CST808: INCIDENCE MANAGEMENT AND DISASTER RECOVERY

AFRICA CENTRE OF EXCELLENCE ON TECHNOLOGY ENHANCED LEARNING (ACETEL)

NATIONAL OPEN UNIVERSITY OF NIGERIA

Course Guide for CST808

Introduction

CST808 – Incidence Management and Disaster Recovery is a 2-credit unit. The course is a compulsory course in second semester. It will take you 15 weeks to complete the course. You are to spend 65 hours of study for a period of 13 weeks while the first week is for orientation and the last week is for end of semester examination.

You will receive the course material which you can read online or download and read off-line. The online course material is integrated in the Learning Management System (LMS). All activities in this course will be held in the LMS. All you need to know in this course is presented in the following sub-headings.

Course Competencies

By the end of this course, you will gain competency to:

Protect and manage system and network infrastructure from risk management, disaster recovery and international standards

Course Objectives

The course objectives are to:

- Promote the management of the basic infrastructure from risk and disaster through proper administration
- Adopt international standards for effective management of systems and network infrastructure

Working Through this Course

The course is divided into modules and units. The modules are derived from the course competencies and objectives. The competencies will guide you on the skills you will gain at the end of this course. So, as you work through the course, reflect on the competencies to ensure mastery. The units are components of the modules. Each unit is sub-divided into introduction, intended learning outcome(s), main content, self-assessment exercise(s), conclusion, summary, and further readings. The introduction introduces you

to the unit topic. The intended learning outcome(s) is the central point which help to measure your achievement or success in the course. Therefore, study the intended learning outcome(s) before going to the main content and at the end of the unit, revisit the intended learning outcome(s) to check if you have achieved the learning outcomes. Work through the unit again if you have not attained the stated learning outcomes.

The main content is the body of knowledge in the unit. Self-assessment exercises are embedded in the content which helps you to evaluate your mastery of the competencies. The conclusion gives you the takeaway while the summary is a brief of the knowledge presented in the unit. The final part is the further readings. This takes you to where you can read more on the knowledge or topic presented in the unit. The modules and units are presented as follows:

Module 1 An Overview of Information Security and Risk Management

Unit 1 Concept of Information Security
Unit 2 Concept of Risk Management
Unit 3 Planning for Organisational Readiness

Module 2 Contingency Strategy for IR/DR/BC

Unit 1 Contingency Planning
Unit 2 Incidence Response
Unit 3 Disaster Recovery
Unit 4 Business Continuity

Module 3 Incidence Response - Organizing and Preparing the CSIRT

Unit 1 CSIRT Actions
Unit 2 CSIRT Design
Unit 3 CSIRT Development

Module 4 Crisis Management and International Standards for IR/DR/BC

Unit 1 Role of Crisis Management
Unit 2 Element of Plan to prepare for Crisis Response
Unit 3 International Standards for IR/DR/BC

There are thirteen units in this course. Each unit represent a week of study.

Presentation Schedule

The weekly activities are presented in Table 1 while the required hours of study and the activities are presented in Table 2. This will guide your study time. You may spend more time in completing each module or unit.

Table I: Weekly Activities

Week	Activity
1	Orientation and course guide
2	Module 1 Unit 1
3	Module 1 Unit 2
4	Module 1 Unit 3
5	Module 2 Unit 1
6	Module 2 Unit 2
7	Module 2 Unit 3
8	Module 2 Unit 4
9	Module 3 Unit 1
10	Module 3 Unit 2 and 3
11	Module 4 Unit 1
12	Module 4 Unit 2
13	Module 4 Unit 3
14	Revision and Response to Questionnaire
15	Examination

The activities in Table I include facilitation hours (synchronous and asynchronous), assignments, mini projects, and laboratory practical. How do you know the hours to spend on each? A guide is presented in Table 2.

Table 2: Required Minimum Hours of Study

S/N	Activity	Hour per Week	Hour per Semester
1	Synchronous Facilitation (Video Conferencing)	1	13
2	Asynchronous Facilitation (Read and respond to posts including facilitator's comment, self-study)	3	39
3	Assignments, mini-project, laboratory practical and portfolios	1	13
	Total	5	65

Assessment

Table 3 presents the mode you will be assessed.

Table 3: Assessment

S/N	Method of Assessment	Score (%)
1	Portfolios	10
2	Mini Projects with presentation	30
3	Assignments	20
4	Final Examination	40
Total		100

Portfolio

A portfolio has been created for you tagged "**My Portfolio**". With the use of Microsoft Word, state the knowledge you gained in every Module and in not more than three sentences explain how you were able to apply the knowledge to solve problems or challenges in your context or how you intend to apply the knowledge. Use this Table format:

Application of Knowledge Gained

Module	Topic	Knowledge Gained	Application of Knowledge Gained

You may be required to present your portfolio to a constituted panel.

