INSTITUTO POLITÉCNICO NACIONAL
ESCUELA SUPERIOR DE CÓMPUTO
ESCOM

Thursday First of June of 2017

“Incident Handling Scenario 1”

Present

Gabriela Saldaña Aguilar

Profesor

Jessie Paulina Guzmán Flores

Table of Contents

Chapter 1. THEORETICAL FRAMEWORK

Chapter 2. Incident Scenario

Chapter 3. Conclusion

CHAPTER 1

THEORICAL FRAMEWORK

1.1 Security Governance Background

Organizations today face a global revolution in governance that directly affects their information management practices. There is an increased need to focus on the overall value of information protected and delivered (in terms of enabled services). It is estimated that in less than a decade, organizations will typically deal with 30 times more information than they do today. Due to the high-profile organizational failures of the past decade, legislatures, statutory authorities and regulators have created a complex array of new laws and regulations designed to force improvement in organizational governance, security, controls and transparency[2].

The focus of security had been on protecting the IT systems that process and store the vast majority of information, rather than on the information itself. An enlightened approach to information security takes the larger view that an organization's information and the knowledge based on it must be adequately protected regardless how it is handled, processed, transported or stored. It addresses the universe of risks, benefits and processes involved with all information resources.

In order to accomplish a better way to handle information security a bunch of best practices and handling books where maid about [2]:

1. Understanding the criticality of information and information security to the organization.
2. Reviewing investment in information security for alignment with the organization strategy and risk profile .
3. Endorsing the development and implementation of a comprehensive information security program.
4. Requiring regular reports from management on the program's adequacy and effectiveness.

1.2 Incident handling (NIST)

No matter the extent of our defenses, it inevitable that Information Security Incidents will occur. For this reason establishing, periodically assessing, and continually improving incident management processes and capabilities is very important.

The goal of an effective information security incident management strategy is a balance of driving the impact of the incidents down, while processing incidents as efficiently as possible. Good incident management will also help with the prevention of future incidents.

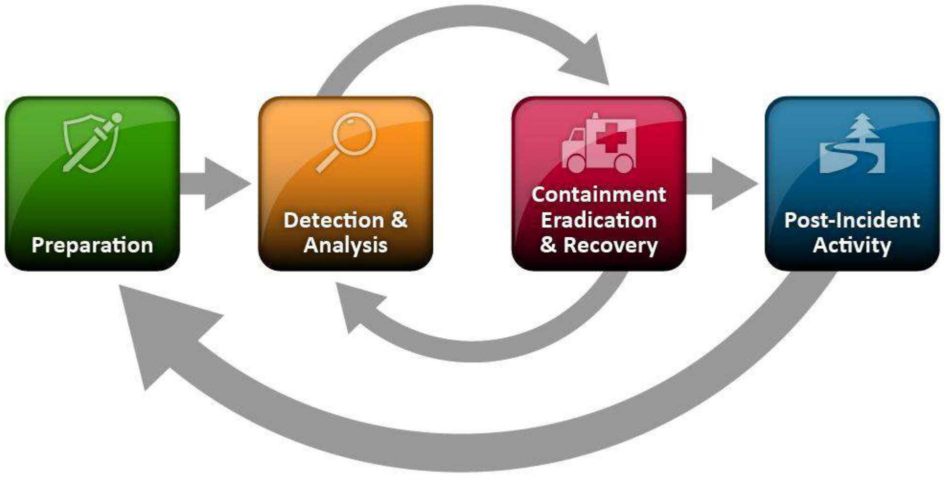
From a management perspective, it involves identification of resources needed for incident handling, as well as developing and communicating the formal detection and reporting processes. An effective security program includes important aspects of detecting, reporting, and responding to adverse security events as well as weaknesses which may lead to events, if they are not appropriately addressed. The primary elements of incident management are:

- Preparation, Detection, and Reporting
- Security Incident Response and Process Improvement

Effective incident response in many organizations other than IT, involve having trained personnel equipped and ready for response. Effective, appropriate communication at all levels of an organization is essential for limiting the impact of security events, using formal detection and reporting processes. In addition, technical controls must be implemented for the automated detection of security events, coupled with as near real-time reporting as possible, to investigate and initiate immediate responses to problems. For new IT systems, often the best time to develop automated detection of security events is when the preventive security controls are being architected.

A formal management procedure and policy for incident response, including roles and responsibilities for each aspect of the response is essential. Aspects include funding and cost models, analysis, containment and recovery responsibilities, decision making authority for notifications; legal and/or law enforcement involvement; forensic investigations; responsibility for after-incident debriefing; and policy, procedure, and process improvements.

NIST, in their 800-61 Computer Security Incident Handling Guide, describes the "Incident Lifecycle" as [1]:



Preparation

Involves identification of resources needed for incident handling and having trained individuals ready to respond, and by developing and communicating a formal detection and reporting process. Effective, appropriate communication at all levels of an organization is essential for limiting the impact of security events. NIST suggests the following policy components:

- Statement of management commitment
- Purpose and objectives of the policy
- Scope of the policy (to whom and what it applies and under what circumstances)
- Definition of computer security incidents and their consequences within the context of the organization
- Organizational structure and delineation of roles, responsibilities, and levels of authority (should include the authority of the incident response team to confiscate or disconnect equipment, to monitor suspicious activity, and the requirements for reporting certain types of incidents)
- Prioritization or severity ratings of incidents
- Performance measures
- Reporting and contact resources

Detection and Reporting

Designing an effective means of the detection of incidents is also essential, using both trained users and trained system administrators, and various technical controls. All members of the community should be trained and comfortable regarding

- procedures for reporting failures, weaknesses, and suspected incidents
- methods to recognize and detect problems with security protections
- how to escalate reporting appropriately

Reporting Information Security Weaknesses

An effective approach is to use analysis tools to help manage intrusion detection systems and summarize the data. Even when log summarization is used, maintaining and monitoring intrusion detection systems can require resources and technical skill that are beyond some institutions' means.

Incident Analysis and Forensics

In many cases, a more in-depth evaluation of the incident and circumstances is warranted. It may be to determine if confidential information was involved in, or stored on, the system in question. It may also to be an effort to determine the vulnerability or action that enabled the incident to occur. This is typically where a forensic evaluation comes into play.

The general activities, or stages to an effective response and improvement are described in the table below. Some may of necessity be serially processed and some may run as concurrent activities.

Stages:	**Activities:**
Identification and prioritization of incident, and performing a timely assessment of the situation	Determine the scope/impact. The number of users affected, or number of devices, or segments of the network should be considered. Is a single user or account involved?
	Assess the severity. What is the sensitivity of data involved? What is the criticality of the service, or system, or application? What is the potential for damage or liability? Is there potential for harm?
	Assess the urgency of the event. Is it an active problem, threat, or event-in-progress? Was the problem discovered after the fact? Is the intrusion "dormant", or completed? Does this involve use of an account rather than a system? Is this involve the safety or privacy of individuals?
Containment of the event	Does the system need to be removed from the network? Does active memory need to be imaged or captured?
	Are there user accounts or system-level accounts that need to be disabled or changed? Are there sessions that need to be dropped?
Investigation of what occurred and how (includes "root cause" analysis)	An incident tracking record needs to be created. If deemed necessary, due to the scope, seriousness, or complexity of the incident, an incident notes log should also be created.
	Gathering and preserving relevant information should be conducted by trained security personnel.
	Evaluation of evidence commences. It may be a "forensic" caliber assessment, or a less comprehensive analysis, depending on the type of incident and your institution's policies. Decisions with respect to the appropriate resolution and response

	should be discussed with decision makers and key stakeholders.
Response (effect)	Eradication of the problem, and associated changes to the system need to be applied. This includes technical actions such as operating system and application software installs, new or changed firewall rules, custom configurations applied, databases created, backup data restored, accounts created and access controls applied
	Recovery to a fully operational state always follows appropriate testing or assurance of the system integrity and stability. Effective customer service includes regular communications with stakeholders who may be anxious for recovery.
	Outcomes, including possible sanctions should be determined. Sanctions, if they are deemed appropriate to the response, may be internal, such as disciplinary action, or they may be external, such as referral to law enforcement.
Follow up (Improvements)	After incident debriefing. Its important to review the process and how it could have been better, after an incident is closed. This is especially valid for new types of incidents, and particularly severe or costly incidents.
	Consider policy and process changes. Were any procedures missing, communications unclear, or stakeholders that were not appropriately considered? Did the technical staff have appropriate resources (information as well as equipment) to perform the analysis and/or the recovery?
	Consider controls improvements, leading to prevention. What can we do to ensure this does not happen again? What improvements can we implement to make our response and recovery more timely?

