Networking Essentials and Security

Your Name (First M. Last)

School or Institution Name (University at Place or Town, State)

.

Networking Essentials and Security

**Part 1**

**Mission Statement**

This CSIRT provides assistance and information to the staff of iFinance for reducing the computer security incidents risk as well as responding to these incidents on their occurrence.

**Vision Statement**

This CSIRT will work to help for creating reliable, clean, and safe cyberspace in the Banking operations of iFinance.

**Key Stake Holders**

1. IT Service Providers is one of the significant stakeholders for the CISRT. As it requires for establishing with all the significant parts of iFinance IT services. Internal stakeholders include developers, network engineer, and database teams.
2. Security Management team is another stakeholder require for CSIRT. The security manager as an incident responder can be expected to own every security aspect. So he should ensure that he has a route for engaging other team members of security management as well.
3. Legal Team is another stakeholder for CSIRT as cybersecurity breach incidents can open the door for several legal considerations. Security managers have to make a decision that what to report and how significant the incident may be. For this purpose, he requires guidance from the real lawyers.
4. Human Resource team is another important stakeholder require for CSIRT. As most of the security incidents happen due to users in the company so, security manager needs to be able to handle such in the right way. For this purpose, the security manager requires engaging with HR.
5. The last important Stakeholder require for CSIRT is Public Relations Team who should be expert in ensuring that the response message of the incident is the right one. If the security manager needs to communicate with the public and there is no response (Mohd, et, al., 2016).

**Personnel, Equipment, and Infrastructure**

 This model of CSIRT utilizes some existing personnel like administrators of the system, administrators of local area network or wide area network, administrators of security, administrators of the database, personnel of help desk, and developers of software for supporting any handling activity of incident at the local level. Outside resources for CSIRT can include some outsource employees which may be both partially outsourced and fully outsourced employees. In case of partially outsourced employees, the iFinance will outsource only certain elements of its CSIRT activities to the external parties while in case of fully outsourced employees the iFinance will outsource all the elements of its CSIRT to external parties. iFinance needs some managed security services provider which monitors intrusion sensors of detection, other security devices and firewalls to an offsite. They analyze and identify suspicious activities and also reports every detected incident to the iFinance's incident response team. As the internal team may not possess the essential intrusion detection system knowledge, management of vulnerability, and techniques of cybersecurity for responding properly to a security incident. Some external security facilities state of the art infrastructure of Information Technology like SOCs (Security Operations Centers) in several areas (Pfleeger, 2017).

In this case, the existing equipment of a computer, pages, telephones, and peripheral will be used. If some extra equipment will be required for the particular analysis work, it may be possible for negotiating with the other enterprises part in order to borrow or utilize the equipment like facilities of software development or lab for testing in a non-productive environment while investigating the activity of the incident. In order to support the activities of CSIRT which are based on the information security technology, network specialists are required for systems of network monitoring or scanning, installation of filters, firewalls, wrappers, virtual private network or authentication mechanism. Such services are considered to be the most significant part of the CSIRT. Some other information security technical staff required for this CSIRT include IT Team Lead or Manager, IT Assistant Managers or groups of leaders, triage or help desk staff, handlers of the incident, handlers of vulnerability, the staff of artifact analysis, trainers, platform specialist, and technology watch. Some software engineers are also required for maintaining and configuring personal digital assistants, laptops, desktop, servers, and some wireless devices on the basis of guidelines of security. Existing resources such as laptops, desktops, routers, switches, cables, and some other technical and networking devices will be needed for the support of CSIRT (Valladares, et, al., 2017).

Mostly the CSIRT will utilize the existing infrastructure which will provide the security features of computer like firewalls and separate networks, baseline configuration of the computer, guidelines of the security for administrators of the system and acceptable policies for the users.