Mini Projects with presentation

You are to work on the project according to specification. You may be required to defend your project. You will receive feedback on your project defence or after scoring. This project is different from your thesis.

Assignments

Take the assignment and click on the submission button to submit. The assignment will be scored, and you will receive a feedback.

Examination

Finally, the examination will help to test the cognitive domain. The test items will be mostly application, and evaluation test items that will lead to creation of new knowledge/idea.

How to get the Most from the Course

To get the most in this course, you:

- Need a personal laptop. The use of mobile phone only may not give you the desirable environment to work.
- Need regular and stable internet.
- Need to install the recommended software.
- Must work through the course step by step starting with the programme orientation.
- Must not plagiarise or impersonate. These are serious offences that could terminate your studentship. Plagiarism check will be used to run all your submissions.
- Must do all the assessments following given instructions.
- Must create time daily to attend to your study.

Facilitation

There will be two forms of facilitation – synchronous and asynchronous. The synchronous will be held through video conferencing according to weekly schedule. During the synchronous facilitation:

- There will be one hour of online real time contact per week making a total of 13 hours for thirteen weeks of study time.
- At the end of each video conferencing, the video will be uploaded for view at your pace.
- You are to read the course material and do other assignments as may be given before video conferencing time.
- The facilitator will concentrate on main themes.
- The facilitator will take you through the course guide in the first lecture at the start date of facilitation

For the asynchronous facilitation, your facilitator will:

- Present the theme for the week.
- Direct and summarise forum discussions.

- Coordinate activities in the platform.
- Score and grade activities when need be.
- Support you to learn. In this regard personal mails may be sent.
- Send you videos and audio lectures, and podcasts if need be.

Read all the comments and notes of your facilitator especially on your assignments, participate in forum discussions. This will give you opportunity to socialise with others in the course and build your skill for teamwork. You can raise any challenge encountered during your study. To gain the maximum benefit from course facilitation, prepare a list of questions before the synchronous session. You will learn a lot from participating actively in the discussions.

Finally, respond to the questionnaire. This will help ACETEL to know your areas of challenges and how to improve on them for the review of the course materials and lectures.

Learner Support

You will receive the following support:

- Technical Support: There will be contact number(s), email address and chatbot on the Learning Management System where you can chat or send message to get assistance and guidance any time during the course.

- 24/7 communication: You can send personal mail to your facilitator and the centre at any time of the day. You will receive answer to you mails within 24 hours. There is also opportunity for personal or group chats at any time of the day with those that are online.

- You will receive guidance and feedback on your assessments, academic progress, and receive help to resolve challenges facing your stuides.

Course Information

Course Code:	CST 808
Course Title:	Incidence Management and Disaster Recovery
Credit Unit:	2
Course Status:	Compulsory
Course Blurb:	This course covers: An Overview of Information Security and Risk Management: Overview of Risk Management, Contingency Planning and Its Components, Role of Information Security Policy in Developing Contingency Plans. Planning for Organisational Readiness; Disaster Recovery Philosophy, Principles and Planning, Contingency Plan Components, Agency response procedures and Continuity of Operations, Planning Processes, Continuity and Recovery Function, Steps of Disaster Recovery Planning Elements Required to Begin Contingency Planning, Contingency Planning Policy, Business Impact Analysis, BIA Data Collection, Budgeting for Contingency Operations. Contingency Strategies for IR/DR/BC; Data and Application Resumption, Site Resumption Strategies. Incident Response: Planning, Detection, Decision Making, Strategies, Recovery and Maintenance. Business Continuity Planning, Crisis Management, and International Standards in IR/DR/BC.
Academic Year:	2020
Semester:	Second
Course Duration:	13 weeks
Study:	65

Course Team

Course Developer:	ACETEL
Course Writers:	Dr Vivian O. Nwaocha & Dr Adebukola Onashoga
Content Editor:	Dr Ismaila Idris
Instructional Designers:	Inegbedion, Juliet O. (PhD) & Dr Lukuman Bello
Learning Technologists:	Dr Adewale Adesina & Mr Miracle David
Graphic Artist:	Mr Henry Udeh
Proofreader:	Mr Awe Olaniyan Joseph

Module 1: An Overview of Information Security and Risk Management

Module Introduction

This module provides background information that will enable you to understand the underlying principles of information security and risk management. Unit 1 presents the concept of information security, while unit 2 introduces the notion of risk management. In the end, unit 3 guides you through the action plans organisations should put in place in readiness for security breaches.

Unit 1: Concept of Information Security
Unit 2: Concept of Risk Management
Unit 3: Planning for Organisational Readiness

Unit 1: Concept of Information Security

Contents

1.0 Introduction

Normally, for organisations to succeed, they need to manage their resources effectively. *Can you think of any resource that is vital for the success of an organisation?* There are several resources that are essential for the success of an organisation, namely: human resources, capital, data, etc. Amongst these resources, data has become one of the most valuable resources required for organisational effectiveness. Meanwhile, for data to be meaningful, it has to be processed and transformed into information.