1.3 Risk management

Risk is part of all our lives. As a society, we need to take risks to grow and develop. From energy to infrastructure, supply chains to airport security, hospitals to housing, effectively managed risks help societies achieve. In our fast paced world, the risks we have to manage evolve quickly. We need to make sure we manage risks so that we minimize their threats and maximize their potential.

Risk management involves understanding, analyzing and addressing risk to make sure organizations achieve their objectives. So it must be proportionate to the complexity and type of organization involved. Enterprise risk management (ERM) is an integrated and joined up approach to managing risk across an organization and its extended networks.

A number of standards have been developed worldwide to help organizations implement risk management systematically and effectively. These standards seek to establish a common view on frameworks, processes and practice, and are generally set by recognized international standards bodies or by industry groups. Risk management is a fast-moving discipline and standards are regularly supplemented and updated.

The different standards reflect the different motivations and technical focus of their developers, and are appropriate for different organizations and situations. Standards are normally voluntary, although adherence to a standard may be required by regulators or by contract.

Commonly used standards include:

- ISO 31000 2009 – Risk Management Principles and Guidelines
- A Risk Management Standard – IRM/Alarm/AIRMIC 2002 – developed in 2002 by the UK's 3 main risk organizations.
- ISO/IEC 31010:2009 - Risk Management - Risk Assessment Techniques
- COSO 2004 - Enterprise Risk Management - Integrated Framework
- OCEG "Red Book" 2.0: 2009 - a Governance, Risk and Compliance Capability Model

Risk analysis is often best done in a group with each member of the group having a good understanding of the objectives being considered.

1. **Identify the Risks**: What might inhibit the ability to meet objectives? E.g. loss of a key team member; prolonged IT network outage; delayed provision of important information by another work unit/individual; failure to seize a commercial opportunity, etc. Consider also things that might enhance the ability to meet objectives e.g. a fund-raising commercial opportunity.

2. **Identify the Causes**: What might cause these things to occur e.g. the key team member might be disillusioned with their position, might be head hunted to go elsewhere; the person upon whom you are relying for information might be very busy, going on leave or notoriously slow in supplying such data; the supervisor required to approve the commercial undertaking might be risk averse and need extra convincing before taking the risk, etc.
3. **Identify the Controls**: Identify all the things (Controls) that you have in place that are aimed at reducing the Likelihood of your risks from happening in the first place and, if they do happen, what you have in place to reduce their impact (Consequence). Examples include: providing a friendly work environment for your team; multi-skilling across the team to reduce the reliance on one person; stressing the need for the required information to be supplied in a timely manner; sending a reminder before the deadline; and provide additional information to the supervisor before he/she asks for it, etc.
4. **Establish your Likelihood and Consequence Descriptors**: The likelihood descriptors are fairly generic however the consequence descriptors may depend upon the context of your analysis. I.e. if your analysis relates to your work unit, any financial loss or loss of a key staff member (for example) will have a greater impact on that work unit than it will have on the University as a whole so those descriptors used for the whole-of-University (strategic) context will generally not be appropriate for the Faculty, other work unit or the individual. The idea is analogous to how a loss of $300,000 would have less impact on the University than it would for an individual work unit.You will need to establish these parameters in consultation with the head of the work unit.
5. **Establish your Risk Rating Descriptors**: I.e. what is meant by a Low, Moderate, High or Extreme Risk needs to be decided upon from the outset.
6. **Add Controls**: Generally, any risk rated High or Extreme should have additional controls applied to it to reduce the rating to an acceptable level. What the additional controls might be, whether they are affordable, what priority might be placed on them etc is something for the group to determine in consultation with the Head of the work unit.
7. **Make a Decision**: Once the above process is complete, if there are still some risks that are rated as High or Extreme, a decision has to be made as to whether the activity will go ahead. Sometimes risks are higher than preferred but there may be nothing more that can be done to mitigate the risk i.e. they are out of the control of

the work unit but the activity must still be carried out. In such situations, monitoring and regular review is essential.

8. **Monitor and Review**: Monitoring of all risks and regular review of the risk profile is a key part of effective risk management.

1.4 Information Security Frameworks

Any organization you work for is going to rely on one or more of these frameworks and standards, whether voluntarily or forced via regulation.

Controls outlined in these standards give you a good idea of both what you'll be expected to do and how you'll be expected to do it.

If you want to get a head start on understanding the expectations of these frameworks and standards, check out the following resources:

- ISO 27000-series
- NIST 800-30: Risk Management
- NIST 800-53: Federal Information Systems Management Act (FISMA)
- Health Insurance Portability and Accountability Act (HIPAA)
- Payment Card Industry Data Security Standard (PCI DSS)
- Sarbanes-Oxley (SOX)
  - Focus on Section 404 – Management Assessment of Internal Controls
- Gramm-Leach-Bliley Act (GLBA)

If you want to dig deeper, check out the following resources:

- COBIT 5: Control Objectives for Information and Related Technology
- ITIL Security Management
- Federal Energy Regulatory Commission: NERC Reliability Standards
- Children's Online Privacy Protection Act (COPPA)

1.5 CSIRT

In the initial phase, the new CSIRT(Computer Emergency Response Team) is organized as an internal CSIRT that provides Services to the company to which it belongs, the local IT department and its personnel. It also supports and coordinates among the different branches the treatment of Incidents related to IT security [4]. The term CSIRT is usually used in Europe instead of the CERT protected term, registered in the USA. By the CERT Coordination Center (CERT / CC).

FIRST is the most important CSIRT organization and is a recognized global leader in Response to incidents. FIRST Incident Response Teams Can give security incidents a more effective response, both reactive and Proactive.

Advantages are:

- Provide centralized coordination for IT security within the organization (contact point).
- React to and deal with IT-related incidents in a manner Centralized and specialized.
- To have at hand the necessary technical knowledge to support and Assist users who need to quickly recover from security.
- Address legal issues and protect evidence in the event of a lawsuit.
- Monitor progress in the area of security.
- Encourage cooperation in IT security among group customers (Sensitization).

Services offered by a CSIRT:

Reactive services	**Proactive Services**	**Management of instances**	**Quality management of the security**
• Alerts and warnings • Treatment of Incidents • Analysis of incidents • Support for response to Incidents • Coordination of Incident response • Response to incidents • Treatment of vulnerability • Analysis of the vulnerability • Response to vulnerability • Coordination of Response to vulnerability	• Press releases • Observatory of technology • Evaluations or Audits of the security • Configuration and Maintenance of security • Development of tools of security • Detection services of intruders • Dissemination of information Related to security	• Analysis of instances • Response to the instances • Coordination of the response to the instances	• Risk analysis • Business continuity and Recovery after a disaster • Security consulting • Awareness raising • Education / Training • Evaluation or certification of products

CSIRTs use various channels of communication. The following have Proved their practical usefulness, so it is worth taking them into consideration:

• Public web site; • Zone reserved for members on the website; • Web forms to report incidents; • Mailing lists; • Personalized email; • Telephone / fax; • SMS; • "old-fashioned" traditional paper-based charts; • Monthly or annual reports

The proper organizational structure of a CSIRT depends greatly on the
Structure of the organization to which it belongs and of the group of clients served.
One common organizational structure is the following:

General

- General Director

Personal

- Director of the office
- Accountant
- Communications Adviser
- Legal Adviser

Technical operating team

- Head of the technical team
- CSIRT technicians, responsible for the provision of services
- Researchers

Technical competences

- Extensive knowledge of Internet technology and protocols.
- Knowledge of Linux and Unix systems (depending on the team of the group of Customers attended).
- Knowledge of Windows systems (depending on the equipment of the group of Customers attended).
- Knowledge of network infrastructure equipment (router, switches, DNS, Proxy, mail, etc.).
- Knowledge of Internet applications (SMTP, HTTP (s), FTP, telnet, SSH, etc.).
- Knowledge of security threats (DDoS, phishing, defacing, sniffing, etc.).
- Knowledge of risk assessment and practical implementations.

Other features

- Willingness to work 24 hours a day, 7 days a week or on duty (according to which Be the service model).
- Maximum travel distance (in case of emergency, availability at the office; Maximum travel time).
- Educational level.

