Journal of Computer Science 4 (10): 864-870, 2008
ISSN 1549-3636

Information Protection in Academic Campuses: A Scalable Framework

D.S. Bhilare, A.K. Ramani and Sanjay Tanwani
School of Computer Science, Devi Ahilya University, Indore, India

Abstract: Problem statement: Most institutions recognize the critical role that information security risk management plays in supporting their missions and objectives. Often, institutions do not pay enough attention towards assessing effectiveness of existing security measures. They are also unable to respond to new security threats in reasonable time. Furthermore, new laws are also forcing institutions to manage security risk more closely and effectively than in the past. **Approach:** In this study, metric based assessment and exception handling plan has been proposed, specific to the needs of an academic environment. Organization structure and reporting strategy which is crucial for effective implementation and monitoring is also proposed. **Discussion and Conclusion:** Proposed assessment metric enables small institutions to make a moderate but quick start, as essential measures are identified and prioritized. As and when institutes gain more experience and resources, remaining levels of the metric can also be implemented. Secondly, to reduce response time, a novel role based communication of exceptions is proposed. Responsibilities are distributed across the institution and security exceptions are reported directly to the predefined roles, responsible for that particular security control. The proposed plan will improve overall risk management with quick response time.

Key words: Information protection, security assessment, scalable framework

INTRODUCTION

Today's Campus Networks are complex grouping of technology (including hardware, software and firmware), processes, students, faculty and staff, all working together to provide institutions with the capability to process, store and transmit information on a timely basis to support various academic and administrative functions. The selection of appropriate security controls is an important task that can have major implications on the operations and assets of an institution. Once employed within an information system, security controls are assessed to provide the information necessary to determine their overall effectiveness; that is, the extent to which the controls are implemented correctly, operating as intended and producing the desired outcome with respect to meeting the security requirements for the system.

It is well known that you cannot mange some thing which can not be measured. Therefore, in order to improve the security levels it is necessary that we understand the strength and weakness of the practices being followed. A comprehensive metrics will help in making informed decisions thereby strengthening security in identified areas.

Though, Information Security is an emerging area but there are enough solutions and products available which are being deployed at various levels. There are Information Security practices and policies in place for quite some now. But measuring of effectiveness of these products and practices is one of the major challenges in Information Security Management. Many institutions, invest in security technologies, policy documents, staff training, but often find no correlation between increased spending on such initiatives and a better overall security record[1].

There are number of incidences which shows the potential for manipulating and exploiting technologies commonly utilized by universities and colleges today[2].

In this study, information security assessment plan is proposed, keeping in view the expectations of academic institutions and relevant regulatory requirements. Basic objective of this plan is not only to provide a checklist of security metric but to provide an inbuilt evaluation and role-based response system. Proposed metric, addresses specific requirements of three levels of institutions, namely small, medium and large. This approach facilitates Iterative implementation and serves as a starting point for small institutions, for protecting their valuable information assets. Another important issue addressed in this study is exception reporting. Exceptions found during assessment and continuous network monitoring, are reported directly to the linked role as specified in the proposed metric, by

Corresponding Author: D.S. Bhilare, School of Computer Science, Devi Ahilya University, Indore, India

an e-mail or SMS alerts. Each metric is associated with a role and corresponding responsibilities. This reporting system should reduce response time required for taking remedial action.

Related work: Information assessment taxonomy[3] for IT Network assessment, divides the metrics space into three categories: Security, Quality of Service (QoS) and availability. These three are further divided in technical, organizational and operational categories.

Saydjari[4] has given pros and cons of considering risk as a base metric. One good property of risk as a security metric is that it directly addresses possible threats and damages. It also deals with how adversaries really attack systems. It also tells about risks fully or partially unattended in a given system and can be used directly by a system owner to decide on acceptability of that risk. One shortcoming is that the metric doesn't explain how to rectify threats.

Policy-Based metrics look at quantities like number of unauthorized login attempts, files accesses and so on. These metrics may end up measuring the inadequacy of user training more than it measures actual system security. Incident-Based metrics look at the actual successful attacks that occur, the frequency and the real damages. This approach is promising and, with time, can become a reliable and useful metric. Currently, there is insufficient data on attack incidence and damage assessments.

