Information Security Assessment and Reporting: Distributed Defense

D.S. Bhilare[1]*, A.K. Ramani[1] and Sanjay Tanwani[1]

ABSTRACT

Network Managers of Higher Educational Institutes, are well aware of general Information Security issues, related to Campus Networks. There are well developed security metrics, giving exhaustive list of security controls, required to mitigate different risks. Accordingly, various security measures and technologies are being deployed. However, at present, not enough attention is being paid on measuring the effectiveness of these controls and overall state of security in the institution. In this study, attempt is made to build a metric based assessment and reporting plan, specific to the needs of an academic environment. Proposed assessment metric facilitates iterative implementation, by prioritizing each metric. Secondly, to reduce response time, a novel approach of pointed reporting is suggested, where responsibilities are distributed across the institution, based on relevant roles. In this approach, security exceptions are reported directly to the predefined roles, responsible for that particular security control. This pointed reporting, delivers message to the right person in minimum time, resulting in improved response time. The proposed assessment metric and pointed reporting structure, will improve overall security governance. As security measures and practices can be assessed systematically and remedial actions can be taken in less time, which is so crucial for effective security governance.

Keywords: information security, security assessment, pointed reporting, distributed defense, iterative implementation

1. 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. As institutions are dependent on these network based information systems to conduct their routine and critical functions, security of these systems is decisive to the success of the institution. The selection of appropriate security controls is an important task that can have major implications on the operations and assets of an institution. Security controls are the management, operational, and technical safeguards or countermeasures prescribed for an information system to protect the confidentiality, integrity, and availability of the system and its information. 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

[1] School of Computer Science & IT, Devi Ahilya University, Indore, India

**Corresponding author :* (E-mail : bhilare@hotmail.com, Telephone: +91 9826606366)

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 systematic evaluation also assures continuity of services and develops confidence in the system. 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 (Adler, 2006; Berinato, 2003).

There are number of incidences which shows the potential for manipulating and exploiting technologies commonly utilized by universities and colleges today (Adler, 2006) . The proliferation of e-mail use, distance learning and other services that enhance the quality of the student experience and extend education beyond the campus carry a potentially significant price when privacy is not maintained.

In this paper, information security assessment plan is proposed, keeping in view the expectations of academic institutions & relevant regulatory requirements. Basic objective of this plan is not only to provide a checklist of security metric but to provide an inbuilt evaluation & 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 paper is exception reporting. Exceptions found during assessment & continuous network monitoring, are reported directly to the linked role as specified in the proposed metric, by 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.

The rest of this paper is organized as follows. In section 2, related works are shown. Section 3.1, identifies various roles necessary to implement proposed assessment plan and their key responsibilities. In section 3.2, proposed assessment plan and reporting system is described. Section 3.3, describes assessment, reporting process and possible applications of outcome of assessment. Finally in section 4, conclusion along with future work is presented.

2. Related Work

Information assessment taxonomy (Bellocci, et.al.2001) 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 (Sami, 2006) 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. In fact, to the extent that risk analysis methods have been developed, they are difficult to put in practice due to the following reasons:

- One must have a complete understanding of all possible attacks. This is particularly difficult because attackers can be incredibly creative and innovative.
- One must assess the probability of attackers attempting attacks and their probability of success.
- To assess the consequences for the attack, one needs a good model of the owner's mission, the owner's system, and how the system supports the mission.
- It is very difficult to validate the accuracy of a risk metric because ground truth is difficult to establish.

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(http://csrc.nist.gov/publications) provide a broad categorization of roles. Secondly, there has been little consideration for academic environment, as generally focus is on industry.

3. Information Security Assessment Metric and Reporting

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, 2006 describes legal obligations of the institutions (www.eprocurement.gov.in/news/act2000mod.pdf) .

Security assessment is not about generating paperwork to pass inspections or audits. Rather, to verify that the implementers and operators of information systems are meeting their stated security goals and objectives.

Proposed metric facilitates iterative implementation and pointed reporting. Proposed plan can be implemented on iterative 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.

3.1 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 & 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 & academics, in addition to governor nominees. Key Responsibilities include:

- Responsible for the overall information security of the University
- Manages strategic, operational and financial risks
- Promotes and supports information security initiatives as part of the risk management
- 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 include:

- Supports the Director IT services & Chief Information Security Officer in ISA initiatives;
- Approves methodologies and processes for information security
- Co-ordinates the implementation of specific information security measures for new systems or services

Deans & Head of Departments

Key Responsibilities include:

- 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 proposals for necessary funding to meet information security commitments
- Develop and implement additional security policies specific to their faculty/department, in coordination with the Chief Information Security Officer(CISO)
- Make business continuity plan in coordination with Director IT and CISO

Registrar (Head of Administration, Finance, Development, Establishment etc.)

