**Cyber Crime Reporting; incident reporting system**

SR Kularathne#1 and Sujith christy#2

# Faculty of Computing, General Sir John Kotelawala Defence University, Ratmalana, Sri Lanka

#1 sachikularathne@gmail.com

Abstract*— cybercrimes affect in many fields in today society. There is a lack of cybercrime reporting software and reporting cybercrimes due to privacy issues. Incident reporting should contain good feedback and response. In an incident reporting system and privacy is a must.*

*As in methodology different user restrictions should include in the system according to the user level of the system. Requested data from the users of the system should be provided via the forms uploaded in the system which is connected to a system database.*

*As include in conclusion most data can be uploaded to the system and the response time and security of the system is high when comparing with the file-based system and other incident reporting systems.*

1. Keywords— **Internet crime**, **Cyber-attacks, Events,**

**Incident, CIA**

I. INTRODUCTION

Internet crime is any crime or illegal online activity committed on the Internet, through the Internet or using the Internet. The widespread Internet crime phenomenon encompasses multiple global levels of legislation and oversight. In the demanding and continuously changing IT field, security experts are committed to combating Internet crime through preventative technologies, such as intrusion detection networks and packet sniffers.   
 Internet crime is a strong branch of cybercrime. Identity theft, Internet scams and cyberstalking are the primary types of Internet crime. Because Internet crimes usually engage people from various geographic areas, finding and penalizing guilty participants is complicated.

IT incident management is an area of IT service management wherein the IT team returns a service to normal as quickly as possible after a disruption, in a way that aims to create as little negative impact on the business as possible.

EventsUnderstand that an event is any observable occurrence in a system or network. An event may be as simple as a user logging on, an application opening a port, or data transferring between systems. IncidentsKnow that an incident is an event with the potential to cause harm to the organization. An incident is usually considered an intrusion by an outside force, but it may also be caused by an internal user. An incident may also be intentional or unintentional

A close up of a card

Description generated with high confidence

Figure 3.cybercrime, top 20 countries

Most of the cybercrime incidents happened in the world are affected by the developer countries with high technological rate.

Most cybercrime incidents in no developed countries are not reported due to cultural, legal and governmental policy issues.

Main cybercrime attacks mainly include user threats, application threats, infrastructure threats. User threats include

Spear phishing, privileged account management. Main infrastructure threats are botnets and DDOS attacks.

II. Literature Review

A.Cyber attacks

Research has shown that the many number of individuals and organizations have affected by many cybercrime attacks. there is a lack of incident reporting software in the country.

US President Obama declared that “cyber threat is one of the most serious economic and national security challenges we face as a nation” and that “America’s economic prosperity in the 21st century will depend on cyber security.”

As in UK Cyber Security Strategy 2011 they have mentioned that “Cyberspace is an interactive domain made up of digital networks that is used to store, modify and communicate information. It includes the internet, but also the other information systems that support our businesses, infrastructure and services.”

Cyber securitizations are particularly powerful precisely because they involve a double move out of the political realm: from the politicized to the securitized, and from the political to the techniﬁed, and it takes an inter-disciplinary effort to assess the implications of the move, and possibly to counter it. (Lene of Copenhagen School and Helen of New York University,2009)

Most of the cyber security attacks happen due to exposure of individuals and organizations to the public communications and internet. They are mainly as follows,

**Malware Introduction** Implantation of malware or malicious code within ads with third-party apps owned by an organization can pose real risks ranging from exposing proprietary information, culminating in the devalue of the corporate brand. End users continuously Security Education and Awareness Training **151** receive emails or solicitations with a “click here” invitation. They need to be informed opening unsolicited attachments and “click here” invitations can trigger the introduction of malware onto their system.

**Social Media Platforms** Employees in most organizations are increasingly using social media platforms like Twitter, LinkedIn, and Facebook to communicate with friends, family,

and business customers. Individuals are sharing more personal information online which poses a significant threat as new “friends” and “followers,” most of whom are

unknown, pose social engineering threats. Through *Twitter feeds* and *online posts*, end users could expose corporate information, including non-public information of a financial

nature that could potentially lead to insider trading. In the event of a corporate crisis where press inquiries were normally made through the public affairs department, end users now simply tweet or post information online, providing a direct link to the press.