Today, information forms an essential part of the operations of any organisation. Hence, organisations need to ensure that their information is properly protected and that they maintain a high level of information security.

In this unit, you will be learning about the concept of information security and fundamental information security principles. You will equally be exposed to the common security breaches as well as the significance of information security.

2.0 Intended Learning Outcomes (ILOs)

By the end of this unit, you will be able to:

- describe the concept of Information Security
- explain Information Systems
- discuss information Security Principles.

3.0 Main Content

3.1 Concept of Information Security

The advents of the Internet and information technology have enabled organisations to handle information resourcefully, yet it has also posed new challenges. With the increasing reliance of organisations on information and information systems, it has become critical for these organisations to protect their valuable information assets from theft, loss, or misuse. Consequently, information security has gained attention in organisations across diverse business sectors.

In your terms, describe Information Security?

Information security, commonly referred to as InfoSec, is simply described as the protection of information and information systems from unauthorised access, use, disclosure, disruption, modification, or destruction to provide confidentiality, integrity and availability (CNSS, 2010). In other words, Information Security is the practice of protecting information by mitigating risks, as could be observed in figure 1.

Figure 1.1: Information Security
https://www.efrontlearning.com/blog/wp-content/uploads/2019/12/information-security-training-810x424.png

3.2 Fundamentals of Information Security

In the previous section, you were introduced to the concept of Information Security. However, to fully grasp this concept, you will need to take a closer look at some basic aspects of Information Security.

3.2.1 Information Systems

Information systems refer to interrelated components working together to gather, process, create, store and disseminate information to support decision making, coordination, control, analysis, and visualization in an organisation (Prentice.., 2012). They comprise three main components: hardware, software, and communications. Common examples of information systems include:

The main purpose of an information system is to identify and apply information security industry standards as mechanisms of protection and prevention at the three levels of protection, namely: physical, personal, and organisational levels. Therefore, while implementing information security industry standards, administrators, users, and operators of

information systems have to adhere to established policies to ensure information security within organisations (Cherdantseva & Hilton, 2013).

3.2.2 Security Breach

In simple terms, a security breach is a violation of the security policy of a system. Ordinarily, it is one of the earliest stages of a security attack by a malicious intruder. ***Can you think of any form of a security breach you have witnessed?*** Generally, a security breach ranges from low-risk to highly critical security such as:

3.2.3 Information Assurance

Information assurance is simply the act of ensuring that information is not compromised in any way when critical issues arise. Critical issues may arise.

In the next section, you will be exposed to vital information security principles as well as other aspects of information security.

3.3 Information Security Principles

At the core of the concept of information security, are three fundamental security principles, namely: Confidentiality, Integrity, and Availability. They are commonly referred to as the Confidentiality, Integrity, and Availability (CIA) triad. Hence, the CIA triad is simply described as a model designed to guide policies for information security within an organisation. Figure 1.0 shows the CIA triad.

Figure 1.2: The CIA Triad

The CIA triad forms the main objective of any security scheme. In other words, Confidentiality, Integrity, and Availability form the basic building blocks of Information Security (Chad, 2012). Moreover, the level of security required to accomplish these principles vary from one organisation to another.

3.3.1 Confidentiality

Within the context of information security, the term confidentiality is simply the act of ensuring that information is not made available or disclosed to unauthorised individuals, entities, or processes. ***Can you think of any sort of breach in confidentiality?*** Breaches of confidentiality can take a number of forms. For instance, if a laptop containing sensitive information about a company's employee is stolen, it could result in a breach of confidentiality.

3.3.2 Integrity

The second principle of information security is integrity. Integrity simply refers to the act of verifying and maintaining the accuracy and completeness of data over its entire lifecycle (). In other words, integrity implies that data cannot be modified without authorization.

Can you think of instances where the integrity is compromised?

Common instances where the integrity is compromised are as follows: when an employee accidentally or with malicious intent deletes essential files, when an Accountant modifies his salary in a payroll database.

3.3.3 Availability

The term availability refers to the act of ensuring that data is accessible the to the authorised user when it is needed. Availability is an indispensable part of a successful information security program. ***Now, can you think of any instance where the availability is compromised***? A common instance where availability is compromised is when a client on a network is unable to access services provided due to a denial-of-service attack.

3.4 Significance of Information Security

Information security performs four important roles in an organisation. These four functions are as follows:

- Information security, protects the organisation's ability to function
- It enables the safe operation of applications implemented on the organisation's information technology systems
- It protects the data that the organisation gathers and uses
- It safeguards the technological assets in use by the organisation.