The Registrar is responsible for Administration, Examination, Human Resources, Finance, Legal

Department and reports to the Vice Chancellor. Key Responsibilities include:

- 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

Legal Advisor

Legal advisor may be a part time or full time employee. Major responsibilities of the legal advisor are as under: Key Responsibilities include:

- Advises VC/Registrar about applicable laws, regulations
- Ensures that all third party contract documents include appropriate provisions with respect to information security
- Understands various international cyber laws and its implications

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 include:

- Accountable for protecting the information assets within the systems they own
- Develop access policies for systems they own
- Ensure new applications comply with security policies
- 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 include:

- Ensures information security is addressed as part of all IT projects
- Maintains an up-to-date record of major information security risks
- Develops Information Security Policies, Guidelines, Processes and Standards
- Ensures infrastructure, systems and applications implemented & maintained
- Coordinate with ISTF & CISO

Chief Information Security Officer

Key Responsibilities include:

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

Information Security Officer

A technical expert assists the CISO and other users in technical matters. Key Responsibilities include:

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

Network Administrators and IT Staff

Network Administrators responsibilities include system, sites or networks administration. They are responsible for installing hardware and software, managing a computer or network, deploying security controls, and keeping a computer or network operational. Key Responsibilities include:

- 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 include:

- 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. Key Responsibilities include:

- Notify all system security issues to the department head & ISO
- Use the facilities in an ethical and legal manner
- Safeguard passwords and/or any other sensitive access
- Ensure that accounts and network privileges are restricted to own use only
- Do not carry out unauthorized mass electronic mailing or news posts
- Do not conduct security experiments without specific authorization
- Do not delete or alter information or data of others without their permission
- Do not misuse resources, spread malicious software or permit misuse of system resources by others
- Do not try to break others passwords from password files or network traffic.

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 & 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.

3.2 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;
- Promotes a better understanding of the risks to organizational operations, organizational assets, individuals, and other organizations; and
- Generates comprehensive and reliable information to support security assurance decisions.

Proposed metric covers the following issues pertinent to University Environment, identified on the basis of policy documents of various universities (http://www.uh.edu/infotech; http://www.wustl.edu/policies/compolcy.html):

- Avoid distasteful, inflammatory, harassing or otherwise unacceptable messages.
- Respect the privacy of others and their accounts.
- Distribution of excessive amounts of unsolicited mail is inappropriate.
- Most of the information published on Internet is protected by copyright law. Copyright protection also applies to much software, individual users and the University may, in some circumstances, be held legally responsible for violations of copyright.
- Many laws, including those prohibiting defamation, violations of privacy, obscenity, and deceptive advertising, apply to network-based communications.
- Because the Internet is international, laws of other countries may apply.
- Internet resources are basically for academic activities. Its use for social and entertainment purposes should be restricted to the extent that such use does not affect the amount of bandwidth available for academic use.
- The University is not responsible for the views expressed by individual users. Under certain circumstances, however, the University may be held liable if it fails to take reasonable remedial steps after it learns of illegal activities.
- The University is the custodian of a wide array of personal and financial data concerning its students, staff, faculty and patients, as well as the University itself.
- Shared facilities should not be tampered, it may disrupt normal operations.
- The University may be compelled by law or policy to examine even personal and confidential information maintained on University computing facilities.
- The use of University resources for commercial or for political activities is inappropriate and possibly illegal.

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)(Ron, 2007) , ISO 17799, Policy documents of various universities(http://www.uh.edu/infotech; http://www.wustl.edu/policies/compolcy.html), our earlier work(Bhilare et. al., 2008) , Indian IT Act 2000 (www.eprocurement.gov.in/news/act2000mod.pdf), UGC/AICTE guidelines and the requirements of academic environment as discussed above, the following metric is proposed in Table I. 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 & 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

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

Table 1: Role Based Information Security Metric

S. No.	Role	Indicator	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 event and activity 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 from a stored backup 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	Number of incidents where students transmitted obscene material to colleagues Number 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 & functions for which cost of compromise