None of the approaches mentioned above provide inbuilt role-based assessment mechanism and exception handling, neither considers issues pertaining to small academic institutions having limited resources. Most of the approaches provide a generalized list of metric without defining associate roles and responsibilities. NIST publications[6] provide a broad categorization of roles. Secondly, there has been little consideration for academic environment, as generally focus is on industry.

MATERIALS AND METHODS

In order to propose a robust and flexible assessment metric, it is essential that we understand necessary measures required in general to protect institutional information assets. This includes various technical, operational and managerial aspects to protect the confidentiality, integrity and availability of the system and its information. These measures are needed to accomplish institutional objectives, protect information assets, fulfill legal responsibilities and protect interest of various stake holders. Indian IT Act 2000, amended on October 16, 2008 describes legal obligations of the institutions[9].

Proposed metric facilitates incremental implementation and pointed reporting. Proposed plan can be implemented on incremental basis, as security culture and awareness matures in the institution. This will assist small and medium sized institutions particularly, in assessing their existing security plans and assuring an acceptable level of security to begin with. This will also improve exception handling, as messages are delivered immediately and directly to the associated role. This effective communication process, where information is sent to right person in time, will reduce time taken in planning and implementation of remedial action. This will improve overall security management, as assessment outcomes are acted upon quickly.

Another contribution is creation of new roles which were non existent in the traditional IT setup earlier and association of existing and new roles with each metric. These new roles are necessary to manage this complex and developing discipline. Key responsibilities and accountabilities of these new roles are also defined and data base of their e-mail addresses and mobile numbers is maintained. As every metric is associated with a unique role, there is no conflict among roles and no time is wasted in taking actions. These provisions will help in assuring a more secure environment with effective implementation and monitoring.

Identification of roles and their job description: In order to implement an efficient and effective information security plan, a suitable organization structure is essential. For a normal routine management, a centralized structure is more suitable, but for effective exception handling and quick reaction, traditional hierarchical system does not serve the purpose. Therefore, a role-based direct reporting system is proposed, where exceptions needing immediate attention are conveyed to the right person in minimum possible time. Time taken to respond a particular event is very critical, particularly in Information Security Management. Secondly, as institutions are answerable and responsible for compliance with existing laws, it is crucial that responsibilities and accountabilities are clearly defined. Therefore, a formal organizational structure, having clear identification of relevant roles and their respective responsibilities and accountabilities is suggested. In view of the complexity and requirements of this new discipline, there is a need for new roles in addition to the existing ones. Accordingly, roles are suggested, namely, Vice-Chancellor/Executive-Council, Information Security Task Force, Registrar, Legal Advisor, Deans, Head of Departments, Dean Student Welfare, Application

Owners, Director Information Technology Services, Chief Information Security Officer, Information Security Officer, Network Administrators, IT Staff and, Users. Key responsibilities of suggested roles, specific to the needs of Indian universities are described as under.

Vice-chancellor/executive-council: Executive-Council comprises prominent persons from society and academics, in addition to governor nominees.

Key responsibilities:

- Responsible for the overall information security of the University
- Manages strategic, operational and financial risks
- Establishes that Risk reporting, controls and review functions are in place
- Ensures the University systems comply with applicable law, regulations and ethics
- Approves necessary budgets

Information security task force: This body comprises University senior Academic, Administrative and IT representatives, who will co-ordinate the management and implementation of information security measures.

Key responsibilities:

- Supports the Director IT services and Chief Information Security Officer in ISA initiatives
- Approves methodologies and processes for information security

Deans and head of departments:
Key responsibilities:

- Monitor and report to the VC on compliance with mandatory information security policies within their faculty/department
- Take appropriate disciplinary actions relating to users who breach IT security policies
- Make business continuity plan in coordination with Director IT and CISO

Registrar (head of administration, finance, development, establishment): The Registrar is responsible for Administration, Examination, Human Resources, Finance, Legal Department and reports to the Vice Chancellor.