Discussion

https://www.youtube.com/watch?v=xtlFO8Q2GDQ&feature=youtu.be

- *Click on the link provided to watch the video*
- *In your opinion which of the components of the CIA triad is vital for hospitals that need to send the reports of their patients via the electronic mail*
- *Post your answer in the discussion forum, giving a justification for your answer*
- *Comment on any other 3 posts of your colleagues within the context of information security*

Case Studies https://edition.cnn.com/2015/04/07/politics/how-russians-hacked-the-wh/index.html

- Click on the link provided and read the case of ''How the US thinks Russians hacked the White House
- Analyse and identify any form of security breach in the aforementioned case

4.0 Self-Assessment Exercise(s)

1. The CIA triad within the context of information security comprises of
   A. Confidentiality
   B. Integrity
   C. Auditing
   D. Availability
   Answer: C

2. Information security has been said to play a critical role in organisations. Identify these roles.
   A. the organisation's ability to function
   B. It enables the safe operation of applications implemented on the organisation's information technology systems
   C. It protects the data that the organisation gathers and uses
   D. It neglects the security of all the personnel in the organisation
   Answer: A, B, and C

5.0 Conclusion

Information Security is the practice of protecting information by mitigating risks. It is vital for the success of any organisation. At the core of the concept of information security, are three fundamental security principles, namely: Confidentiality, Integrity, and Availability.

6.0 Summary

In this unit, you have been introduced to the basic concepts of information security and the common terms associated with information security. You have equally considered information security principles, common security breaches, as well as the significance of information security.

7.0 References/Further Reading

*Schlienger, Thomas; Teufel, Stephanie (December 2003). "Information security culture - from analysis to change". South African Computer Society (SAICSIT). **2003** (31): 46–52. hdl:10520/EJC27949.*

[b] *Samonas, S.; Coss, D. (2014). "The CIA Strikes Back: Redefining Confidentiality, Integrity and Availability in Security". Journal of Information System Security. **10** (3): 21–45. Archived from the original on 2018-09-22. Retrieved 2018-01-25.*

^ *"Gartner Says Digital Disruptors Are Impacting All Industries; Digital KPIs Are Crucial to Measuring Success". Gartner. 2 October 2017. Retrieved 25 January 2018.*

^ *"Gartner Survey Shows 42 Percent of CEOs Have Begun Digital Business Transformation". Gartner. 24 April 2017. Retrieved 25 January 2018.*

^ *"Information Security Qualifications Fact Sheet" (PDF). IT Governance. Retrieved 16 March 2018.*

^ *Stewart, James (2012). CISSP Study Guide. Canada: John Wiley & Sons, Inc. pp. 255–257. ISBN 978-1-118-31417-3.*

*He, Ying (December 1, 2017). "Challenges of Information Security Incident Learning: An Industrial Case Study in a Chinese Healthcare Organisation". Informatics for Health and Social Care. **42**: 394–395 – via Ebscohost*

Unit 2: Concept of Risk Management

Contents

1.0 Introduction

Organisations are prone to various kinds of risks that have the potential to hinder the attainment of their organisational goal. Some risks, if not properly managed, can lead an organisation into bankruptcy or even extinction in extreme cases. Hence, effective risk management is vital for the subsistence of any organisation.

In this unit, you will be introduced to the concept of risk management for an organisation. You will equally be guided through the steps for preparing an Information Security Risk Management Programme (ISRM).

2.0 Intended Learning Outcomes (ILOs)

By the end of this unit, you will be able to:

- describe an Overview of Risk Management
- discuss Risk Management in Organisations
- identify the Risk Management Processes
- describe Risk Assessment.

3.0 Main Content

3.1 An Overview of Organisational Risk

Can you describe the term "risk" and it's impact on an organisation?

In simple terms, risk is an expression of the likelihood that an expected goal will not be achieved as a consequence of uncertainty. According to the NIST (National Institute of Standard and Technology) Special Publication 800-30:

> "*Risk* is a measure of the extent to which an entity is threatened by a potential circumstance or event, and is typically a function of: (i) the adverse impacts that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence." (Joint Task Force Transformation Initiative, 2012).

ISO 31000 describes risk as to the deviation of organisational objectives from their expected values caused by uncertainty in the organisation process. Uncertainty, in this case, refers to inadequate information about an event, its consequence, or its likelihood of occurrence. In other words, you know you are facing a risk when you are in a situation that makes you uncertain about your chances of realising your objectives and when you can realise them.

From the description above, how will you classify the organisatiional risks?

3.2 Classes of Organisational Risks

Risks come from different sources and affect organisational objectives in different ways. Broadly, organisational risks can be classified as either organisation risk or financial risk. Now, you will learn about the two classes of risk and how they may affect your organisation.

3.2.1 Organisational Risk

Organisation risk is a broad class of risk, which is associated with all circumstances that can lower the likelihood of an organisation meeting its organisation goals such as profit, growth, or even continuity. It encompasses all internal (such as manager's strategic decisions) and external (such as competition, economy, consumer preference, operation costs, government regulations, etc.) factors that have the potential to cause serious profit loss to an organisation or even endanger its existence.