**Password Exposure** With the introduction of personal end-user devices, the ability for IT administrators to enforce password best practices has disappeared. After years of password breaches and warnings about weak passwords, a large percentage of people are still choosing words like *welcome* or words derived from personal information such as a birthday for passwords. This ultimately places company data and networks at risk. IT administrators have the

ability to mandate password construction, expiration, and other attributes through such tools as *Group Policy Manager*. But this is only effective with systems where hosts directly connect to the network.

1. Incident reporting systems

Incident reporting is the process of notifying a user or administrator of an abnormal event, process or action identified on a computing device, system or environment. It is part of the security incident and event management (SIEM) process that alerts and logs all security incidents discovered within an IT environment. Incident reporting is also known as security incident reporting or incident tracking.

incident reporting is generally performed by an anti-virus, firewall application or a purpose-built incident reporting software. Incidents can also be detected manually by the network, IT or security administrator. Some of the incidents reported may include:

* Violation of security policies/procedures
* Unauthorized access/access attempts
* Abusive use of an IT asset
* Suspicious usage patterns

All such incidents are recorded within an incident log file and are used to asses, act, neutralize and recover from the incident. (techopedia,2018)

There are many online incident reporting systems including US-CERT,National Incident-Based Reporting System of FBI.

1. User limitations

According to the CIA tried user limitations can be given by access control methods.

Users can login to the system and view and report data by userbase access control methods.

With *discretionary access control* , access is granted to objects (data and applications) based upon the identity of the subject. Typically, the

following actions may be granted to the user for a fi le:

■ Full Control

■ Modify

■ Read & Execute

■ List Folder Contents

■ Read

■ Write

■ Special

1. Information gathering techniques

Analysis Information-Gathering Techniques On many occasions, it will be the responsibility of the security practitioner to participate in the risk analysis process. Information may be gathered under different subject information categories that will be used during the analysis process.

Determine a list of assets. Sometimes it is a major undertaking to locate hardware in racks, closets, and ceiling spaces or to identify software assets such as purchased applications, licenses, databases, proprietary information, and intellectual property stored away on servers and user workstations.

Determine potential threats to an asset. This activity may involve both historical data and

expert opinions.

Determine annual rate of occurrence. This activity may involve log data and historical information.

Determine how much of an asset was lost based upon prior attacks. This is attempting to determine the exposure factor based upon historical information.

This information is required for accurate calculations during risk analysis. Much of it comes from accounting data sources and historical data, while other information might be available from subject matter experts (SMEs)Subject matter experts such as database administrators, network managers, and administrators as well as technical staff may supply knowledge concerning the performance of an asset. Another source of data used in risk calculations may be supplied by department managers, executives, or general users based upon recollections or memory of loss occurrences.

The following techniques can be used in gathering information relevant to an asset within its operational boundary or knowledge area.

Questionnaire in Risk assessment can develop questionnaires ,by different types of questionnaires can return relevant information. A questionnaire may ask for identification of all hardware and software items within a department or used by a personal. A separate questionnaire may ask the number of times an asset was unavailable for service. To avoid confusion, a clear procedure should be established describing the asset by name or inventory asset number.

Onsite Interviews Onsite interviews might be much more effective than attempting to retrieve questionnaires that were previously sent to individuals. It may, in fact, be easier and faster to discuss information in person to be included on a questionnaire. Onsite interviews often allow the interviewer to observe the asset and determine operation and asset security.

Document Review During a document review, all things pertinent to an asset are examined, including system documentation, directives, policies, user guides, and an acquisition document. Security-related documentation such as spot reports, risk assessment reports, system test results, system security plans, and system security policies might be examined. Important documents also include prior impact analyses or asset criticality assessments.

Scanning Tools, A wide variety of scanning tools are available that can be used to scan for potential vulnerabilities on both networks and host devices. Scans may be both active and passive. Active scans are scams that are initiated for a particular purpose such as identifying weak passwords, open ports, or vulnerabilities in applications. Passive scans may be performed continuously as actions occur on a regular basis. For example, passive scans may review individual passwords as they are created by users on a daily basis ,to protect the users from unautorized access to their accounts.

III. METHODOLOGY

In incident management following process can be taken to identify the incident and overcome from the threat.