**Policies**

1. One of the most significant policies of CSIRT, in this case, is considered to be the Network Connection Policy which describes the constraints and requirements for attaching a computer to the work of iFinance. All the computers installed on the network of iFinance fall under the responsibility and authority of the DPICSO (Data Processing Installation Computer Security Officer. In this, they can meet the minimum requirement of security of the company's policies and regulations.
2. Acceptable Encryption Policy is another efficient policy in this case which can provide guidance that limits the utilization of encryption to those algorithms which have received a substantial review of public and have also be proven for working effectively. Moreover, this policy also gives direction for ensuring that Federal regulations are followed and legal authority is granted for the dissemination and utilization of encryption technologies.
3. Information Sensitivity Policy is given for helping employees which determine what type of information can be disclosed to non-employees as well as the information relative sensitivity which must not be disclosed outside of iFinance without any proper authorization.
4. Another important policy of server security is used for establishing standards for the configuration of the base of the equipment of internal server which is owned or operated by iFinance. The efficient implementation of such policy will decrease the unauthorized access to the proprietary technology and information of iFinance.
5. Virtual Private Network Policy is used for providing guidelines for the Remote Access or Virtual Private Network of L2TP connections to the iFinance corporate network.

**Procedures**

1. Escalation Procedures for Security Incidents is considered to be one of the most significant procedures in this case which describes the steps that should be taken for computer and physical security incidents that occur within the facility of iFinance. The physical events of security which can be covered in this procedure include illegal access of organization, theft or destruction of property.
2. Incident Handling Procedure generates the document which provides some general procedure and guideline for dealing with the incidents of computer security. The purpose of this document is for providing iFinance support with some significant guidelines on discovering the incident of the security.
3. ASP Security Standards procedures is another document which defines the criteria of minimum security which an ASP (Application Service Provider) must meet to be considered for utilization by iFinance.
4. Password procedures are considered to be the most important factor of any computer security. They are front protection line for the accounts of the user. The wrongly chosen password can result in the iFinance compromise of the whole network of corporate. As such the employees of iFinance that includes vendors and contractors with access to the system of iFinance are considered to be responsible for taking the correct steps for selecting and securing their passwords.
5. The procedure of third party connection agreement is used for completing agreement between the parties for concerning the subject matter of such agreement and also replaces any written communication among the parties (Meiia, et, al., 2016).

**Reporting Structure**

The support members who are from different departments including IT, Management, PR, and Legal will report to the Assistance information security manager who coordinates with the responses of an individual and is an expert on the equipment or area where the event occurred. The CSIRT manager who is the information security manager of the iFinance will report to the management of high-level like chief security officer (Mena, et, al., 2018).

**Organization Model**

Organization Model of Internal Centralized CSIRT will be used which is considered to be completely staffed and dedicated which provides the services of incident handling for any organization. In this case, team members will spend a hundred percent of their time in order to work for this CSIRT while such model type can also be provided utilizing the staff of part-time on the basis of rotation.

**Authority**

In this case, the CSIRT has the shared authority which participates in the process of decision regarding what actions should be taken during the incident of the computer security but cannot make the decision but only influence it. It can only provide influence on the outcomes of the decision but it is the participant in the process of decision making rather than the maker of the decision. In the following case, the CSIRT can only recommend that the system can be disconnected from the network at the time of an attack and discusses the action which needs to be taken.

**Additional Cost**

This CSIRT requires ninety employees and more than five hundred employee hours for resolution and investigation which will cost more than fifty-nine thousand dollars. It will also require a hundred additional Linux Computers as well which will cost an average of fifteen hundred dollars per host. The average cost per investigation will be turned out to be more than two thousand dollars (Fuertes, et, al., 2017).

**Communication**

The communications plan is necessary for making security a priority for iFinance's employees in different offices which are distributed throughout twenty-five states. It is considered to be the most critical factor in determining whether the CSIRT is successful or not. So, in this case, setting the expectations at the top and communicating the progress with team members, constituents, peers, and supervisors are of utmost significance. The supervisors need for understanding the rewards and challenges so that they can continue to justify the assigned resources. Team members can get courage if they feel like they are making progress. Moreover, Peers need to understanding service value and expectation. Similarly, constituents also need for knowing the available service., when they can expect for receiving them, and knowing about the situation for which they are receiving it (Reyes, et, al., 2018).

**Scope**

The Scope of this CSIRT is that it is applicable to all technology and information resources, at all the level of sensitivity and operated on the behalf of the Information Security Department. Additionally, employees, outside workers of the agency, volunteers assume the reporting responsibilities of the department employee which is established within this CSIRT. It also establishes minimum standards for the iFinance functions of CSIRT

**Level of Services**

The important step after establishing the CSIRT is to define its level of services according to available resources. This CSIRT will provide a proactive level of services. It consists of post reports of the incident from constituency or other incidents which are related to attacks or threats like vulnerabilities, malware, compromised hosts or other kinds of similar incidents. It is designed for preventing and detecting the attacks before there is any impact on the system of production. In this level of services, the information generated by the CSIRT gets dispersed to their partners and constituency for protecting the assets avoiding it from any target. This level provides the services of an announcement, security pentests/audits, detection of intrusion, development of the tool, and intelligence sharing of threat (Skierka, et, al., 2015).