- Work experience in the field of IT security.

External Consultants

- Hired when needed

For a complete service during office hours and maintenance services:
Minimum of 6 to 8 full-time or equivalent workers.

Since CSIRTs often handle very sensitive information, it is good practice
Let the team take control of the physical security of the office.

General rules concerning the building

- Use access controls.
- Restrict access to the CSIRT office, as a minimum, to CSIRT staff.
- Check offices and entrances with cameras.
- File confidential information under lock and key or in a safe.
- Use secure IT systems.

General rules regarding IT equipment

- Use equipment to which staff are able to provide support.
- Protect all systems.
- Correct and update all systems before connecting them to the Internet.
- Use security software (firewalls, multiple antivirus, antispyware programs, etc.).

Maintenance of communication channels

- Public website.
- Access restricted to members on the website.
- Web forms to report incidents.
- Email (which supports PGP / GPG / S / MIME).
- Mailing list software.
- Have a telephone number reserved for the customer group served:

- Phone,
- Fax,
- SMS

Record Locator System (s)

- Contact database with information about team members, others Equipment, etc.
- CRM tools.
- Incident treatment guards system.
- Standard e-mail design and standard notice bulletin.
- "Outdated" letters on paper.
- Monthly or annual reports.
- Incident information form.

The first step is to become aware of the IT systems that have installed the Group attended. In this way, the CSIRT will be able to assess the relevance of the information That it arrives and filter it before distributing it again, so that the group is not seen Overwhelmed with information that turns out to be of little use.

Category	Aplication	Software	Version	OS	OS Version	Attended Group
Personal computer	Office	Excel	x-x-x	Microsoft	XP-prof	A
Personal computer	Browser	Internet Explorer	x-x-	Microsoft	XP-prof	A
Network	Router	CISCO	x-x-x	CISCO	x-x-x-	B
Server	Server	Linux	x-x-x	L-distro	x-x-x	B
Services	Web server	Apache	Unix	x-x-x	B	

The generation of alerts, warnings and announcements is always the same scheme:

- Collection of information;
- Assessment of information on relevance and source;
- Risk assessment based on the information collected;
- Distribution of information

There are usually two important types of sources of information that contribute Information to the services:

- Information of the vulnerability of (own) IT systems;
- Incident reports

Some of the most important factors to consider are:

- Is the vulnerability well known?
- Is it widespread?
- Is it easy to exploit?
- Is it a vulnerability that can be exploited remotely?

All these questions help to form an adequate picture of the seriousness of the vulnerability.

To calculate the risk you can use a very simple formula:
Impact = risk X potential damages (Potential-Medium-Low)
Potential damages can be :

- Unauthorized access to data;
- Denial of service (DOS);
- Obtaining or extending permits.

Each CSIRT can choose between different distribution methods, according to the Preferences of the customer group served and its own communication strategy:

- Website;
- Email;
- Reports;
- Archiving and research.

A vulnerability report should consider the following[4]:

Title ………………………………………………………………………………………
Reference number …………………………… Affected Systems - …………………………… - …………………………… OS version and related information …………………………… Calculated Risk(Potential-Medium-Low) ……… Consequences / Potencial damages (Potential-Medium-Low) ……… External IDs: (vulnerabilitie's IDs, acces IDs) …………
Vulnerability description …………………………………………………………… Consequences …………………………………………………………… Solution …………………………………………………………… Description of the solution ……………………………………………………………

INCIDENTS TRATMENT

STEP 1 Receiving incident reports

As already mentioned, the incident reports arrive at the CSIRT by different channels, especially by email, but also by phone or fax. It should be emphasized that it is good practice to write down all the details in a format while receiving the incident notice, to ensure that there is no forgotten information [4].

INCIDENT COMMUNICATION FORM

Please complete this form and send it by fax or email to: ....
Lines marked with an asterisk (*****) are mandatory.

Name and organization
1. Name *:
2. Name of organization *:
3. Sector:
4. Country *:
5. City:
6. Email address *:
7. Phone number *:
8. Others:

Affected computer (s)
9. Number of computers:
10. Computer Name and IP *:
11. Function of the computer *:
12. Time zone:
13. Hardware:
14. Operating System:
15. Software Affected:
16. Files affected:
17. Security:
18. Computer Name and IP:
19. Protocol / port:

Incident
20. Reference number:
21. Type of incident:
22. Inception of the Incident:
23. The incident has yet been resolved: Yes NO
24. Time and method of discovery:
25. Known Vulnerabilities:
26. Suspicious files:
27. Measures:
28. Detailed description *:

Step 2: Assessing the Incident
In order to evaluate the incident there are some categories to take into account:

Identification:

In order to avoid unnecessary actions, it is important to check that the creator of the report is reliable and belongs to the group of clients served by an associated CSIRT.

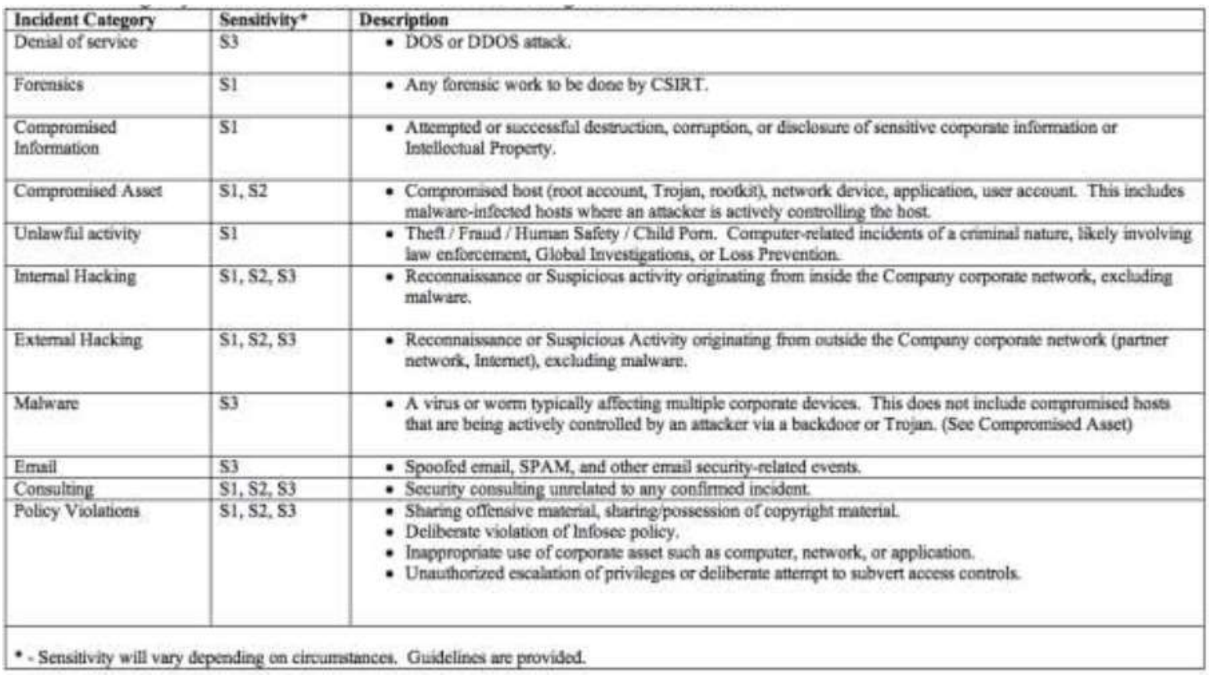
Relevance:

This step checks whether the incident handling request comes from the client group served by the CSIRT, or if the reported incident affects IT systems of the group being served. If this is not the case, the communication is usually sent to the relevant CSIRT.

Classification:

In this step the incident it's classified according to its gravity.