A close up of text on a white background

Description generated with very high confidence

Figure 2.Incident management process

An Incident response plans should be the requirement that the incident response team should be required to make incident response plans and keep activity records starting at the beginning of the incident and continuing through resolution. Team responders should record all actions

and activities, either during the process or immediately thereafter, to completely document all actions taken during the event. The collection and documentation of all evidence, description of the scene, statements from individuals, and evidence processing notes must be fi led and maintained

in the event of a formal forensics examination or eventual legal action. Team responders should record all actions and activities, either during the process or immediately thereafter, to adequately document all actions taken. In the event of a forensic examination or eventual legal

action, the collection and documentation of all evidence, description of the scene, statements from individuals, and evidence processing notes must be fi led and maintained.

Many incident response teams regularly review after-action reports to identify areas of improvement.

At a minimum, the following incident response information should be recorded which should be included in an incident response plan,

■ Date and time of incident

■ Type of incident or incident level

■ Incident summary

■ Incident discovery information

■ Actions taken by individuals

■ Contact information for individuals involved

■ After-action report

1. Access control for the system users

According to the CIA triad we have to maintain access control for the users according to their user level. There are three main types of users in this system they are admin, staff and customers. Admin has the all the privileges in the system while staff has privileges to read, write and execute. customers only have the privilege to read and write.

1. Incident response Containment and Restoration

The incident response plan should provide the details of all actions to be taken during a specific incident. Actions might include isolating the device from the network by, for example, disconnecting the Ethernet plug or pulling the power plug from the wall to shut down the affected network equipment. Plans may differ depending upon forensic investigation requirements. For instance, a forensic investigation might include disconnecting the device

from the network but keeping the unit powered up so that volatile RAM memory can be recorded or examined. A Faraday bag may be utilized to shield a device that is connected to a wireless access point.

It is never advisable to not take action and “monitor” an attack while it is in progress. In some cases, an IT individual may attempt to trace an attack back to its origin

rather than terminating the attack. Such a trace is usually fruitless as attackers have many ways of disguising their actual location. Devices such as log fi les, monitoring

appliances, honeypots, bastion hosts, and other devices may record the IP address or vectors of an attack. If an attack is discovered and not stopped, the organization may

face various legal liabilities.

Many corporate incident response policies require that a post-incident restoration action be invoked after an attack. These usually require that the attack unit be reimaged or

restored from known good backups. Rarely are devices placed back into service after only one anti-malware or antivirus scan.

1. Implementation of countermeasures

Countermeasures are usually put in place as a response to a risk analysis. In many cases they are intended to mitigate specific threats or vulnerabilities. Controls involve a much

broader category of risk mitigation tools and may be put in place in response to best practices or due care. In many situations, the terms countermeasure and control are used

interchangeably.

The application of countermeasures in a network or on a device such as a host computer does not relieve the operators or administrators from responsibility. User training is important so that controls and countermeasures are installed and operated correctly.

1. Disaster recovery plan

After a disaster event, it is extremely important to restore IT services and functions. The

restoration process may be detailed for a disaster recovery plan. The high-level disaster recovery policy is an executive-supported policy that sets forth the creation of the disaster

recovery plan (DRP). In the event of a disaster affecting IT operations, all IT personnel, will participate in recovery efforts to restore IT services as soon as possible. As you

have seen, in business continuity planning, the majority of business operations are contingent upon active and reliable IT services and functions. The difference between a disaster recovery plan and an incident response plan is that an incident response plan details the methods and procedures used to detect and stop an imminent threat to the organization’s IT assets while the disaster recovery plan is designed to rebuild, recover, and restore damaged assets to full operational capacity. Restoration operations may take a period of time and significant coordination and effort to rebuild or refurbish facilities, restore order, restore and provision hardware products, and restore data

and applications from backup sources. There are some things to consider during the creation of the disaster recovery plan. Some of these considerations are detailed in the following sections.

1. Incident response Containment and Restoration

The *risk treatment schedule* documents the plan for implementing preferred risk mitigation strategies for dealing with identified risks. A risk treatment schedule is an output of the risk assessment phase. Risks have been identified, and various controls have been selected to reduce risk. The risk treatment schedule is a listing of risks in order of priorities.

A screenshot of a cell phone

Description generated with high confidence

Figure 3.Risk Treatment schedule and plan

Although each risk treatment plan can be customized specifically for an organization, at a minimum the plan should include the following sections:

Risk Identification NumberFor example, identified risks can be sequentially numbered in a hierarchy format such as 1.0, 2.0, and 3.0 as the main risks, with 1.1 as a sub-risk and

1.1.1 as an underlying risk under this risk.