Key responsibilities:

- Accountable to the VC regarding information security risk management
- Ensures information security risks are managed to an acceptable level
- Responsible for legal aspects and acts as an interface with external world

Application owners: The application Owner is the University Employee responsible for the particular application. For example, the Deputy Registrar (Exam.) is owner of the result processing application.

Key responsibilities:

- Accountable for protecting the information assets within the systems they own
- Develop access policies for systems they own
- Notify all system security issues to the Chief Information Security Officer

Director information technology services: The director reports to the Vice-Chancellor and is responsible for the provision of enterprise information services to the University, including; the management of the University's networks and related IT Services.

Key Responsibilities:

- Ensures information security is addressed as part of all IT projects
- Develops Information Security Policies, Guidelines, Processes and Standards
- Ensures infrastructure, systems and applications implemented and maintained
- Coordinate with ISTF and CISO

Chief information security officer:
Key responsibilities:

- Collaborates and liaises with all information security stakeholders
- Formally assesses information security related risk and develops mitigation plan
- Develops information security policies
- Coordinates security awareness initiatives

Information security officer:
Key responsibilities:

- Oversees monitoring to detect breaches of security related policies
- Manages the response to any security incidents
- Develops or customizes in house security solutions
- Monitors online resources and provides appropriate security consultancy

Network administrators and it staff:
Key responsibilities:

- Prepare procedures that implement the IS security policies in their local environment
- Take reasonable precautions to guard against corruption, compromise or destruction; e.g., conduct security scans, take backups
- Maintain administrative accounts
- Applying all relevant security patches
- Develop procedures, guidelines and standards; e.g., hardened server configurations

External consulting agencies: The University must ensure risks associated with third party organizations while providing access to our internal systems. External organizations must therefore:

Key responsibilities:

- Ensure proper information security management
- Ensure that all tools used or deployed are certified or follow mutually agreed standards
- Take responsibility of proper conduct of their employees

User (faculty, staff and student): Comply with University security policies as published on the University web site.

In addition to above, new roles may be created, depending upon changes in technical or managerial skill requirements. This distribution of responsibilities has dual advantage: As institutions are answerable and responsible for any violations of prevailing laws, structure proposed above will pinpoint non performing roles. Second advantage will be swift communication of messages to the right person in less time so that overall reaction time is reduced. Thus, non ambiguous roles and responsibilities will help in effective implementation of the information security plans. After identifying and describing required roles and responsibilities, now assessment metric necessary to measure effectiveness of security controls and practices, along with associated roles and level is proposed in the following section.

Proposed assessment metric: While proposing the metric, efforts are made to ensure that the metric:

- Enables consistent, comparable and repeatable assessments of security controls
- Facilitates cost-effective assessments of effectiveness of security controls
- Generates comprehensive and reliable information to support security assurance decisions

Proposed metric covers various issues pertinent to University Environment, identified on the basis of policy documents of various universities[6,8,10].

Implementation of the full set of metric described below may not be practical for even large institutions. Therefore, an incremental approach is proposed, where institutions may begin with a base set of metric which is subset of full metric. Over the period, as institutions mature and get more resources, full set of metric may be implemented. Incremental approach ensures basic minimum security with minimal resources, remaining measures may be incorporated as institutions gain more experience and get additional budget allocation depending on success of the implementation of base plan.

Based on the guidelines published by various standards agencies NIST (800-53, 800-55)[7,5], ISO 17799, Policy documents of various universities[6,8,10], Indian IT Act 2000[9], UGC/AICTE guidelines and the requirements of academic environment as discussed above, the following metric is proposed in Table 1. There are three columns in the table namely role, indicator and control. Control column, describes security measures to be assessed. Role column, describes roles responsible for a metric. Each metric is associated with a unique role, so that there are no ambiguities and plans are implemented smoothly. In order to assist start up institutions or institutions in early phase of Information Security implementation, level of metric is shown in the indicator column. Base line metrics which should be implemented in the first phase are indicated by "S". Medium sized institutions may use additional metrics indicated by "M".