Incident classification system [6]:



Incident Category	Sensitivity*	Description
Denial of service	S3	• DOS or DDOS attack.
Forensics	S1	• Any forensic work to be done by CSIRT.
Compromised Information	S1	• Attempted or successful destruction, corruption, or disclosure of sensitive corporate information or Intellectual Property.
Compromised Asset	S1, S2	• Compromised host (root account, Trojan, rootkit), network device, application, user account. This includes malware-infected hosts where an attacker is actively controlling the host.
Unlawful activity	S1	• Theft / Fraud / Human Safety / Child Porn. Computer-related incidents of a criminal nature, likely involving law enforcement, Global Investigations, or Loss Prevention.
Internal Hacking	S1, S2, S3	• Reconnaissance or Suspicious activity originating from inside the Company corporate network, excluding malware.
External Hacking	S1, S2, S3	• Reconnaissance or Suspicious Activity originating from outside the Company corporate network (partner network, Internet), excluding malware.
Malware	S3	• A virus or worm typically affecting multiple corporate devices. This does not include compromised hosts that are being actively controlled by an attacker via a backdoor or Trojan. (See Compromised Asset)
Email	S3	• Spoofed email, SPAM, and other email security-related events.
Consulting	S1, S2, S3	• Security consulting unrelated to any confirmed incident.
Policy Violations	S1, S2, S3	• Sharing offensive material, sharing/possession of copyright material. • Deliberate violation of Infosec policy. • Inappropriate use of corporate asset such as computer, network, or application. • Unauthorized escalation of privileges or deliberate attempt to subvert access controls.
* - Sensitivity will vary depending on circumstances. Guidelines are provided.		

Step 3: Actions

Incident protection

The incident slip number should already have been generated in a previous step. If not, the first step will be to create it, for use in subsequent communications about the incident.

Incident life cycle

When dealing with an accident there is a circle of steps that are applied repeatedly until the incident is finally resolved and all the parties involved have all the necessary information. The life cycle contains the following processes:

-Analysis:
All details of the reported incident are analyzed.
-Contact information:
Contact information must be obtained in order to communicate the incident information to all parties involved, like other CSIRTs, the victims and probably the owners of the systems that could have been used to make an attack.
-Technical assistance:
Victims are helped to recover quickly from the results of the incident and more information is gathered on the attack.
-Coordination:
Other stakeholders are informed, such as responsible for the CSIRT of the IT system used for an attack or other casualties.

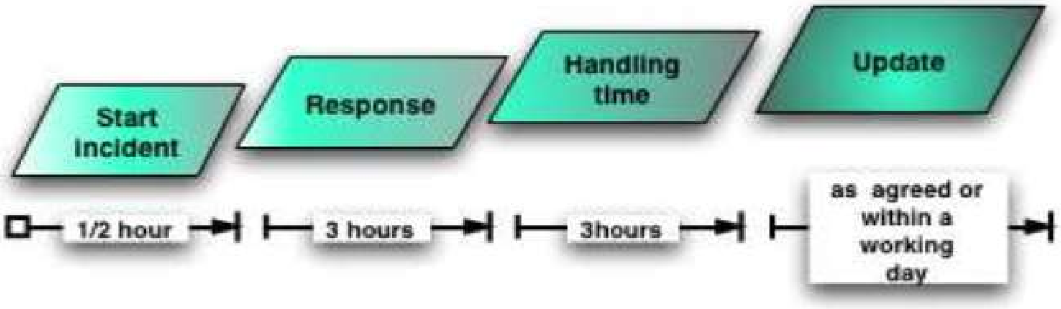
The process ends when all the affected parties have received and communicated all the necessary information.

Incident processing report

Prepare reports to help you respond to management's questions about incidents. It is also good practice to write a document (internal use only) "Lessons Learned", which will help staff to avoid errors in the
treatment of future incidents.

Sample response plan

Here is an example of a practical response plan from the point of view of an incoming assistance request:



It is also good practice to inform the customer group about their own response times, especially when contacting the CSIRT for an emergency.

Available tools for CSIRT

Email and message encryption software

- GNUPG http://www.gnupg.org/

GnuPG is the complete and free software of the GNU project of the openPGP standard, defined in RFC2440. GnuPG allows you to encrypt and sign data and communications.

- PGP http://www.pgp.com/

Commercial variant

Incident Handling Tools

Incident management and tracking, tracking actions.

- RTIR http://www.bestpractical.com/rtir/

RTIR is a free and open source system for the treatment of incidents. Its design meets the needs of CERT and other response teams.

CRM Tools

If the group served needs to locate all the details, a CRM database will be useful. There are different varieties, of which we offer some examples:

- SugarCRM http://www.sugarcrm.com/crm/
- Sugarforce (open source free version) http://www.sugarforge.org/

Verification of information

- Website watcher http://www.aignes.com/index.htm

This program detects updates and changes in websites.

- Watch that page http://www.watchthatpage.com/

The service sends by e-mail information about changes in web pages (free and commercial).

Search for contact information

Searching for the most appropriate contact for incident communication is not an easy task. The following sources of information can be used, for example:

- RIPE [7]
- IRT-object [8]
- TI [9]

CHAPTER 2

INCIDENT SCENARIO

2.1 SCENARIO 1

On a Saturday afternoon, external users start having problems accessing the organization's public websites. Over the next hour, the problem worsens to the point where nearly every access attempt fails. Meanwhile, a member of the organization's networking staff responds to alerts from an Internet border router and determines that the organization's Internet bandwidth is being consumed by an unusually large volume of User Datagram Protocol (UDP) packets to and from both the organization's public DNS servers. Analysis of the traffic shows that the DNS servers are receiving high volumes of requests from a single external IP address. Also, all the DNS requests from that address come from the same source port [1].

INFRMATION SECURITY POLICY

The present is a proposal of the security policies in matter of informatics. The objective is to develop policies that regulate the proper use of these technological skills and recommendations to take an advantage and avoid their misuse, causing problems in the goods and services of the entities.

1. COMPUTER EQUIPMENT

-Of the equipment and installation of it:

All computer equipment that is connected to the Network, or that which is autonomously owned and owned by the institution must be subject to the rules and procedures of installation issued by the Department of Networks.

-Inventory and control over equipment:

The IT Management in coordination with the Property Control department must have a record of all the equipment owned by the company.

-Physical location and security:

Delicate computer equipment dedicated to a specific purpose requires being located in an area that meets the requirements of physical security, environmental conditions, power supply and adequate access level.

-Of responsibilities and reporting:

The physical protection of computer equipment corresponds to those initially assigned to them, and it is the responsibility of the corresponding authorities to notify the movements.

-Of the equipment maintenance:

The Network department is responsible for the preventive and corrective maintenance of the equipment, the maintenance of its installation, the verification of the physical security, and its specific conditioning to take place.

-About the equipment's personal:

It is the responsibility of the Department of Networks to disclose the lists of persons who may have access to the equipment and provide basic maintenance services, except for those serviced by third parties. It is also incumbent upon the establishment of dedicated procedures in case of incidents. Technical personnel in case of incidents most be available 24/7.

2. ACCESS CONTROL

-Establishment of levels access:

According to the level of authority the personal has, the IT area manager will assign a custom access level.

-Connection procedures:

The security department will be responsible for establishing access and connection procedures. A log must be generated to store the activity history that each user generates when making an access request.

-About Knowledge of the regulation:

The Computer Security Directorate is responsible for disseminating the regulations for the use of the network and ensuring compliance.

3. SOFTWARE AND SERVICES

-Of mater of actualization:

All computer equipment (personal computers, workstations, supercomputers and other related), owned by the organization must be kept up to date, tending to conserve and increase the quality of the service it provides.

-About services provided:

All the services that are given must be listed and monitored whenever a request is made, keeping data of: time, date, information accessed, modifications made. Start a stopwatch to measure the time of absence, if it exceeds 5 minutes, the service will be disconnected.

-Web-sites:

Access to web pages through browsers must be subject to the rules that are previously stated in the Regulation of access to the Network. The website should be 24/7 up , the amount of time before it turns into an incident to be reported is 1 minute.

-Software installation and protection:

Software to be installed on critical computer equipment must be authorized by the IT department head, computers must necessarily have malware controls installed and these must be continuously updated.

4. INFORMATION MANAGMENT

-Of recollection and access:

Information about the assets of the company will be collected and an inventory will be made of them, which must be constantly updated. Only those in charge of the inventory and senior personnel as managers can have access.

-Of the classification and labeling:

The information will be labeled in any of its forms: physical or virtual. The information will be classified by:

*Low risk: That in case of being revealed or lost does not cause serious damages, it is recoverable.

*Medium risk: Difficult to recover, causes damages and losses.

*High risk: Not recoverable, generates big losses and damages to the company.

The computer security officers will assign those responsible for guarding this information.

-Backing up:

It is the obligation of all department that handle big amounts of information, to maintain the corresponding support since it is considered as an asset of the institution that must be preserved. The process of backing up information need to be done at least weekly.