Since organisation risk can be due to various factors, it exists in different types, each of which impairs organisations successes in its special way. Now, let us have a look at the major types of organisation risk.

3.2.1.1 Strategic Risk

This is the type of organisation risk that arises from the likelihood that an organisation's organisation strategy will become less effective due to events such as the entrance of strong competitors into the market, technological advancement, change in customers' preference, etc. thereby seeing the organisation struggling to reach its goals. As a top manager, you must agree with the reality that the highly rewarding organisation strategy that earns you a boom today can suddenly become obsolete due to some market dynamics. You must be prepared to adapt appropriately to such dynamics to save your organisation from going into extinction.

3.2.1.2 Operational Risk

This is a type of organisation risk that is associated with the likelihood of the failure of some organisation processes due to human actions and errors, breakdown of some critical machines, or any event that can disrupt some critical organisation activities. It covers all kinds of risks incurred from the organisation operations due to events such as criminal activities, infrastructural failure, human errors/mistakes, product defects, hacking, data theft, bribery, tax evasion, etc. Operational risks can have severe impacts on an organisation, including reputational damage, regulatory overhead, serious loss, or even extinction of the organisation.

3.2.1.3 . Compliance Risk

This is a type of organisation risk associated with an organisation's compliance or non-compliance with the laws and regulations that apply to its organisation operations. When an organisation operates an organisation in a government-regulated industry such as oil and gas, telecommunication, banking, healthcare, etc., there is the likelihood that a government or regulatory body will amend existing laws and regulations or introduce a new one entirely. Compliance or non-compliance with such changes may pose some risk to your organisation.

3.2.1.4 Reputational Risk

This is a type of organisation risk that may come as a supplementary consequence of some types of organisation risk or any event that can damage the reputation of an organisation. Just like humans, every organisation has a name and brand to protect, and anything that has the potential to give a bad impression about that brand poses a reputation risk on the organisation.

Reputation risk can have a grave consequence on the survival of an organisation. It can lead to a drastic drop in customer base and loyalty, sudden withdrawal of sponsors, partners and supporters, the resignation of highly competent employees and difficulty in finding replacements, etc.

3.2.1.5 Financial Risk

Financial risk is the type of risk associated with the likelihood that an organisation will have a shortage of cash flow to meet its financial obligations. Any situation that makes the cash inflow of an organisation consistently less than the cash outflow exposes it to financial risk. A time may come when the organisation will fail to meet financial obligations to stakeholders such as employees, creditors, suppliers, investors, etc.

Can you think of two events that can expose an organisation to financial risk?

Financial risk usually arises as a result of instabilities, losses in the financial market or movements in stock prices, currencies, high-interest rates on loans, failure of debtors to back, etc. It can even be a supplementary consequence of some other types of risk.

3.2 Organisational Risk Management

In the previous section, you learned about the basic aspects of risks. This unit will take you through the process of recognising and dealing with these unavoidable risks in an organisation.

According to the International Standards Organisation, risk management refers to a set of coordinated activities aimed at directing and controlling an organisation concerning risk. Figure 2.0 illustrates an internationally recognised model of the risk management process defined in ISO 31000. you can adapt this model to an organisation to develop a risk management programme for any organisation.