**Timeline**

Depending on the resources which are provided from its necessary constituency and stakeholders, CSIRT can take almost eighteen to twenty-four months in order to become completely operational. The timeline of CSIRT for iFinance can be compressed or extended that depends on several factors and decision point which are made. The availability of the number of resources will determine how swiftly the project of CSIRT can move to the starting stage from planning and then into the operations and implementations stages. There are also possibilities to overlap some of the operational and implementation components that depend on the project implementation and planning. According to an estimate for this CSIRT, the process of planning will take almost five months. The process of implementation can take nine to twelve months and the process of operations may be expected to be completed in six months. This timeline usually focuses on the initial four development stages. It does not include collaborative development phase of maturation during the activities of operation. Training and education requirements will also be scheduled at every Friday for supporting the activities of CSIRT that include information security team, incident handlers, administrative staff, support staff, and analysts. Such mentoring and training activities can affect the range and service level which are provided and implemented to the constituency. In order to make CSIRT successful, it is necessary to have a firm commitment to the project throughout every development stages as well as to have plans of long range for sustaining and operating the team over time (Lord, Rush, & Massa, 2018).

**Establishing ROI**

Establishing the ROI (Return on Investment) has several benefits related to incident management. The most significant benefit is considered to be the reduction of the volume of the incident. The reduction of handling time of the elapsed incident by the agreements of improvement between the first and second level of support teams is another benefit of ROI. It can also help in maintaining IT services quality. It can increase communication and visibility of incidents to CSIRT. Moreover, it can also increase the confidence of business in the capabilities of IT.

In order to identify the total cost of an incident, CSIRT needs to consider the direct costs of manpower, equipment, and lost production time, and also other indirect costs, such as the potential cost of lost business and damage to the company's reputation and brand image. The incident of handle time, a resolution rate of the first call is also required for this incident management ROI. Assumptions for this ROI include:

Incidents per month= 5000

Cost of Manpower, equipment =$8167

Potential Cost of Lost Business = $150

Damage to the Reputation of Company= $40

Average time in Initial Contact= 12 minute

Average time in escalated incident= 18 minute

IT headcount =100

First Call Resolution = 40%

So estimated Incident management ROl is given as below:



consider the direct costs of manpower, equipment, and lost production time, and also other indirect costs, such as the potential cost of lost business and damage to the company's reputation and brand image.

**Part 2**

After the resource commitment from the CTO, iFinance is ready for starting the process of designing and planning their CSIRT. The CSIRT manager has several tasks that start with documenting the goals, vision, and mission of the CSIRT. Some government regulations which would be required in this CSIRT include Taxes such as estimated tax, employment tax, and excise taxes, Labor and Employment Law such as wages and hours, workplace health and safety, equal opportunity, benefit security of employee, antitrust laws, advertising, environmental regulations, and privacy. Freedom of Information Act is also another government regulation which gives the right to the iFinance for accessing to the federal agency information or records. Organizationally the CSIRT of iFinance staffing structure have a full-time manager of CSIRT, members of the core team, extended team, and a representative from distributed teams. The core-team members and managers are responsible for daily operation of the core team and coordinating the efforts of CISRT across the functional areas and business units within iFinance.

The manager of CSIRT has agreements with the supervisors in the department of technology in which during the incident they will assign temporarily experts of needed subject matter without any question to CSIRT. These commitments and agreements demonstrate the importance that iFinance has placed upon the CSIRT. It also ensures that the impact of the incident on iFinance can be minimized. The security manager is responsible for the implementation of issues at a certain location. They are required for following the policies and procedures of iFinance's CSIRT. The CSIRT monitors all the activities at affiliate sites which help them for identifying potential problems at one site and spread guidance and information to the security mangers so that they can address and assess any potential or real threats which may arise quickly or proactively. In order to provide regular updates with to the senior managers, iFinance established the Information committee of security which is comprised of a security team.