5. SYSTEM MAINTENANCE

-Periodic reviews:

The Information Security Department has the authority to carry out the periodic review of access to our information services, and to keep traffic information.

-Monitoring:

Critical systems must be under permanent monitoring.

-Computer equipment maintenance:

The computer will be maintained monthly.

6.BUSINESS CONTINUITY PLAN

-Contingency plans:

Each of the departments must issue the contingency plans that correspond to the critical activities they carry out. These contingency plans should be delivered to the incident response team.

-Sanctions:

Any violation of the security policies and norms must be sanctioned in accordance with the regulation issued by the Directorate of Information Security group.

-Capacity planning:

The capacity of systems and networks must be continuously monitored. Reports will be issued on predictions of their behavior.

-Incidents:

Any description of a computer incident should be kept for further analysis and improvement.

2.2 The following are additional questions for this scenario:

1. Whom should the organization contact regarding the external IP address in question?

R= If we use the NIST reference [1], the organization should contact:

* Public Affairs and Media Relations

* CIO
* Head of information security
* Other incident response teams within the organization
* Systems owners
* Human resources (for cases involving employees, such as harassment through email)
* Legal department (for incidents with potential legal ramifications), in Mexico the official legal department would be the INAI Federal Institute of Access to Public Information so the organization needs a POC for connecting with this institute.

* The management group

* Head of IT and IT support

*Network manager

*POC with law enforcement

*Owner of the external IP address

*External CSIRTs

*Information Assurance

*Business Continuity Planning

2. Suppose that after the initial containment measures were put in place, the network administrators detected that nine internal hosts were also attempting the same unusual requests to the DNS server. How would that affect the handling of this incident?

R=Well lets think that the internal personal have reported this incident to the Information Security manager and they started to detect the origin of the problem, on the way they found nine internal hosts having the same problem, first more personal would be needed, in that way, they have to contact the rest of the team because this could be a cyber-attack, the next thing to do is to alert all parties involved to don't attempt entering the website page because is down temporarily.

3. Suppose that two of the nine internal hosts disconnected from the network before their system owners were identified. How would the system owners be identified?

R= The organization needs to prevent this cases for that reason there should be an emergency distributed user catalog that stores information related to personal information of the user, ownerships, level of access, information that the user can access and more.
This catalog needs to be protected by the Information Security officer and should be available in dedicated situations such as System recoveries. Having an emergency catalog separated of the main application would give the organization a contingency plan in case of have lost system's administrator information.

2.3 PREPARATION

This questions cover the main specs for starting an investigation due to the incident.

1.-Would the organization consider this activity to be an incident? If so, which of the organization's policies does this activity violate?

R= Yes, the organization should consider this as an incident of security.

First we need to define the Incident Response Policy, once we have done it we need to review the document in order to find what is violated. The policies that were violated are the following:

*The continue monitoring of the network is not doing its work, because the personal in charge of monitoring the bandwidth should notify this unusual behavior before it turns into an obvious incident.

*There is no sufficient personal on Saturday, the only person that responded to this unusual behavior was a member of the networking staff, the policy says that is needed a hole group in charge. And the responsibility of notifying this to the manager of the response incident team should be the person in charge of the networking team.

*There is a metric or an specific measure that says how long does the website can be down before calling in an "incident", so it violates the website's permitted time to be down.

*There is no data reported in a formal way, this incident needed to be wrote down using a report incident format so the organization can have a management of the incident's historical or to enhance the security policies.

*They doesn't share information with the parties being affected such as external users that doesn't know the website is down.

*The network security was violated, somehow the system is sending and receiving UDP packages from the same source IP and port, and investigation should take place in order to find how the security were infringed.

2.-What measures are in place to attempt to prevent this type of incident from occurring or to limit its impact?

R=In order to prevent this type of incident from occurring or limit we can implement the following practices or measures:

*Having a periodically risk assessment this can show us back doors or vulnerabilities that can be potential threats, for this case in particular we need to found ways to break into the DNS server.

*Because someone somehow found the way to send requests from the DNS server, the response incident team needs to lead an operation to ensure that there is a enough security level for all users of this server. One way of finding the origin of who break in to the server is taking a look to the DNS server's logs getting the date and time it started to fail.

*Using the tools provided by the response incident team we can access to the networks logs of each device inside the network and monitor them in case of suspicious activity. By the other hand, we can monitor the network capacity so we can contemplate possible changes of infrastructure.

*Applying firewalls and software to detect malware or intruders.

*Having a good awareness of the policies.

2.4 DETECTION AND ANALYSIS

1.- What precursors of the incident, if any, might the organization detect? Would any precursors cause the organization to take action before the incident occurred?

R= Yes, all this precursor help to take action before the incident occur. Some examples are [1]:

1- Web server log entries that show the usage of a vulnerability scanner
2- Network capacity tool predicts a big transit of packages coming.
3- Network capacity tool predicts improvements needed in the network architecture for further applications.
4- Software notice of new update available.
5- Antivirus software denies entry from unknown sources.

2.- What indicators of the incident might the organization detect? Which indicators would cause someone to think that an incident might have occurred?

R= The number 1 and 4 [1].

1- An application registers multiple failed login attempts from an unfamiliar remote system.
2- Antivirus software triggered alerts of unidentified packages coming.
3- A member of the organization's networking staff responds to alerts from a Internet border router.

4- An unusual large volume of UDP packets are found.
5- Internet bandwidth is being consume rapidly.

3.- What additional tools might be needed to detect this particular incident?

R= A IDPSs, SIEMs, Antivirus and antispam software, Network device and Operating system logs and Third party monitoring tools [3][4].

Detect incidents
SysInternals-detect: The Sysinternals web site was created in 1996 by Mark Russinovich to host his advanced system utilities and technical information. Whether you're an IT Pro or a developer, you'll find Sysinternals utilities to help you manage, troubleshoot and diagnose your Windows systems and applications.
Windows GodMode-detect: If you're sick of switching between the Settings menu and the Control Panel, searching for your lost settings, there is a way to access all settings and controls in one place: GodMode.
ArcSight ESM: HPE's ArcSight ESM collects security log data from an enterprise's security technologies, operating systems, applications and other log sources, and analyzes that data for signs of compromise, attacks or other malicious activity.
Cyphort: It's an open scalable software platform that deploys quickly, works with the security products you already have in place, and accelerates the productivity of security analysts and incident responders. Just as important, it

strengthens your organization’s security posture.
RTIR : RTIR is a free and open source system for the treatment of incidents. Its design meets the needs of CERT and other response teams.

4.- How would the incident response team analyze and validate this incident? What personnel would be involved in the analysis and validation process?

R=First the response team members need to understand the normal behavior of the network and the devices inside it, they need to know what kind of traffic does it handles, the maximum time it can be down, how to use the monitoring tools, etc.

The next thing to do is to alert third parties that your website is down temporarily, and report the incident with the Information Security Officer. Next, the personal member of the response team and departments such as IT and information security need to divide chores such as: Check logs, use monitoring or sniffers to find the source of the IP address, and if there was some vulnerabilities the team doesn’t count into consideration. There is also needed evidence of the incident to be reported someone need to handle this evidence. Once found the origin the team can restore all to their normal state and punish who tried to take down the website remotely, if it was some members of the organization Human resources needs to apply a sanction in function of the damage caused.

5.- To which people and groups within the organization would the team report the incident?

R= Using NIST reference [1]:

*CIO
*Head of information security
*Systems owners
*The management group(In order to report the incident and stablish the response policy for this kind of incidents)

*IT head leader and support team

*Information Assurance team (In case we need to alter secure controls such as firewalls, privileges, passwords etc.)

*Business Continuity Planning team (To ensure that incident response policies and procedures and business continuity processes are coordinated)

6.- How would the team prioritize the handling of this incident?

