Today, organisations must be able to respond to computer security incidents effectively in order to minimize the damage and to protect their asset. Computer Security Incident Response Plans should help organisations to respond to security related incidents in an effective manner. The design of an IRP is characteristic for any organisation and must be developed individually. This paper suggests a universal strategy to create an effective Computer Security Incident Response Plan (CSIRP) and constitutes general steps, design considerations, processes and procedures based on common project management concepts.

The initial development strategy of an Incident Response Plan can be derived from common project management principles (Schwalbe, 2007). A project is "a temporary endeavour undertaken to create a unique product, service, or result" (Project Management Institute., 2008). However, an IRP is a living document or policy; therefore, it must be regularly reassessed in order to adapt to changes in the organisation, technology and people. In summary, the strategy to build an IRP is based on common project management phases.

Stakeholder and participants are identified during the concept phase. During the initial phase, management must create a business case describing the benefits of the Incident Response Plan to the organization (Schwalbe, 2007). Also, it is crucial to identify the constituency which is serviced or supported ("CERT®/CC: Action List for Developing a Computer Security Incident Response Team (CSIRT)," n.d.). In the same token, it is important that management can see the value an IRP can bring to the organization. Moreover, project scope, time and cost must be well defined to facilitate the entire process (Schwalbe, 2007). Stakeholders and their functions must be identified during the concept phase in order to understand where specific activities are performed and how the implementation of an IRP will affect current and future business processes. Typically, stakeholders should include personnel from upper management, Human Resource, Information Technology, Information Security, Procurement and external contacts which are involved or affected directly or indirectly (Schwalbe, 2007). Ideally, an IRP should correspond to an Organization's Information Security Policies, guidelines and procedures ("building-incident-response-program-suit-business_627," n.d.).

The Incident Response Plan must be supported and approved by upper management ("CERT®/CC: Action List for Developing a Computer Security Incident Response Team (CSIRT)," n.d.). A sponsor and champion should be appointed in order to facilitate, support and communicate the project within the organisation (Schwalbe, 2007). Resources must be assigned and approved for specific tasks during any project phase. Ultimately, the success or failure of a project is based on the support and credo of upper management.

At this point stakeholders and management should evaluate different Computer Security Incident Response Team (CSIRT) models and structures based on their organizational size, structures, resources and needs. Central or Internal Incident Response Teams provide services to their constituency and are managed by their parent organization ("CERT®/CC: Computer Security Incident Response Team FAQ," n.d.). In addition, external or national CSIRT provide incident handling services to a country ("CERT®/CC: Computer Security Incident Response Team FAQ," n.d.). Finally, Coordinating Centers coordinate and manage incident response operations of different CSIRT ("CERT®/CC: Computer Security Incident Response Team FAQ," n.d.). Analysis Centers collect and synthesise reported incident data from various CSIRT to determine future trends and threads along with counter measures and mitigation recommendations ("CERT®/CC: Computer Security Incident Response Team FAQ," n.d.). Typically, Analysis Centers disseminated advisories across the enterprise so organizations can proactively implement necessary steps to mitigate the risks as part of their defense in depth strategy. Furthermore, vendor Teams analyze vulnerabilities and develop patches and mitigation strategies for their hardware and software products.("CERT®/CC: Computer Security Incident Response Team FAQ," n.d.). Finally, Incident Response Providers are professional teams which provide commercial services to customers.

The development of a CSIRT in an organization mainly depends on the business requirements. Therefore, organizations should first formulate a tentative CSIRT mission statement which

defines specific services the team provides to the constituency. Then, the organization should decide if it has the expertise to provide these services with their own employees and the state of the employee morale. Specifically, how do employees adapt to new tasks and how is the learning motivation in general? What incentives does the organization provide to maintain and facilitate the employee moral?
The mission statement should also define the operating hours of the CSIRT, specifically, must the CSIRT be available 24/7 and how must the organisation respond to incidents after working hours or on the weekends? Finally, what is the cost factor to run any type of the aforementioned CSIRT within the own organisation. A cost-benefit analyses will help to determine the best approach from an economically standpoint.
The CSIRT structure is derived from the results of the cost-benefit analysis and from the organisation's business philosophy. Fundamentally, organisations can provide the service internally or externally; also, a hybrid structure can be a compromise in certain scenarios to divide the responsibilities. Outsourcing has many advantages but also potential trade-offs. For instance, sensitive information must be revealed to the contractor which might contradict with the implemented security policy ("CERT®/CC: Action List for Developing a Computer Security Incident Response Team (CSIRT)," n.d.). However, contractors might have better and more professional resources and technical expertise than in house staff. Also, in house staff must be educated continuously in Incident Response related areas; in contrary, contractors might lack the necessary organization-specific knowledge. Also, hybrid models can result in an inefficient collaboration between the two entities caused by the lack of correlation and division of responsibilities.
After, the CSRIT model and structure is defined in the mission statement funding must be approved ("CERT®/CC: Action List for Developing a Computer Security Incident Response Team (CSIRT)," n.d.). This includes short-term and long-term operations as well. Facilities, training, equipment, tools, hardware and software for detecting and analyzing, tracking etc. must be taken into consideration ("CERT®/CC: Action List for Developing a Computer Security Incident Response Team (CSIRT)," n.d.).
Next, the CSRT services must be defined in detail ("CERT®/CC: Action List for Developing a Computer Security Incident Response Team (CSIRT)," n.d.). This includes which services are offered to which segment of the constituency and the process for delivery of the services. For instance, contact methods, operating hours, dissemination methods are all part of the delivery process.
The CSRT must fit into the organizational structure. The primary goal is that CSRIT can effectively fulfil its mission. Therefore, the level of authority must be transparent to other departments within the organizational structure ("CERT®/CC: Action List for Developing a Computer Security Incident Response Team (CSIRT)," n.d.). Finally, organizational structure changes must be communicated to all stakeholders and employees within the organization. Resources, staff and equipment must be assigned to CSIRT.
The CSIRT infrastructure should be secured and monitored. This includes data and physical premises as well. In addition, Processes for collecting, recording, tracking and archiving information must be defined ("CERT®/CC: Action List for Developing a Computer Security Incident Response Team (CSIRT)," n.d.). Also, job descriptions outlining required skills can be created in cooperation with Human Resource. Likewise, requirements for background checks and security clearance should be manifested. Full time and part-time CSIRT members must be updated regularly on new technology and trends; therefore, a training and mentoring strategy is crucial for the effectiveness of a team ("CERT®/CC: Action List for Developing a Computer Security Incident Response Team (CSIRT)," n.d.). Specific function and roles must be assigned to all team members. Also, overlapping and external interfaces collaborating with the CSIRT must be identified ("CERT®/CC: Action List for Developing a Computer Security Incident Response Team (CSIRT)," n.d.).