			(loss, damage, disclosure, disruption in access) 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 system architecture changes that has IS approval
55.	ISTF	M	Percentage of systems with critical information assets that use stronger authentication than user-id and password
56.	ISTF	S	Percentage of systems & applications where user privileges are role-based
57.	ISTF	M	Percentage of mobile devices that are -examined before granting network access -with automatic malicious code protection -using encryption for critical information assets
58.	ISTF	M	Percentage of passwords and PINS that are encrypted in accordance with policy
59.	ISTF	L	Number of security incidents that exploited existing vulnerabilities with known tools Number of systems affected that exploited existing vulnerabilities with known tools
60.	ISTF	M	Number of hacking attempts from university domain reported -By commercial organization -From national security point of view
61.	ISTF	S	Periodic comparative review of various critical IS metric
62.	ISTF	S	Percentage of systems where configuration do not deviate from approved standards
63.	ISTF	S	Percentage of systems with critical information assets have been backed up
64.	ISTF	S	Percentage of security incidents that were managed in accordance with established policies, procedures and processes.
65.	ISTF	M	Percentage of vulnerability assessment findings that have been addressed since last reporting period
66.	REG	L	Number of total incidents Number of incidents that did not cause damage beyond limit
67.	REG	L	Percentage of third party agreements where information security is part of the agreement and are implemented
68.	REG	L	Percentage of users who have undergone background checks
69.	REG	M	Number of required internal/external audits Number of required internal/external audits completed
70.	REG	M	Number of audit findings Number of audit finding resolved
71.	REG	M	Number of employees handling confidential information Number of employees who have signed Confidentiality or non-disclosure agreement
72.	REG	M	Percentage of department heads who have ensured compliance with IS policy and controls
73.	REG	M	Percentage of job descriptions that defines IS roles, skills for 1:Security Administrators 2:IT Staff 3:General application Users
74.	REG	M	Number of identified risks Number of risks having mitigation plan

			Number of risks for which status is reported as per policy
75.	REG	M	Percentage of information assets that have been classified as per policy
76.	REG	S	Percentage of departments with business continuity plan
77.	REG	M	Percentage of continuity plans that have been reviewed, tested and updated
78.	REG	S	Percentage of critical assets that have been reviewed for physical risks Percentage of critical assets for which risk mitigation plan are implemented
79.	REG	S	Percentage of critical assets that have been reviewed for environmental risks such as fire, flood, earthquake etc
80.	REG	S	Percentage of sections, where physical border security facility has been implemented to protect the Information processing service.
81.	REG	M	Percentage of host servers that are protected from becoming relay hosts

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.

3.3 Assessment and reporting

Figure I, gives 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:

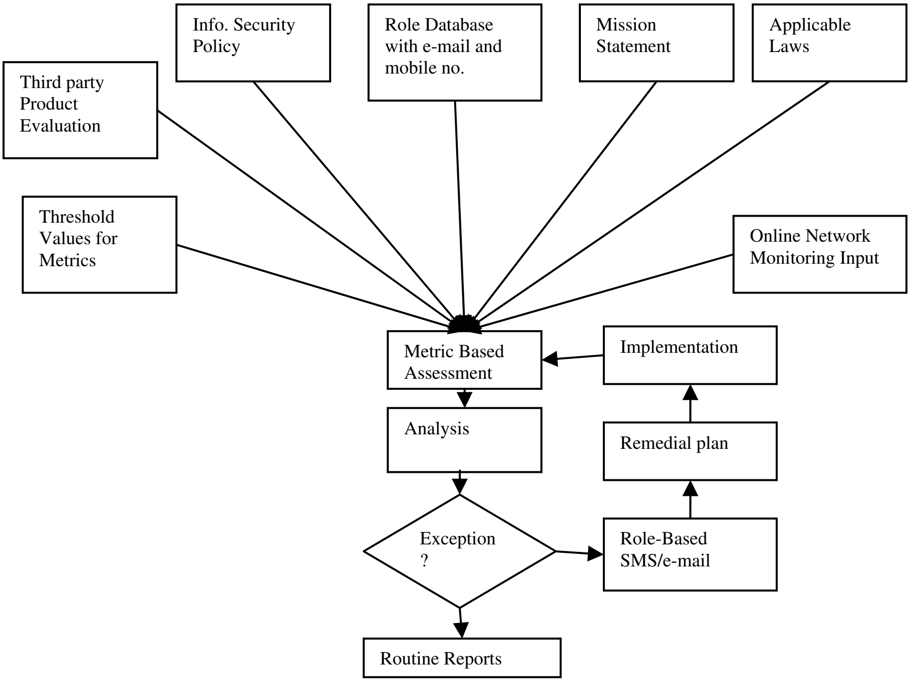

Figure 2: Information Security Assessment and Pointed Reporting

- 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 & 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 & 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; and
- Justify budgetary provisions.