R=The response team first, should consider how the incident will impact the existing and future functionality of the affected systems. The functionality being affected in this case is the website page, the team need to think about how this affect to the continuity of the business plan, how critical is to have this server working fine. Next, they need to evaluate what kind of information is flowing through the DNS server and if it is likely to get lost in this incident because we don't know what kind of requests are being sent and arrived both from the DNS server, probably is a trap to break into the organization's security and filtrate sensitive information. Finally, they need to measure recoverability, this is in function of the information impact and functionality impact. We can establish levels of impact in each category, weighting from 0 (less impact) through 3 (big impact) [1]:

Functional Impact

0	No effect to the organization's ability to provide all services to all users
1	Minimal effect; the organization can still provide all critical services to all users but has lost efficiency
2	Organization has lost the ability to provide a critical service to a subset of system users
3	Organization is no longer able to provide some critical services to any users

Information Impact

0	No information was exfiltrated, changed, deleted, or otherwise compromised
1	Sensitive personally identifiable information (PII) of taxpayers, employees, beneficiaries, etc. was accessed or exfiltrated
2	Unclassified proprietary information, such as protected critical infrastructure information (PCII), was accessed or exfiltrated
3	Sensitive or proprietary information was changed or deleted

Recoverability Effort

0	Time to recovery is predictable with existing resources
1	Time to recovery is predictable with additional resources
2	Time to recovery is unpredictable; additional resources and outside help are needed
3	Recovery from the incident is not possible (e.g., sensitive data exfiltrated and posted publicly); launch investigation

There is a lot of factors involved when prioritizing chores is needed, such as the organization's objectives, preferences and more, but what we need to think here is: What suits us? To recover functionality over information? Or vice versa? What would happen if I recover the DNS server first and then I recover information using an up to day back up, what if I do not have a backup that comes handy for the situation? well in the process the team would find out the best way.

2.5 CONTAINMENT, ERADICATION, AND RECOVERY

1.- What strategy should the organization take to contain the incident? Why is this strategy preferable to others?

R= Probably the best strategy is the sandboxing [1], redirecting the flow of the UDP packages to other server that is less critical, or to have some dedicate computers just for the propose of receive the attack, this will give enough time to the team to analyze better the situation and meanwhile mitigating the future damage.

Another thing to contain the problem is to block the IP being used, taking offline the website, if the server is found to be infected probably is better to disconnect it from the network so other servers don't get infected too.

The sandboxing is preferable over the other strategy because this helps to make more time while this incident is being reviewed in case of turn into something more than a big number of requests to broke down the website, probably this is an attack to penetrate the servers security but as the response team doesn't know, they need to analyses better the situation not just terminate it in first instance.

2.- What could happen if the incident were not contained?

R=The team could have lost significant time and the problem may worsen, we could have lost the DNS server integrity, or even worse, external programs could have entered to the network to install scripts to be executed for stealing, corrupting or destroying important information.

These scenarios could have happened not only to the DNS server so is to the rest of the entities connected to the organization's network.

3.- What additional tools might be needed to respond to this particular incident?

R= Tools [3][4]:

Respond incidents
Splunk: Splunk offers the industry's leading operational intelligence

platform. They allow curious people to observe in detail what others are ignoring (the machine data) and to find what others will never see: information that can help your company more productive, profitable, competitive and secure.
FireWalls: Computer program that controls the access of a computer to the network and of elements of the network to the computer, for security reasons.
SugarCRM http://www.sugarcrm.com/crm/ Sugarforce (open source free version) http://www.sugarforge.org/
Website watcher http://www.aignes.com/index.htm This program detects updates and changes in websites

4.- Which personnel would be involved in the containment, eradication, and/or recovery processes?

R=Some of the previous mentioned will help, such as:

-Legal Department

-Public Affairs and Media Relations

-Head of information security

-Human resources

-Information Security Officer

-The manager of the incident group.

-The manager of the networking team.

-The technical lead.

-The Incident lead.

-The POC for external parties affected

-The networking staff:

-The person who monitors the network bandwidth.

-The person who is in charge of predicting network capacity.

-The coder, if is necessary to make changes of lower level.

-The person who is tracking the logs of the servers.

5.- What sources of evidence, if any, should the organization acquire? How would the evidence be acquired? Where would it be stored? How long should it be retained?

R=We need first to document the incident, the document must have the following structure:

-An introduction or summary telling when, where and what is the incident.

-Background of the incident, giving more details of the incident and similar incidents in the past.

-The process step by step of the analysis, containment, eradication and recovery and post-incident activity. In each point of the process is necessary to talk about the personnel involved and how they interact.

The second part of the evidence is to recollect the physical evidence such as information related to the servers, computer equipment, CDs, hard drives, USBs, printed information, information recollected from monitoring tools, data bases, time and dates, reports, calls and information gather from the media involved.

It is important to have a dedicated repository just for storing historical of incidents.

Once we have the enough evidence of the incident, we need it to store is distributed repositories so we have access any time but not all information needs to be store about this incident just the document need to be store permanently in the incident repository the rest of the information is just needed while the incident is being eradicated.

2.6 POST-INCIDENT ACTIVITY

1.- Who would attend the lessons learned meeting regarding this incident?

R= All parties involved are invited to the meeting, at least who needs to attend are:

Personnel of the CSIRT:

- General Director
- Manager of the CSIRT
- Communications Adviser
- Legal Adviser
- Researchers

Others:

*CIO

*Security Officer

*Head of the technical team

*Head of the network team

*The POC with external parties involved

2.- What could be done to prevent similar incidents from occurring in the future?

R= In order to respond more efficiently the next time a similar incident occurs we need to take into consideration the following steps:

-Have a meeting talking about the summary of the problem, the process to recover the DNS server functionality and problems during the process of recovery and eradication.

-We need to wrote down a “to do list” for a better handling of similar incidents, the to do list for this scenario could take into consideration this:

*Improve the security inside the DNS server, such as to restrict the ports being used and change to others that hasn’t being used before.

*Implement validation tools more restrictive.

*Change the way the personnel roles on weekends, probably using home office to have them before the indicator fires.

*Get a special server to be used as bait, for containment strategies.

*Have a list of contacts of trust will come handy if someone is not available.

*Implementing more strategies of monitoring and prediction of network traffic.

*Mitigate vulnerabilities.

3.- What could be done to improve detection of similar incidents?

R=The threat of being host attack is pretty high nowadays, this people and their attacks have become wittier, they learn of their fails too and find new ways to disrupt the system's work flow. The organization needs to be cleverer and think beyond what is actually being implemented. Having a intelligent monitoring control and security of critical infrastructure systems using technologies such as artificial intelligence, machine learning, pattern detection can leave the organization one step further of detection of incidents.

2.7 GENERAL QUESTIONS

1.- How many incident response team members would participate in handling this incident?

R=

General

- General Director

Personal

- Director of the office
- Accountant
- Communications Adviser
- Legal Adviser

Technical operating team

- Head of the technical team
- CSIRT technicians, responsible for the provision of services
- Researchers

2.- Besides the incident response team, what groups within the organization would be involved in handling this incident?

R= Using NIST [1]:

The management group: In order to report the incident and stablish the response policy for this kind of incidents.

Information Assurance: In case we need to alter secure controls such as firewalls, privileges, passwords etc.

IT Support: We need experts that knows exactly how some module of the system works, the technology it manages and understanding of the network.

Legal Department: In case the incident could have legal ramifications such as we are managing confidential information during the time the website was down, or if there may be a need for a memorandum.

Public Affairs and Media Relations: Because we need to inform the media and external parties we are having troubles.

Human Resources: If an employee is suspected of causing an incident.

Business Continuity Planning: To ensure that incident response policies and procedures and business continuity processes are coordinated, because this incident can alter the business continuity there is a need of knowing how to proceed in such cases.

3.- To which external parties would the team report the incident? When would each report occur? How would each report be made? What information would you report or not report, and why?

R= All groups affected need to be aware of the situation, specially does who are affected directly such as IT group, Business Continuity Planning group, Management group and the Information Assurance group besides the internal groups external parties being affected also may be informed about what happened inside the organization, what controls where violated, what proceeded and possible damage or lost.