Essentially, the responsibilities of the CSIRT member and its collaborating entities must be accurately defined ("building-incident-response-program-suit-business_627," n.d.). For instance, CSIRT should define and classify incidents, determine the necessary tools and methods, determine the basis to conduct an investigation, securing the network, conducting follow up reviews, and promote awareness throughout the organization ("building-incident-response-program-suit-business_627," n.d.).

The workflow or life cycle of an Incident Response Plan can be derived from the components of an Incident Response Program. It includes preparation, reporting, discovering, responding, investigation, recovery and follow-up of an incident ("building-incident-response-program-suit-business_627," n.d.).

Incident Detection and incident analysis are based on the aspects of reporting and discovering. Organizations must monitor vulnerability advisories on a regular basis. In return, IRT can raise awareness about potential vulnerabilities and inform about proper behaviour within the organization. For instance, the Information Technology department can take actions to patch and update the systems. Organizations can monitor the release of vendor specific updates and advisories in the internet. Consequently, CSIRT should develop procedures to monitor, disseminate and document advisories and follow-on measures.

Moreover, Information System log files should be monitored in order to discover incidents. Different methods, tools and technologies are available for automated monitoring. Scripts can be developed to synthesize log files effectively. Also, Intrusion Detection Systems and Intrusion Prevention Systems, Firewalls and content filtering software or appliances are used to detect, analyze, correlate and classify potential intrusions ("defenseindepth.pdf," n.d.).

CIRT member should be automatically notified about incidents via pager, phone, email or SMS ("SANS: building-incident-response-program-suit-business_627," n.d.). Organizations should track their incidents in a database in order to determine incident trends, attack methods and system vulnerabilities. Based on this information CSIRT and InfoSec members can quickly adapt to future attacks by improving its security mechanisms and policies ("SANS: building-incident-response-program-suit-business_627," n.d.).

Organisations should develop risk rating metrics to classify security incidents. Incident classification helps to identify and initiate proper response actions. Typically, incident are classified as high/medium/ and low risks ("SANS: building-incident-response-program-suit-business_627," n.d.). High risks incidents are active or passive attacks that have a monumental impact on data confidentiality, data integrity and availability ("SANS: building-incident-response-program-suit-business_627," n.d.). Medium risks are significant or have the potential to have a monumental impact on Information Systems; low risks have the potential to become significant or monumental ("SANS: building-incident-response-program-suit-business_627," n.d.).

Organizations must define procedures when an incident has been reported to CIRT. First, CIRT members must verify and classify incidents based on checklists containing indications for malicious activities. Once an incident has been verified the incident must be reported and contained in order to prevent further Information System compromise ("SANS: building-incident-response-program-suit-business_627," n.d.). Next, Information Systems must be eradicated from malicious activities to restore readiness for operation and service. Depending on the level of intrusion further investigation may be performed by computer forensic experts ("SANS: building-incident-response-program-suit-business_627," n.d.). Organizations should follow up on the incident in order to avoid recurrence of the same or similar incident. Hence, stakeholders and CSIRT members should set up a meeting in order to progress the IRP.

In summary, the development of an IRP is characteristic for any organization. Common project management principles can be applied to facilitate the development. The project must be supported and sponsored by upper management. Different IRT models and structures are available and the creation depends heavily on the business philosophy. Specific protocols must be implemented for effective response. Personnel and especially CIRT members must be trained

and updated regularly on technologies, threads and policy changes. It is imperative that organization learn from past incidents to avoid recurrence.

References:

building-incident-response-program-suit-business_627. (n.d.). Retrieved from http://www.sans.org/reading_room/whitepapers/incident/building-incident-response-program-suit-business_627

CERT®/CC: Action List for Developing a Computer Security Incident Response Team (CSIRT). (n.d.). Retrieved from http://www.cert.org/csirts/action_list.html

CERT®/CC: Computer Security Incident Response Team FAQ. (n.d.). Retrieved from http://www.cert.org/csirts/csirt_faq.html#4

defenseindepth.pdf. (n.d.). Retrieved from http://www.nsa.gov/ia/_files/support/defenseindepth.pdf

Project Management Institute. (2008). *A guide to the project management body of knowledge (PMBOK Guide) an American national Standard ANSI PMI 99-001-2008* (4th ed.). Newton Square Pa: Project Management Inst.

SANS: building-incident-response-program-suit-business_627. (n.d.). Retrieved September 16, 2011, from http://www.sans.org/reading_room/whitepapers/incident/building-incident-response-program-suit-business_627

Schwalbe, K. (2007). *Information technology project management* (5th ed.). Boston Mass.: Course Technology Cengage Learning.