4. Concluding Remarks

Establishing a resilient information security mechanism, for higher education requires not only understanding of expectations of academic environment & 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 & accountabilities are defined, which is necessary to manage this complex and evolving discipline. Each metric is associated with a predefined role. As each metric is prioritized, an iterative assessment can be planned. Secondly, exception handling is distributed across the institution, and approach of pointed reporting is adopted. Security exceptions are reported directly, without wasting any time to the predefined roles responsible for that particular security control. This pointed reporting helps in reducing response time, as right person is involved and more time is available for planning and implementation. The proposed assessment metric and pointed reporting structure, 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. Another issue is design of a model projecting an optimal investment plan, keeping in view the financial value of assets, and potential tangible or intangible gains or losses in monetary terms.

References

1. Berinato, S. (2003) The state of information security 2003. *CIO Magazine* 17, 2 (Oct. 15, 2003).
2. Bhilare D.S., Ramani A.K., Tanwani S., (2008), A Modular and Iterative Approach to Information Security Risk Management, *NCFAI-08 proceedings*, 211-217.
3. *Information Technology ACT 2000*, www.eprocurement.gov.in/news/act2000mod.pdf
4. M. Peter Adler, (2006) Uniform approach to information security compliance, EDUCAUSE Review, vol. 41, no. 5 (September/October 2006): 46–61
5. Mohammad S S, Saad H B (2005), Using ISO 17799: 2005 Information Security Management, Stope View with six sigma approach, *International Journal of Network Management*, June 2006.
6. National Institute of Standards and Technology, http://csrc.nist.gov/publications
7. Sami S O (2006), QoP’06, , *Alexandria*, Virginia, USA. ACM 1-59593-553-3/06/0010.
8. Ron R, (2007) NIST SP-800-53A, *Guide for assessing the security controls*, December 2007
9. Swanson, M., Bartol, N., Sabato, J., Hash, J., Graffo, L. (2003) Security Metrics Guide for Information Technology Systems. *NIST Special Publication* 800-55, Jul., 2003.

10. Swanson, M. (2001) Security Self-Assessment Guide for Information Technology Systems. *NIST Special Publication* 800-26, Nov., 2001.
11. Thomas Bellocci, Chwee Beng Ang, Parbati Ray, Shimon, (2001) *CERIAS Tech Report* 2001-34 Information Assurance in Networked Enterprises: Definition, Requirements, And Experimental Results, No. 01-05 Purdue University West Lafayette, IN 47907
12. *University of Houston, Information Security Manual*, http://www.uh.edu/infotech, Jan 2008
13. *University of Washington policy document*, http://www.wustl.edu/policies/compolcy.html, October 2006.
14. *University of Auckland Newzeland, Security policy and organization* http://www.auckland.ac.nz/security/SecurityOrganisationPolicy.htm#1.1, Jan 2008

About the Authors

D.S. Bhilare: M.Tech.(Computer Sc.), M.Phil.(Computer Sc.) and MBA from Devi Ahilya University, Indore. Worked as a Senior Project Leader for ten years in the industry and developed various business applications for different industries. Since last eighteen years, working in the University as a Senior Manager & Head IT Centre, involved in Computer Centre and Campus Network Management.

A.K. Ramani: Ashwani Kumar Ramani received his Master of Engineering (Digital Systems) and Ph.D, from Devi Ahilya University, Indore. He worked as a research engineer in ISRO Satellite Center, Dept. of Space, Bangalore, India, during 1979-83. Later he joined the Military College of Telecommunication Engineering, Mhow, India. From 1986-89, he was assistant professor in the Department of Electronics and Computer Engg, at S.G.S. Institute of Technology and Science , Indore, India. Since Jan. 1990, he is a professor with the School of Computer Science at Devi Ahilya University. He acted as Director of International Institute of Professional Studies, Indore, India during 1993-95 and 1999-2003. He was associate professor at University Putra Malaysia, Dept. of Computer Science during May95 toMay99. During Sept 2005- July 2006, He was with the College of Computer Science and Information Technology, at King Faisal University (KFU), Kingdom of Saudi Arabia, and was responsible as Chairman of the Accreditation Committee to pursue ABET Accreditation. He has guided 13 PhDs in different areas of Computer Science and Information Technology and has authored about 70 research papers. He has been associated with NAAC and NBA for assessment and accreditation for the past several years.

Sanjay Tanwani received his Master of Engineering (Digital Systems) and Ph.D, from Devi Ahilya University, Indore. He Joined School of Computer Science, Devi Ahilya University as a lecturer in 1986. At present he is working as a professor, since 2002.