The external parties identified here are:

*Media such as users of the website

* Mexico:

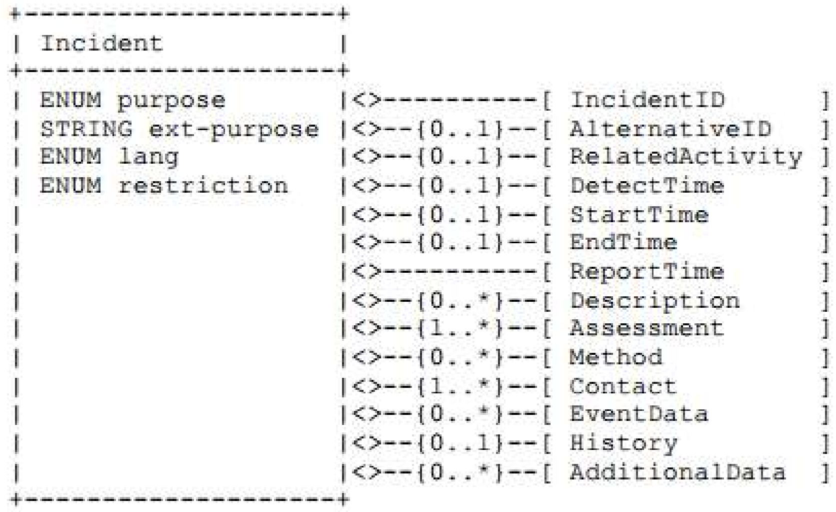
> In means of law enforcements agencies, we need a POC with the Federal Institute of Access to Public Information INAI, other organizations may be the Internet service providers ISPs, the owners of Attacking Addresses, Software Vendors and affected external parties in general.

*USA

> Agencies in USA are FBI, US-CERT and ISACs, Internet service providers (ISPs), owners of Attacking Addresses, Software Vendors and affected external parties in general.

The report must be created immediately, at the same time the incident was detected, the date and time the report is sent to the external parties
it is subject to the external organization agenda.

In order to have an deo of what information needs to be reported, the team can lean on this incident structure, it was taken out of the rfc5070 (Request for Comments standards-setting bodies for the Internet) [5]:



```
+--------------------+
| Incident           |
+--------------------+
| ENUM purpose       |<>----------[ IncidentID      ]
| STRING ext-purpose |<>--{0..1}--[ AlternativeID   ]
| ENUM lang          |<>--{0..1}--[ RelatedActivity ]
| ENUM restriction   |<>--{0..1}--[ DetectTime      ]
|                    |<>--{0..1}--[ StartTime       ]
|                    |<>--{0..1}--[ EndTime         ]
|                    |<>----------[ ReportTime      ]
|                    |<>--{0..*}--[ Description     ]
|                    |<>--{1..*}--[ Assessment      ]
|                    |<>--{0..*}--[ Method          ]
|                    |<>--{1..*}--[ Contact         ]
|                    |<>--{0..*}--[ EventData       ]
|                    |<>--{0..1}--[ History         ]
|                    |<>--{0..*}--[ AdditionalData  ]
+--------------------+
```

Another format found to report incidents is the following:

INCIDENT COMMUNICATION FORM

Please complete this form and send it by fax or email to: ....
Lines marked with an asterisk (*****) are mandatory.

Name and organization
1. Name *:
2. Name of organization *:
3. Sector:
4. Country *:
5. City:
6. Email address *:
7. Phone number *:
8. Others:

Affected computer (s)

9. Number of computers:
10. Computer Name and IP *:
11. Function of the computer *:
12. Time zone:
13. Hardware:
14. Operating System:

15. Software Affected:
16. Files affected:
17. Security:
18. Computer Name and IP:
19. Protocol / port:
Incident
20. Reference number:
21. Type of incident:
22. Inception of the Incident:
23. The incident has yet been resolved: Yes NO
24. Time and method of discovery:
25. Known Vulnerabilities:
26. Suspicious files:
27. Measures:
28. Detailed description *:

This is the minimum required data for reporting and identify the incident.

4.- What other communications with external parties may occur?

R= Once the team have detected to whom this IP address belongs, the team should find them and contact them.

The team needs also to connect with the users of the website, this could be specific clients or public in general.

In case of have broken the law, the team need to contact human resources and law enforcement agencies to discuss evidence handling. The team can contact this institutions with the help of a primary and secondary point of contact (POC).

5.- What tools and resources would the team use in handling this incident?

R= Sources in the USA:

* Anti-Phishing Working Group (APWG)

* Computer Crime and Intellectual Property Section (CCIPS), U.S. Department of Justice

* Government Forum of Incident Response and Security Teams (GFIRST)

* High Technology Crime Investigation Association (HTCIA)

* National Council of ISACs
* United States Computer Emergency Response Team (US-CERT)

* https://www.howtogeek.com/

* SANS Institute: Information Security Resources
* Infosecurity Magazine - Information Security & IT Security News

Tools[3]:

Prevent incidents	**Detect incidents**	**Respond incidents**
EMET: The Enhanced Mitigation Experience Toolkit (EMET) is a utility that helps prevent exploits of software security vulnerabilities.	**SysInternals-detect:** The Sysinternals web site was created in 1996 by Mark Russinovich to host his advanced system utilities and technical information. Whether you're an IT Pro or a developer, you'll find Sysinternals utilities to help you manage, troubleshoot and diagnose your Windows systems and applications.	**Splunk:** Splunk offers the industry's leading operational intelligence platform. They allow curious people to observe in detail what others are ignoring (the machine data) and to find what others will never see: information that can help your company more productive, profitable, competitive and secure.
Q-Radar: IBM QRadar SIEM consolidates logging events and network flow data from thousands of endpoints, devices and applications distributed across the network. It normalizes and correlates raw data to identify security offenses and uses the advanced Sense Analytics engine to establish baseline normal behavior, detect anomalies, discover advanced threats, and eliminate false positives.	**Windows GodMode-detect:** If you're sick of switching between the Settings menu and the Control Panel, searching for your lost settings, there is a way to access all settings and controls in one place: GodMode.	**FireWalls:** Computer program that controls the access of a computer to the network and of elements of the network to the computer, for security reasons.
PIM: A Product Information Management (PIM) system centralizes and harmonizes all marketing and technical	**ArcSight ESM:** HPE's ArcSight ESM collects security log data from an enterprise's security technologies, operating systems, applications and other log sources, and	**SugarCRM** http://www.sugarcrm.com/crm/ Sugarforce (open source free version) http://www.sugarforge.org/

information in product listings and catalogs.	analyzes that data for signs of compromise, attacks or other malicious activity.	
ARGUS: ARGUS Enterprise is the global standard for property valuation and most comprehensive asset and portfolio management solution in the world. Trusted by leading investment firms to value property, secure capital, manage assets, and generate wealth.	**Cyphort:** It's an open scalable software platform that deploys quickly, works with the security products you already have in place, and accelerates the productivity of security analysts and incident responders. Just as important, it strengthens your organization's security posture.	**Website watcher** http://www.aignes.com/index.htm This program detects updates and changes in websites
	RTIR : RTIR is a free and open source system for the treatment of incidents. Its design meets the needs of CERT and other response teams.	

6.- What aspects of the handling would have been different if the incident had occurred at a different day and time (on-hours versus off-hours)?

R= Since the incident occurred on a Saturday afternoon, probably there wasn't enough technical personal to attend all the departments involved to prevent this of being a mayor incident. If this would have happened in a different day and time the probability of had worsen would be decreased significantly, there would have been more services available, the contact with external parties would have been easier because many of they don't work on weekend.

7.- What aspects of the handling would have been different if the incident had occurred at a different physical location (onsite versus offsite)?

R= The location is very important nowadays, having a distributed architecture is more reliable than having a centric one. If the incident had occurred at different physical location, we would have the opportunity to connect the branch offices with others located mills away, this increases the chance of finding more technical resources such as specific personal, computer equipment that can be accessed remotely, distributed services and backs up of the information in case this would have worsen.