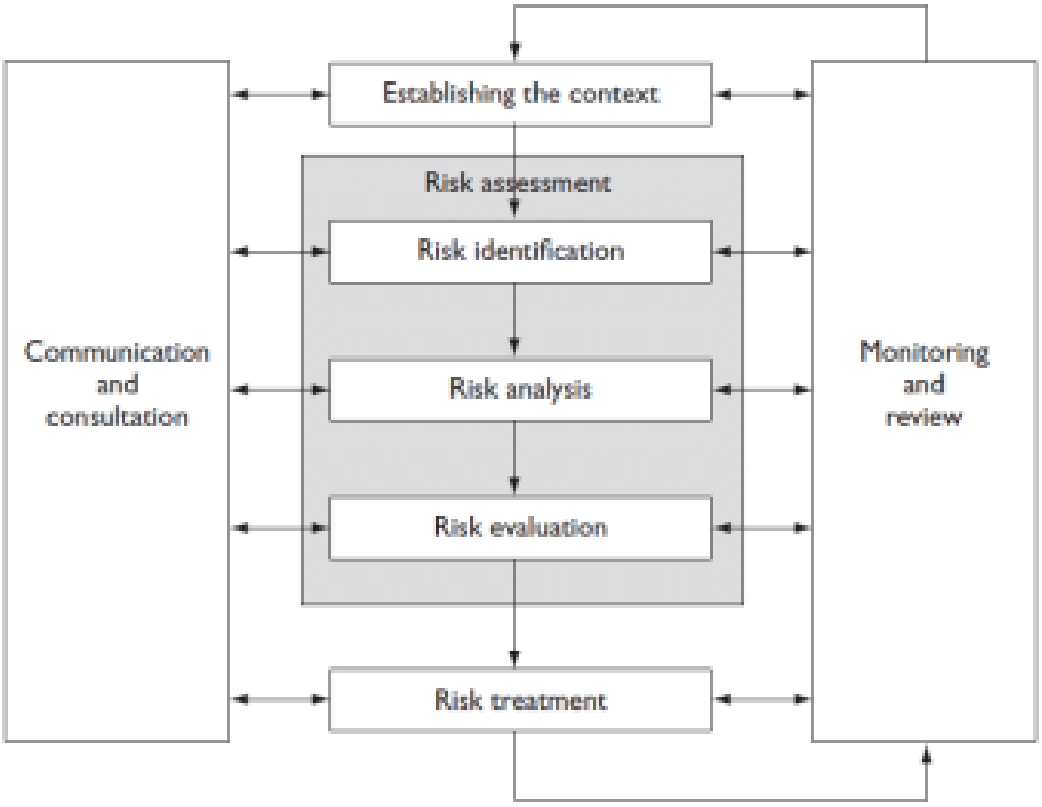


Figure 1.3: Risk Management Process [Adapted from ISO 31000]

From Figure 3, risk assessment and risk treatment are at the core of the risk management process. It equally depicts different elements of risk assessment. While the diagram gives overviews of the other components of the risk management process, it is recommended that you consult the ISO 31000 documentation to study them in more significant details.

Can you think of the main goal of risk assessment in the risk management process?

3.3 Risk Assessment

Risk assessment, as an essential element of risk management, describes a systematic way of determining:

a. The events that can threaten the objectives of an organisation at different levels
b. Their likelihood of occurrence and the severities of their consequences when they occur
c. The ways to reduce the likelihood of such occurrences and mitigate their consequences
d. Whether the consequences can be reasonably and practicably accommodated in the organisation process or not.

Ultimately, risk assessment serves as tool support for evidence-based and well-informed strategic decisions with regards to organisational risks.

The risk assessment process comprises three sequential sub-processes namely: risk identification, risk analysis, and risk evaluation. We will briefly introduce the roles of each sub-process in the rest of this sub-section.

3.3.1 Risk Identification

Risk identification is the first stage in the risk assessment process, which is aimed at compiling a comprehensive list of events that can affect (positively/negatively) the chances of achieving organisational objectives, their causes, areas of impact and potential consequences.

In addition to applying suitable techniques, comprehensive identification of risks requires the service of personnel with appropriate knowledge of the context as well as relevant and up-to-date background information in the identification process. Examples of risk identification methods and techniques include:

- Brainstorming
- Delphi methodology
- Evidence-based methods such as reviews of historical data
- Checklist
- Inductive reasoning techniques; e.g., HAZOP

You are encouraged to consult ISO 3010 and ISO/IEC 31010 documentation for detailed descriptions of these methods and techniques and many more.

3.3.2 Risk Analysis

At this stage, each of the risks identified in the previous stage will be subjected to rigorous examination to quantitatively or qualitatively determine the severity of its consequences, likelihood, and any other relevant factor. A properly executed risk analysis process should provide incontrovertible evidence to rank the risks and to prioritise and select appropriate risk treatment options.

There are several techniques for undertaking risk analysis. Your choice of technique may be determined by factors such as the required degree of details, the purpose of the analysis, the nature and amount of data available for investigation, etc. Each technique is classified under one of two categories:

- Qualitative method
- Quantitative method.

Some techniques that are suitable for situations that fall between these two methods are referred to as semi-quantitative methods.

Note that risk analysis methods are also called risk assessment methods in the literature. This is because

- Risk analysis is a core component of risk assessment and
- Some risk analysis techniques are also used for risk identification and risk evaluation.

We will give you overviews of qualitative and quantitative methods in this unit. We recommend that you consult the ISO/IEC 31010 standard documentation for detailed coverage of the various techniques, including their strengths and weaknesses.

3.1.1.1 . Qualitative Method

These methods cover the analysis techniques that do not numerically express the likelihood of occurrence of events and their consequences. They are expressed verbally with specialised quantifiers such as rarely, likely, frequently, high, medium, low, etc. In this case, decisions are based on personal judgements, experience, and intuition.

Examples of techniques in this method include:

- Brainstorming
- Delphi technique (Judgment of specialists and experts)
- Structured interviews
- SWOT (Strength, Weakness, Opportunity, and Threats) analysis
- Questionnaire
- HAZOP (Hazard and Operability) study
- SWIFT (Structured "What if" Technique).

3.1.1.2 . Quantitative Methods

These methods comprise all analysis techniques that use numeric measures express likelihoods of occurrence of events, their consequences, and the level of risk associated with the affected organisation entity.

They are usually preferred in situations where:

- There is sufficient data to support numeric estimation of likelihoods and consequences and we can transform available information into numeric values.
- There is a high level of uncertainty, and the consequence of wrongdoing can be very severe.