Coding structure used in the metric:
Role column:

VC: Vice-Chancellor/Executive-Council
ISTF: Information Security Task Force
REG: Registrar (Head of Administration, Finance, Development, Establishment)
LA: Legal Advisor
DN: Deans and Head of Departments
DSW: Dean Student Welfare
AO: Application Owners
DIT: Director Information Technology Services
CISO: Chief Information Security Officer
ISO: Information Security Officer
NA: Network Administrators and IT Staff

Table 1: Role Based Information Security Metric

Sno	Role	Indi-cator	Control
1.	VC	M	Number of institutional functions, Number of functions for which protection is planned
2.	VC	L	Estimated financial loss from security incidents
3.	VC	M	Percentage of service down time due to security incident
4.	VC	S	Number of key information assets, Number of assets for which protection is planned
5.	VC	S	Number of external compliance/legal requirements, How many of them have been addressed?
6.	VC	S	Number of departments, Number of departments having business continuity plan
7.	CISO	M	Percentage of users whose access privileges have been reviewed during this reporting period a. Application users, b. Application owners, c. Retired/Terminated/Suspended employees
8.	CISO	L	Number of known security risks that are related to third party relationship
9.	CISO	M	Number of critical assets or functions for which outsourcing has been done
10.	CISO	S	Number of individuals who are able to assign security privileges
11.	CISO	S	Preparation of management report with target values for chosen metric
12.	CISO	S	Percentage of systems and applications that perform password policy verification
13.	CISO	S	Percentage of systems where vendor-supplied accounts and passwords have been changed
14.	CISO	S	Percentage of computer where configuration changes are done as per policy
15.	CISO	S	Percentage of system where event and activity logs are maintained, Percentage of system where logs are monitored
16.	CISO	S	Percentage of system for which log size and retention period have been specified
17.	CISO	S	Percentage of system that give alert for suspicious activity
18.	CISO	S	Percentage of workstations with malicious code protection
19.	CISO	S	Percentage of servers with automatic malicious code protection
20.	CISO	S	Percentage of systems where latest approved patches are installed
21.	CISO	S	Percentage of firewalls configured in accordance with policy
22.	CISO	S	Number of privileged users, Number of users where justification of privileges is examined
23.	DIT	L	Percentage of remote users who access network using secure communication methods
24.	DIT	M	Percentage of new users, undergone basic security training before using network
25.	DIT	M	Percentage of users who completed periodic refresher training as required by policy
26.	DIT	M	Mean time from vendor patch availability to patch installation
27.	DIT	L	Percentage of software changes that were reviewed for security impacts
28.	DIT	M	Percentage of backup media stored offsite in secure storage
29.	DIT	S	Percentage of servers under controlled physical access
30.	DIT	S	Percentage of systems for which approved configuration setting have been implemented as required by policy
31.	DIT	S	Percentage of systems that are being monitored for configuration policy compliance
32.	DIT	S	Percentage of computers whose configuration is compared with a trusted baseline
33.	DIT	S	Percentage of systems with critical information assets or functions where restoration has been successfully demonstrated
34.	DIT	S	Percentage of used backup media sanitized prior to reuse or disposal
35.	DIT	S	Percentage of systems with critical assets that have been assessed for vulnerabilities
36.	DN	S	Number of department wise security breaches by the students, Number of cases where action has been taken
37.	DN	S	Percentage of equipment, which are protected from power failures
38.	DSW	L	Percentage of foreign students for whom background check is carried out
39.	DSW	S	No. of incidents where students transmitted obscene material to colleagues, No. of incidents reported to proctorial board
40.	DSW	M	Number of social engineering incidences resulted in financial loss to students
41.	ISO	S	Percentage of systems with account blocking parameters are set as per policy
42.	ISO	S	Percentage of systems with automatic timeout is set as per policy
43.	ISO	S	Percentage of systems where permission to install non-standard software is limited
44.	ISTF	L	Percentage of performance reviews that include IS related issues
45.	ISTF	L	Percentage of critical information assets stored in encrypted form
46.	ISTF	M	Percentage of Security roles for which responsibilities and authority are assigned
47.	ISTF	L	Total number of meetings where IS was on the agenda
48.	ISTF	M	Percentage of staff assigned responsibilities from IS policies and controls
49.	ISTF	M	Percentage of IS policy compliances reviews with no violations
50.	ISTF	M	Percentage of user roles, systems and applications that comply with the separation of duties principle
51.	ISTF	M	Percentage of critical assets and functions for which cost of compromise has been quantified
52.	ISTF	M	Percentage of security incidents that involved third-party personnel
53.	ISTF	M	Percentage of third-party agreements that have been reviewed for IS requirement compliance
54.	ISTF	M	Percentage of systems with critical information assets that use stronger authentication than user-id and password
55.	ISTF	S	Percentage of systems and applications where user privileges are role-based
56.	ISTF	M	Percentage of mobile devices that are -examined before granting network access, with automatic malicious code protection, using encryption for information assets
57.	ISTF	M	Percentage of passwords and PINS that are encrypted in accordance with policy
58.	ISTF	M	Number of hacking attempts from university domain reported by commercial organization
59.	ISTF	S	Periodic comparative review of various critical IS metric
60.	ISTF	S	Percentage of systems where configuration do not deviate from approved standards
61.	ISTF	S	Percentage of systems with critical information assets have been backed up