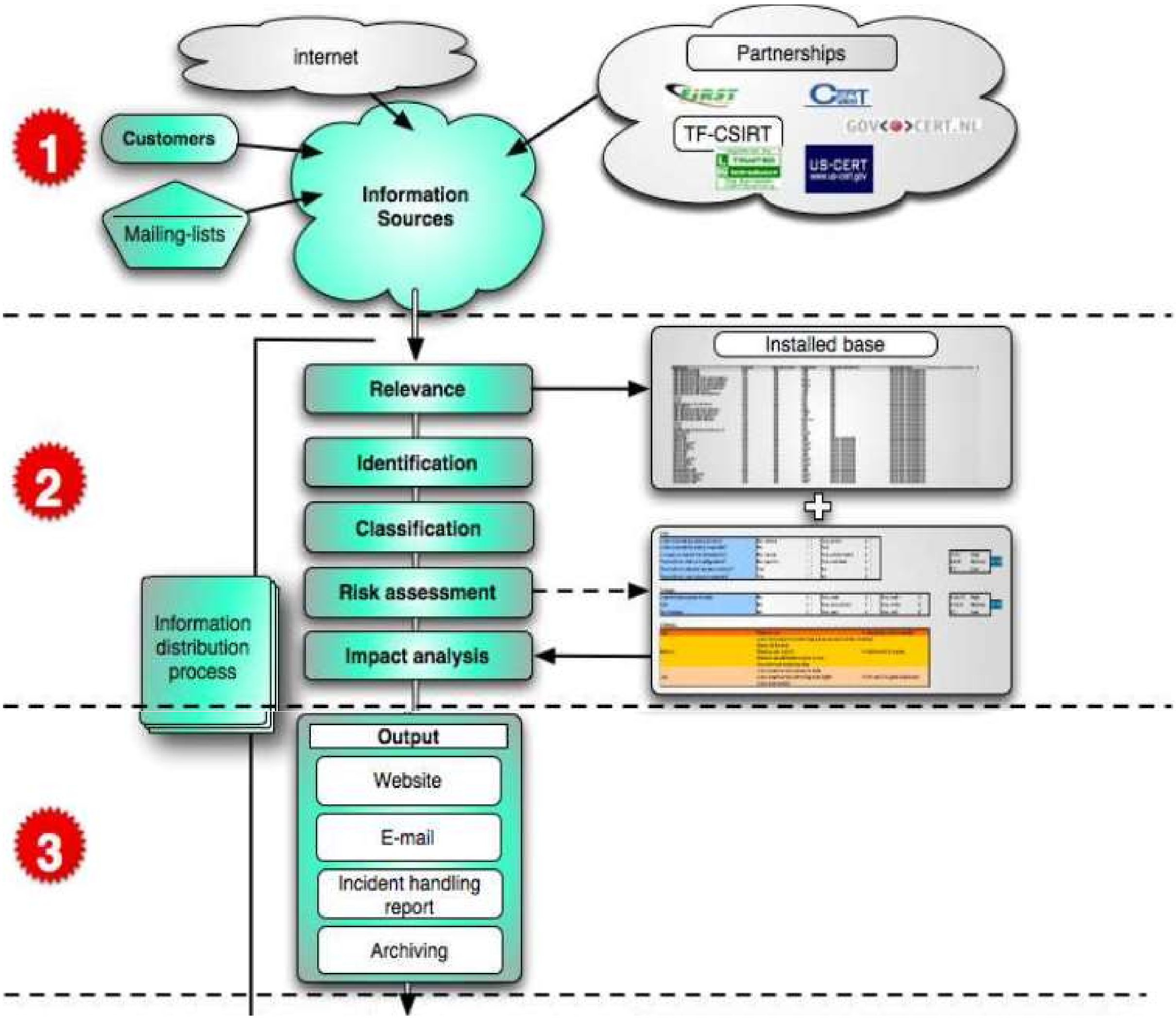
2.8 SCENARIO 1 CSIRT HANDLING EXAMPLE

By way of illustration, this chapter describes an example of day-to-day practice of a CSIRT: The creation of a security warning. The trigger was the following original security warning sent by email from the internal network staff to the CSIRT:

ID	WS06-042
Title	Web site is down
Description	The internet border router shows an unusual volume of UDP packages flowing to and from the public DNS server. Analysis of the traffic shows that the DNS servers are receiving high volumes of requests from a single external IP address.
Calculated Risk	Vital
consequences	Remote program execution, possible intrusion to other servers, possible attack.
OS affected	Windows Server

The bulletin addresses an incident detected on public DNS servers.

After receiving this vulnerability information through a mailing list, the CSIRT begins to apply the scheme described below [4]:



Step 1: Gathering Incident Information

The first is to check the authenticity of the report by searching the database for the name of the person sending the incident report.
The second is once verified its validity, begin to review the affected internal IT systems as well as external parts that are affected.
The network logs will be checked as well as those of the servers to obtain date and time of the supposed sending of packages coming from the mentioned external IP address.

Step 2: Evaluation of information and risk assessment

Identification

The information has already been verified by collating the data received by e-mail with the text that appears on the provider's website.

Relevance

The CSIRT compares the list of affected systems against the ones used by the served group. He realizes that several of the clients of the group served use that server and that they must immediately inform them of the problem before it worsens, so the information about the incident is pertinent.

Since the CSIRT serves only to the organization (it is local) the personnel to which it needs to notify the incident are: To the Security Officer, IT technical head leader, The manager of the networking team.

Category	Aplication	Software	Version	OS	OS version	Attended group
DNS public Server	Web-site	Windows Server	2016	Microsoft	x-x	Internal

Classification

The information is public, so it can be used and redistributed. It is necessary to warn that the website is temporarily down.

Risk assessment and consequence analysis

The answers to the following questions show a risk and high level consequences (considered critical by Microsoft).

¿Is vulnerability well known?	N
¿It has extended?	N
¿Is it easy to abuse?	S
¿ It is a vulnerability that can be used improperly remotely?	S

Damage

Possible consequences are remote accessibility and remote program execution. This vulnerability presents numerous problems, which makes the High risk of damage

This information below is ready for distribution. As it is a decisive newsletter, it is advisable to also call the customers of the group served, if possible

Step 3: Distribution

Your available communication channels are email, phone and an internal website. The CSIRT produces this notice:

Title
DDoS attack detected from the DNS public server

Reference
082006-1

Affected Systems

- Web Server
- DNS public server
- Microsoft Windows Server 2016 Service Pack 1
- Microsoft Windows Server 2016 for Itanium-based Systems and Microsoft Windows
Server 2016 SP1 for Itanium-based Systems

Risk
HIGH

Consequences/damage
HIGH

External IDs:
MS-06-42

Incident description
The internet border router shows an unusual volume of UDP packages flowing to and from the public DNS server.
Analysis of the traffic shows that the DNS servers are receiving high volumes of requests from a single external IP address.

Consequences
An attacker could take complete control of the system, install programs, add users and view, change or delete data.
Mitigating factor: All that can only happen if the user is logged in with administrator rights. The consequences on users
Connected with few rights may be minor.

Solution
Disconnect the page temporarily, redirect the attack to less important server while tracing the origin of the IP, block the IP and the maximum of packages that can be received in a given time of the same IP, increase the security in the listening ports, update software, do virus analysis, search for possible damages, restore integrity. Turn the page on again. Contact with the owner of the external IP address.

Details
For more information about how to stop a DDoS:
https://foro.elhacker.net/tutoriales_documentacion/intentando_detener_un_ddos-t137442.0.html

CHAPTER 3

CONCLUSION

CONCLUTION

Information security has become very important today, not having a good management of information security could lead to the total loss of the company. The management of information security is not only to protect the information and the systems themselves it is necessary to make a specific organizational architecture for this process, it must be contemplated the turn of the company, as they communicate between departments, the monitoring of their systems, Access control, policies, training, documentation, external relationships and more. That is why it becomes so extensive and complex because it is an entire organism by itself.
This practice gave us the opportunity to contemplate only the incident response part and yet it involves all functionalities mentioned above, it gives us an idea of how complex and important this organism is within an institution. It helped us to be more analytical and to carry out an organized incident mitigation process that in fact can apply to incidents of all kinds not just computer.

REFERENCES

[1] Paul Cichonski, Tom Millar, Tim Grance Karen Scarfone. NIST Special Publication 800-61 Revision 2. Computer Security Incident Handling Guide. (August2012). Obteined from NIST.SP.800-61r2.pdf

[2] Everett C. Johnson, CPA, Deloitte & Touche LLP (retired), USA, International President. Guidance for Boards of Directors and Executive Management 2nd Edition. Obteined from information-security-govenance-for-board-of-directors-and-executive-management_res_eng_0510.pdf

[3] JD Sartain. 13 must-have security tools.(May 2018). Obteined from http://www.networkworld.com/article/2923433/security0/13-must-have-security-tools.html
[4] ENISA.How to build a CSIRT step by step.(2006).Obteined from CSIRT_setting_up_guide_ENISA-ES.pdf

[5] R. Danyliw, CERT.(December 2007. Obteined from rfc5070.txt.pdf

[6] http://www.first.org/resources/guides/csirt_case_classification.html.

[7] RIPE whois: http://www.ripe.net/whois

[8] IRT-object: http://www.enisa.europa.eu/cert_inventory/pages/04_02_01.htm
[9] Trusted Introducer:

http://www.enisa.europa.eu/cert_inventory/pages/04_01_03.htm#07