authority and vulnerable Technologies coupled with Anonymity, freedom of expression, remote accessibility and characteristics of Cyber security [10] make it an optimal target for crime. Illegal activities and terrorism are some of the big challenges faced by almost all the institutions of the country.

2. Risk Management and the Cyber Security Framework

Organizations deploy technological means to protect their information and technology resources, but they also rely on their employees. Employees who use the information and technology resources of their organizations assume certain roles in and are responsible for safeguarding (protecting)those resources, so we are interested in what factors drive an employee to perform those roles and meet their responsibilities. We define information security policy as a statement of the roles and responsibilities of the employees to safeguard the information and technology resources of their organizations.

Over the years, there has been heightened concern and focus on the lack of effectiveness in the current approach to risk management due to critical threats brought on by the rapidly changing global fundamentals and the inability of the risk management programs to predict critical risks at all levels. It has become increasingly clear that a need exists for re-evaluation of the approach to risk management.

The Cyber-Security Risk Management framework has been marked by a series of high-profile Cyber-Security breaches and other global, national, local and industrial crises, scandals and failures where nations, its governments, investors, businesses, individuals and other stakeholders, individually and collectively suffered tremendous losses in many formats.

Cyber security is an international issue and it requires international cooperation to be effective. For instance, the cyber breach of Ebay has international legal ramifications and one cannot contend that the place of establishment alone would feel the consequences. However, there are some nations that are not in favour of international technology transfer in the field of cyber security.

2.1 Security Framework Activities

- Data protection
- IT Operations Security.
- Security Policy Architecture.
- Personal Security for information Systems.
- Security training and awareness.
- Information Security Management.
- Physical and Environment Security.
- Cryptographic Controls.
- Information system Authorization and account Management Risk Management.
- System Life Development Cycle Security.
- Data classification. Information System Auditing and Testing.
- Security Compliance Management.
- User identification and authorization.

This activity set of procedures (Framework) provide a means to the management of information security throughout the University. It applies to: All those with access to University information systems, including staff, students, visitors and contractors. Any systems attached to the University computer or telephone networks and any systems supplied by the University; All information (data) processed by the University pursuant to its operational activities, regardless of whether it is processed electronically or in paperwork (hard copy) form, any communications sent to or from the University and any University information (data) held on systems external to the University' network; All external parties that provide services to the University in respect of information processing facilities and business activities.

Principal information assets including the physical locations from which the University operates [2].

In order to achieve those above mentioned objectives following procedure has to be followed to achieve maximum safety.

- Password Management
- Network Access Control
- Network Connection Control

Direct public access must be restricted between external networks and any system component that stores restricted data. Internal network access must be restricted depending on the user and device credentials, with access granted based on user access permissions and the device's security profile.

2.1.1 Network Routing Control:

Inbound and outbound traffic must be restricted to that which is necessary for the restricted data environment only with all other inbound and outbound traffic not being allowed.

Operating System Access Control, Systems configuration and monitoring

2.1.2 Authentication Methods:

Academic Institutions implementing the above mentioned policies must monitor developments in authentication technologies to ensure that this standard and any associated procedures are kept up to date with current security good practice.

2.1.3 Device Configuration

Vendor-supplied default passwords must be changed prior to installing a system on the Institutions network. Where available, all system components must be configured to use centralized authentication systems.

2.2 Use of Personal Devices

Device maintenance and security for personal mobile computing and communication devices (including but not limited to laptops, tablets and mobile phones) remains the responsibility of the asset owner. The Information Security exports or technical staff must inform all users of personal devices of their security obligations concerning mobile computing devices. Personal devices must only connect to the networks designated for such usage. These include mobile device and guest networks only.

2.3 Use of University Devices

Personal firewalls and anti-virus must be installed on all of the university issued laptop computers and mobile computing devices. All of the university mobile computing devices must be registered as per the institution's mobile device Management policy. The user will be responsible for the secure storage and management of mobile computing device.

The university technical team must conduct an audit of all of the university provided mobile computing devices on an annual basis.

This audit must physically verify the device and its condition, identify any damage or modifications since issue. Verify device registration details and Verify the allocated user remains unchanged.

The concerned Institution issued mobile computing devices must be returned upon leaving the organization (including all issued peripherals and storage media).

2.4 Network Usage

When connecting with a mobile device on campus, staff and students must only connect to designated networks for mobile devices (including Wi-Fi and tethering).

The IT team must ensure that personal or unknown devices are prevented from connecting to the secure internal networks.

3. Remote Access Governance and Management Authorization

Remote access authorizations should be reviewed annually.

3.1 Logging and Monitoring

All remote access activity must be logged and monitored in line with the university Vulnerability Management standard.