Table 1: Continued

62.	ISTF	M	Percentage of vulnerability assessment findings that have been addressed since last reporting period
63.	REG	L	Number of total incidents, Number of incidents that did not cause damage beyond limit
64.	REG	M	Number of required internal/external audits Number of required internal/external audits completed
65.	REG	M	Number of audit findings Number of audit finding resolved
66.	REG	M	Number of employees handling confidential information, Number of employees who have signed non-disclosure agreement
67.	REG	M	Percentage of department heads who have ensured compliance with IS policy and controls
68.	REG	M	Percentage of job descriptions that defines IS roles, skills for 1: Security Administrators, 2: IT Staff, 3: General application Users
69.	REG	M	Number of identified risks Number of risks having mitigation plan, Number of risks for which status is reported as per policy
70.	REG	S	Percentage of departments with business continuity plan, Percentage of plans that have been reviewed and updated
71.	REG	S	Percentage of critical assets that have been reviewed for physical risks, Percentage of critical assets for which action is taken
72.	REG	S	Percentage of critical assets that have been reviewed for environmental risks such as fire, flood, earthquake etc
73.	REG	S	Percentage of sections, where physical border security has been implemented to protect the Information processing service.
74.	REG	M	Percentage of host servers that are protected from becoming relay hosts

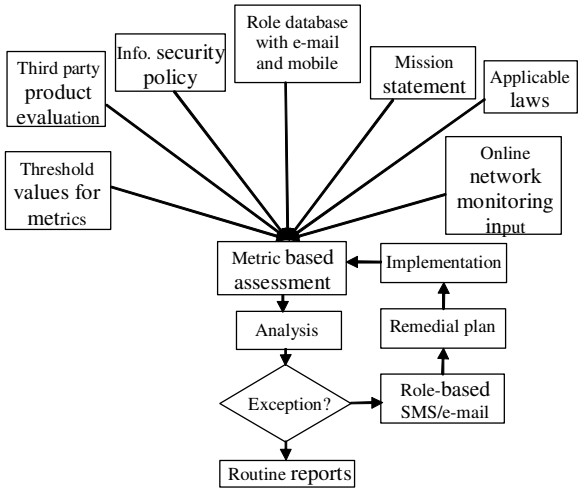

Fig. 1: Information Security Assessment and Pointed Reporting

Indicator column:

S: Indicates base metric, Starting Point for beginners, applicable to all
M: Applicable to Medium sized University/College with moderate resources
L: Applicable to Large Universities with ample resources

The metric proposed above can be implemented in a phased manner, iteratively. Initial round of assessment will give an idea of present state of security, in the institution and areas where more attention is required. Accordingly, risk mitigation strategies can be planned and implemented. This cycle may be repeated, till full metric implementation is achieved. This process would also lead to enhancement in the proposed metric.