Name of RiskRisks are listed in order of priority.

Risk Treatment TechniqueList techniques such as acceptance, avoidance, reduction, and transference.

Selected ControlInclude a list of controls selected to reduce the risk. Risk Rating after TreatmentUse high, medium, and low or a 1-to-10 risk rating scale. Cost Benefit AnalysisThis is an optional analysis of the cost benefit of the control that mitigates risk. Person Responsible for Implementation of the ControlUsually listed by department and role.

Timetable for ImplementationThis is a date when the control will be fully operational.

Control Monitoring MethodThis is a description of how to monitor the control after it is in place. Baselines and standards to be used should be specified.

Incident ResponseA brief description of the intended response to an incident. This field may also refer to an incident response plan document. Although the risk treatment schedule takes the form of a spreadsheet template, many of the fields are brief descriptions. The risk treatment plan should include full documentation

supporting the identification of a risk during a risk assessment activity, an impact analysis, some control selection criteria, control baselines and standards, and an incident response document.

1. Risk Register

A *risk register* is a primary document used to maintain a record of risks. It is a direct output of the risk assessment process. A risk register includes a detailed description of each risk that is listed. Although the risk register may appear to overlap the risk treatment schedule, the two documents serve different purposes. The risk treatment plan should include complete documentation concerning the identification of threats and asset vulnerabilities.

It also prioritizes risks, so they can be addressed with available resources. The risk registers

might include the following fields or columns:

■ Risk Identification Number

■ Name of Risk

■ Name or Title of Team Member Responsible for the Risk

■ Initial Date Reported

■ Last Updated

■ Impact Rating

■ Impact Description

■ Probability of Occurrence

■ Timeline for Mitigation

■ Completed Actions

■ Future Actions

■ Risk Status

IV. EVALUATION

After evaluating the and gathering the data following details can be identified. In most of the devolved systems excel sheets or forms are used as online incident management systems. Many features should be added to incident management systems including feedback that has to be provided to the user/customer.

There should be a method to report cybercrimes that has happen to organizations as well as individuals. Privacy of the information should be protected.

Restrictions should be given to each system user according to their roles.

V. CONCLUSION

The internet attacker and the web are getting vulnerable day by day with the advancement of the information technology. Many personal attacks and industrial attacks has happened and there is a lack of incident reporting and lack of incident reporting software.

Many incident reporting websites and forms are available, most of the are not user friendly and nonreliable. Accuracy of incident man agent should be high when giving a respond to a customer by these types of software.

VI. LIMITATIONS

Faults in the hardware device and din not count in as a factor of consideration in this paper. There is a limitation of time that can be given to respond to the customer.

Acknowledgment

Authors would like to acknowledge all who supported during this research and the authors of the references that help to contribute in a vast amount in this research.

References

internet crime rate - Bing. 2018. internet crime rate - Bing. [ONLINE] Available at: <https://search.handy-tab.com/?q=internet%20crime%20rate&f=ht&type=images&page=8>. [Accessed 30 October 2018].

Techopedia.com. 2018. What is Internet Crime? - Definition from Techopedia. [ONLINE] Available at: <https://www.techopedia.com/definition/26587/internet-crime>. [Accessed 30 October 2018].

Bright hub Project Management. 2018. ITIL Incident Management: Diagram with Example. [ONLINE] Available at: <https://www.brighthubpm.com/risk-management/71332-strategies-for-incident-management-teams-sample-diagram/>. [Accessed 30 October 2018].

Incident Reporting System | US-CERT. 2018. Incident Reporting System | US-CERT. [ONLINE] Available at: <https://www.us-cert.gov/forms/report>. [Accessed 30 October 2018].

Techopedia.com. 2018. What is Incident Reporting? - Definition from Techopedia. [ONLINE] Available at: <https://www.techopedia.com/definition/30161/incident-reporting>. [Accessed 30 October 2018].

National Incident-Based Reporting System - Wikipedia. 2018. National Incident-Based Reporting System - Wikipedia. [ONLINE] Available at: <https://en.wikipedia.org/wiki/National_Incident-Based_Reporting_System>. [Accessed 30 October 2018].

B. murphy, G., 2015. SSCP Systems Security Certified Practitioner Study Guide. 2nd ed. Canada: SYBEX.