Quantitative methods usually require formal (mathematical) models of the risk for rigorous analysis to obtain the required level of confidence in the result.

Examples of techniques in this method include:

- Computer simulation
- Monte Carlo analysis
- Bayesian analysis
- Markov analysis
- FMEA (Failure Mode and Effect Analysis).

3.3.3 Risk Evaluation

Risk evaluation, the last stage of risk assessment, is the process of comparing the results of the risk analysis stage with the risk criteria established in the context of the risk management process (see Figure 1). The result of this comparison will be used to determine whether the consequence of the risk is as low as reasonably practicable (ALARP) and hence tolerable in the organisation process or the risk needs to be treated in the next stage of the risk management process.

 Scenario

A. The call credit sales organisation in the Gambia

Many people have made fortunes by selling call credits either in the form of scratch cards or printed slips with the emergence GSM about two decades ago. Recently, commercial banks have entered the call credit organisation, **as super competitors**, **allowing their customers to buy call credits with ease using USSD codes on their phones, anywhere, anytime.** This poses a high risk to the survival of roadside call credit sellers as their strategy has been rendered obsolete by the superior strategy of the banks. Identify this risk?

 Discussion

- According to the International Standards Organisation, risk management refers to a set of coordinated activities aimed at directing and controlling an organisation concerning risk. Furthermore, there are two main risk analysis techniques.
- *In your opinion which of the techniques will be suitable for SWOT analysis?*
- *Post your answer in the discussion forum, giving a justification for your answer.*
- *Comment on any other three posts of your colleagues within the context of information security.*

4.0 Self-Assessment Exercise(s)

1. _____ is an expression of the likelihood that an expected goal will not be achieved as a consequence of an uncertainty
   a. Scan
   b. Risk
   c. Threat
   d. Integrity
   Answer: b

2. Which of the following is not a component of risk assessment?
   a. Risk evaluation
   b. Risk treatment
   c. Risk analysis
   d. Risk identification

   A. i and ii
   B. ii and iv
   C. i, ii, and iv
   D. ii and iii

   Answer: *b and d*.

5.0 Conclusion

Organisations are almost always prone to risks. Therefore, the ability to recognise and manage risks of systems and data is essential for an organisation's success. However, to effectively manage organisational risks and protect critical assets and effectively respond to emerging cyber threats, it is essential to develop an Information Security Risk Management programme.

6.0 Summary

You have learned from this unit that organisational risk is any uncertain event or situation that has the potential to alter the outcome of an organisation activity from its expected value. You also learned different categories of risk and their potential impacts on the realisation of organisational objectives and the process to manage risk within the scope of your organisation and the context of your organisation activities. You will

build on these skills in the next unit to plan and implement the strategies that give your organisation the resilience to survive disruptive incidents.

7.0 References/Further Reading

Bowen, P., Hash, J., & Wilson, M. (2006). *SP 800-100. Information Security Handbook: A Guide for Managers*. Retrieved from *https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-100.pdf*

Course note on Crisis Management Management Study Guide https://www.managementstudyguide.com/crisis-management.htm

Gitanjali Maria (2019). How to Create a Cybersecurity Crisis Management Plan in 5 Steps.Published by GetApp, Jul 9, 2019. Downloaded from https://lab.getapp.com/cybersecurity-crisis-management-plan/

30.Esbensen. L. H. and Krisciunas (2008) Crisis Management & Information Technology. Master Thesis, Submitted to Lund University, June, 2008.

Marcus K. G. Adomey (2016). Introduction to Computer Security Incident Response Team (CSIRT). An Article downloaded from https://www.managementstudyguide.com/crisis-management-team.htm

Unit 3: Planning for Organisational Readiness

Contents

1.0 Introduction

This unit guides you through the action plans organisations should put in place to be able to manage risks effectively.

2.0 Intended Learning Outcomes (ILOs)

By the end of this unit, you will be able to:

- describe the Readiness for Security Breaches
- explain Proactive Strategy for Organisational Risk Management
- manage risks in an organisation.

3.0 Main Content

3.1 Organisational Readiness for Security Breaches

The constant advancement in technology has brought about the rapid access to and diffusion of information from one organisation to another. Nevertheless, this has equally fueled the prevalence of a plethora of security incidents. No matter how hard organisations try, there is no guarantee that the organisation's network will be immune to incidents.

Consequently, for organisations to stay up-to-date, they are to develop and improve practices to mitigate risks. Ultimately, organisations must proactively prepare for security breaches to minimise potential risks and respond to incidents effectively.

How can organisations prepare for security breaches to minimise potential risks and respond to incidents effectively?

3.2 Proactive Strategy for Organisational Risk Management

For organisations to effectively minimise potential risks and respond to incidents, they must be preemptive in planning for security breaches.

Organisations need to develop a proactive approach that will discover potential security threats and prevent any imminent incident from occurring.
In the next sub-section, you will learn about these strategies.