Assessment and reporting: Figure 1 shows an overview of the assessment and reporting procedure. Assessment of present security measures is carried out using proposed assessment metric and various other inputs described as under:

- Applicable Laws, Information Security Policy and Mission statement are considered, while adapting proposed metric by any institution
- Third party product reviews, which are available publicly for the products being used
- Threshold values for the assessment metric, which are arrived at, on the basis of level of security desired by the institution
- Out come of the online network monitoring and analysis
- Role database with e-mail addresses and mobile numbers, required for sending exception alerts

Whenever, threshold values are violated for a particular metric, or an online network monitoring software detects, some suspicious activity, an exception condition occurs. This exception triggers a search in the data base for getting the associated role and contact information for that particular exception. After getting required information message is sent by an SMS or e-mail. Based on the information and situation analysis, remedial action is planned and implemented.

The outcome of above assessments can be used to:

- Identify potential problems or shortcomings of present measures
- Prioritize risk management plans
- Confirm that problems identified earlier are addressed
- Justify budgetary provisions

DISCUSSION

Establishing a resilient information security mechanism, for higher education requires not only

understanding of expectations of academic environment and relevant threats but a collective effort where all stake holders are involved. Such mechanisms can't be established overnight, however, with proposed approach, effective governance can be ensured.

Proposed metric based assessment and reporting plan has been designed as per the specific needs of an academic environment. Additional roles are created and their key responsibilities and accountabilities are defined, which is necessary to manage this complex and evolving discipline. Each metric is associated with a predefined role. In order to assist small and medium institutions each metric is prioritized. Security exceptions are reported directly, without wasting any time to the predefined roles responsible for that particular security control.

CONCLUSION

As each metric is prioritized, an incremental assessment can be planned, depending on available resources. Secondly, exception handling is distributed across the institution and alerts are communicated directly to the concerned role. This approach helps in reducing response time, as right person is involved and more time is available for planning and implementation. The proposed solution, will improve overall security governance. Reduction in response time is very crucial for effective security governance.

Future work: Design of an automated process to assess vulnerability score using open data bases.

REFERENCES

1. Berinato, S., 2007. The fifth global state of information security, CIO Magazine. http://www.cio.com/article/133600/The_Fifth_Annual_Global_State_of_Information_Security?page=1
2. Peter Adler, M., 2006. Unified approach to information security compliance. Educause Rev., 41: 46-61. http://connect.educause.edu/Library/EDUCAUSE+Review/AUnifiedApproachtoInforma/40660
3. Bellocci, T., C.B. Ang and P. Ray, 2001. Information assurance in networked enterprises: definition, requirements, and experimental results. Report No. 01-05. https://www.cerias.purdue.edu/assets/pdf/bibtex_archive/2001-34.pdf
4. Saydjari, O.S., 2006. Is risk a good security metric? Proceeding of the 2nd ACM Workshop on Quality of protection, Oct. 30-30, Alexandria, Virginia, USA., pp: 59-60. http://doi.acm.org/10.1145/1179494.1179508
5. Swanson, M., Bartol, N. Sabato, J. Hash, J. Graffo and L. Security 2003. Metrics Guide for Information Technology Systems. http://connect.educause.edu/Library/Abstract/SecurityMetricsGuideforIn/44961
6. Auckland University Newzeland, 2008. Information security organization policy. http://www.security.auckland.ac.nz/SecurityOrganisationPolicy.htm
7. Ron Ross, 2007. NIST SP-800-53A, Guide for assessing the security controls. https://cramer.cs.nmt.edu/~risk/RA_PPT/risk_assessment_nist_sp800_53a.pdf.
8. University of Houston, IS Policy, http://www.uh.edu/infotech/php/template.php?security_id=31
9. Information Technology ACT, 2000. www.eprocurement.gov.in/news/act2000mod.pdf
10. Washington University Policy document, 2007. http://www.wustl.edu/policies/compolcy.html