The CSIRT budget of iFinance includes the cost of the salary of existing and additional employees, rates of offered services, and the support provided by other departments of iFinance. The total budget cost for CSIRT includes five hundred thousand dollars. This budget includes both long-term and short-term cost. The short term cost includes the cost of infrastructure, equipment, and staff while the long term cost keeps on growing with the passage of time. It also includes base funding for supporting the initial activities and services. Some basic costs may also include incident tracking and reporting system, mechanism of communication which include helpdesk, mailing lists of distribution, pagers, and cell phones. Some cost of the security mechanism of communications includes extranets or intranets (Reyes- Mena, et, al., 2018).

The average cost of several incidents and attack include more than one hundred dollars. The compromise attack will cost more than five thousand dollars, the harmful code will cost three thousand dollars, denial of service will cost more than thirty thousand dollars, hacker attacks will cost more than ten thousand dollars, and violations of copyright cost thousand dollars. The estimated established ROI shows that this CSIRT can save more than one hundred thousand dollars per month. By fulling, the cost required for these attacks CSIRT will reduce the rate of incidents to large extent. Depending on the resources which are provided from its constituency and key stakeholders. CSIRT for iFinance requires almost twenty-four months for becoming fully operational. The timeline can be compressed or extended that depends on several factors Organization Model of Internal Centralized CSIRT will be used which is considered to be completely staffed and dedicated which provides the services of incident handling for any organization. In this case, team members will spend a hundred percent of their time in order to work for this CSIRT while such model type can also be provided utilizing the staff of part-time on the basis of rotation. This model can easily help the team to manage both the internal and external employees required for CSIRT. This CSIRT is expected to the reduced response time of the incident by more than fifty percent.

References

Mohd, N., Yunos, Z., Ariffin, A., Nor, A., & Malaysia, C. (2016, September). CSIRT Management Workflow: Practical Guide for Critical Infrastructure Organizations. In *Proceedings of the 10th European Conference on Information Systems Management, ECISM*.

Pfleeger, S. L. (2017). *Improving Cybersecurity Incident Response Team (CSIRT) Skills, Dynamics and Effectiveness*. Trustees of Dartmouth College Hanover United States.

Valladares, P., Fuertes, W., Tapia, F., Toulkeridis, T., & Pérez, E. (2017, July). Dimensional data model for early alerts of malicious activities in a CSIRT. In *2017 International Symposium on Performance Evaluation of Computer and Telecommunication Systems (SPECTS)* (pp. 1-8). IEEE.

Mejía, J., Muñoz, M., Ramírez, H., & Peña, A. (2016). Proposal of content and security controls for a CSIRT website. In *New Advances in Information Systems and Technologies*(pp. 421-430). Springer, Cham.

Mena, F. X. R., Díaz, W. M. F., Jaramillo, C. E. G., Estévez, E. P., Barzallo, P. F. B., & Silva, C. J. V. (2018). Application of business intelligence for analyzing vulnerabilities to increase the security level in an academic CSIRT. *Facultad de Ingeniería*, *27*(47), 2.

Fuertes, W., Reyes, F., Valladares, P., Tapia, F., Toulkeridis, T., & Pérez, E. (2017). An Integral Model to Provide Reactive and Proactive Services in an Academic CSIRT Based on Business Intelligence. *Systems*, *5*(4), 52.

Reyes, F., Fuertes, W., Tapia, F., Toulkeridis, T., Aules, H., & Pérez, E. (2018, July). A BI Solution to Identify Vulnerabilities and Detect Real-Time Cyber-Attacks for an Academic CSIRT. In *Science and Information Conference* (pp. 1135-1153). Springer, Cham.

Skierka, I., Morgus, R., Hohmann, M., & Maurer, T. (2015). CSIRT Basics for Policy-Makers. *The History, Types & Culture of Computer Security Incident Response Teams*.

Lord, J., Rush, K., & Massa, M. (2018). *Security Operations Overview*. Carnegie Mellon University the Pittsburgh United States.

Reyes-Mena, F. X., Fuertes-Díaz, W. M., Guzmán-Jaramillo, C. E., Pérez-Estévez, E., Bernal-Barzallo, P. F., & Villacís-Silva, C. J. (2018). Application of business intelligence for analyzing vulnerabilities to increase the security level in an academic CSIRT. *Facultad de Ingeniería*, *27*(47), 21-29.