3.2 Configuration and Operation

3.2.1 Authentication

Strong authentication must be used for remote access to the network by staff and authorized third parties. Where exceptions to this item are required (such as guest and mobile wireless networks), these networks must be segregated from core university data storage systems and networks. Remote access must not be permitted using system administration accounts, or accounts with system administration privileges. The university should strongly encourage that remote devices employ anti-virus and firewall software.

4. Development of Operational Standards

The university must develop daily operational security procedures that are consistent with the requirements of this Information Security standard. All information systems must be managed in accordance with industry best practice. Documented Standard Operating Procedures must be prepared for all those system activities associated with information processing and communication facilities. Therefore the following must be considered for the Operating procedures.

System start-up and close-down;

Backups;

Equipment maintenance;

Media handling;

System version;

Application versions;

Secure area working;

Health and safety.

4.1 Responsibility and Accountability

Departmental IT Managers are responsible for ensuring the development, maintenance, updating and implementation of any Standard Operating Procedures (SOP's).

4.2 Control and Definition of Process

It is the responsibility of the concerned institution to document the control procedures peer reviewed in order to protect the integrity, availability and confidentiality of the institutions information systems [8]. Formal management responsibilities and procedures must be in place to ensure satisfactory control of all changes to equipment, software or procedures. The Manager, IT Infrastructure must approve all changes that impact the security of the institution.

Conclusions and Suggestions

The digital domain has become more interweaved with our daily lives. Citizens, government bodies and businesses are using digital applications for online interactions and transactions for more efficient collaboration, communication and entertainment. This increasing digitization is not only for ease, efficiency and pleasure, but is also an important drive for innovation and economic growth. Moreover governments, military, corporations, financial institutions, hospitals and other businesses collect, process and store a great deal of confidential information on computers and transmit that data across networks to other computers. With this growing volume and sophistication of cyber-attacks, ongoing attention is required to protect sensitive business and personal information, as well as safeguard national security. Hence we need firm strategies for cyber security as well as growing awareness. It must be remembered that the existing strategies are not immutable; actions will evolve as technologies advance, as threats and vulnerabilities change, and our understanding of cyber security issues will improve. Going ahead we need to continue national dialogue on cyber security, calling for voluntary partnerships among government, industry, academia and non-governmental groups to secure and defend our cyberspace. This paper will help researchers to design and develop the effective policies and strategies in this dynamic field of Cyberspace with techniques and advancements inline with the sophistication of attacks and threats posed by the arena.

References

[1]. Dar W.M (2015), "*Advances in Computational Research"* , Vol. 7, No. 1, pp. 159-163.

[2]. Dar W.M. (2014). *International Journal of Advanced Research in Computer Science and Software Engineering*, Vol. 4, No. 7, pp. 756-763.

[3]. Innovation and Skills (2013). "Department for Business, Information security breaches survey". Technical Report, PwC, UK.

[4]. Sipior J.C. and Ward B.T. (2008). *Issues in Informing Science and Information Technology*, Vol. 5, pp. 51-60.

[5] Siponen M. and Willison R. (2009). *Information and Management*, Vol. 46, No. 5, pp. 267-270.

[6]. Alfantookh A. (2009). "An Approach for the Assessment of The Application of ISO 27001 Essential Information Security Controls". *Computer Sciences*, King Saud University.

[7]. Potter C. and Beard A. (2010). "*Information security breaches survey 2010*", Price Water House Coopers, Earl's Court, London.

[8]. Barker W.C. (2003). "Guide for mapping types of information and information systems to security categories", *Network Security*.

[9]. Wilson C. (2014). "Cyber threats to critical information infrastructure". In *Cyber terrorism*, Springer New York, 123-136.

[10]. Friedman A. and Singer P. (2014). *Cyber security and Cyber war*: what everyone needs to know.

[11]. Tripathi S.P., Goyal R., Shukla P.K. (2014). *Introduction to information security and cyber laws*, KLSI

ABOUT THE AUTHOR

Mr. Dar is presently working in the Department of Computer Science, School of Technology, Islamic University of Science and Technology Awantipora (IUST), Pulwama, Jammu and Kashmir, India. He received his Masters Degree in Computer Science and Applications from Indira Gandhi National Open University. He has 11 years of Technical and Research experience and has 12 National and International Publications besides Workshops, Conferences and Seminars of both National and International repute. He has worked as Senior/guest faculty at Global Collage of Professional Studies Humhama Srinagar and Academic Councilor IGNOU Srinagar and Annatnag Centre. He is associated in the Field of research since 2009. His Field of research is Cyber Security, Cloud Computing and Information Security. He is also a member in International Association of Engineers.