3.2.1 Steps in Planning for Organisational Risk Management

The practical steps organisations must take to manage risks are outlined in this sub-section proactively

Step I

Take an inventory of authorised software, devices, and other assets

Step II

Enforce security configurations and policies

Step III

Train personnel of the organisation

Step IV

Deploy low footprint defense systems

Step V

Undertake Continuous Assessment and Prompt Response before Incidents

 Discussion

https://www.business.com//articles/5- key- steps-toward-a-proactive-approach-to-it-security

- *Click on the link provided read the article*
- *In your opinion which of the steps is useful for preventing unauthorised access to a network?*
- *Post your answer in the discussion forum, giving a justification for your answer*
- *Comment on any other 4 posts of your colleagues within the context of mitigating security breaches*
- *Digital Author , please ensure that a student is only able to view other student's posts only after sending out a post*

4.0 Self-Assessment Exercise(s)

1. Outline the practical steps to be undertaken to manage risks in organisations effectively?

Step I

Take an inventory of authorised software, devices, and other assets

Step II

Enforce security configurations and policies

Step III

Train personnel of the organisation

Step IV

Deploy low footprint defense systems

Step V

Undertake Continuous Assessment and Prompt Response before Incidents

5.0 Conclusion

Taking a proactive approach to security is the best means of countering security breaches. Every organisation should develop a proactive security program to ensure that when an incident occurs, it is handled efficiently.

6.0 Summary

In this unit, you have learned the proactive strategy organisations should adopt to mitigate security breaches and manage risks effectively. You have equally learned about the practical steps to be adopted for effective organisational risk management.

7.0 References/Further Reading

Baybutt. P. (2003). A Scenario-based Approach for Industrial Cyber Security Vulnerability Analysis. A paper downloaded from:http://www. primatech. com/images/docs/paper_a_scenario_based_approach_for_industrial_cyber_security_vulnerability_analysis.pdf

Diane Chinn (2019). The purpose of contingency planning. Retrieved from smallbusiness.chron.com/

Incident Handling Step-by-Step and Computer Crime Investigation: Book 1 CERT.

Jason T. Luttgens and Matthew Pepe, Incident Response & Computer Forensics,(3rd Edition), McGraw-Hill.

Kouchakji, J. (2016). Pentesting vs Vulnerability in Typical Application Scenarios, An Article Published by Cybrary, downloaded from https://www.cybrary.it/0p3n/pentesting-vs-vulnerability-assessment-typical-application-scenarios/

Leighton R. Johnson III, Computer Incident Response and Forensics Team Management, 2014

Michael E. Whitman, Herbert J. Mattord, and Andrew Green, Principles of Incident Response and Disaster Recovery.

Study.Com, Cybersecurity Contingency Plans: Purpose, Development & Implementation. Chapter 13, Lesson 2.

Module 2: Contingency Strategy for IR/DR/BC

Module Introduction

This module presents the contingency strategy for ensuring business sustainability. While units 1 and 2 cover the contingency planning and incidence response respectively, units 3 and 4 present the schemes for disaster recovery and business continuity in turn.

Unit 1 Contingency Planning
Unit 2 Incidence Response
Unit 3 Disaster Recovery
Unit 4 Business Continuity

Unit 1 Contingency Planning

Contents

1.0 Introduction

Studies have shown that there is no system that is entirely secure. Therefore, irrespective of how much care is put into operating and testing the system, failure in that system is still very likely. For this reason,

procedures are required that will enable organisations to plan for the unexpected and thus continue essential functions if information technology support is interrupted.

This unit presents the planning for unexpected incidents in the event where the use of technology is disrupted, and business operations are about to come to a halt.

2.0 Intended Learning Outcomes (ILOs)

By the end of this unit, you will be able to:

- describe the concept of contingency planning
- establish the relationship in contingency planning
- explain the techniques used for data and application backup and recovery.

3.0 Main Content

3.1 Overview of Contingency Planning

What do you understand by Contingency? Generally, contingency is anything that occurs outside the range of normal operations that may adversely affect an organisation's ability to operate.

Contingency Planning (CP) simply refers to the process of planning for unanticipated events. It is a blueprint on how to deal with unusual events (Diane, 2019).

NIST describes the need for contingency planning as follows:
"These procedures (contingency plans), business interruption plans, and continuity of operations plan) should be coordinated with the backup, contingency, and recovery plans of any general support systems, including networks used by the application. The contingency plans should ensure that interfacing systems are identified and contingency/disaster planning coordinated."

Consequently, a cyber security contingency plan is a written risk management document that provides instructions, recommendations, and considerations for an organisation on how to recover their IT Services and data in the event of a security breach, disaster, or system disruption.

Through contingency planning, organisational planners position their organisations to prepare for, detect, respond to, and recover from incidents that threaten the security of the organisation's information and assets.

Ultimately, the main purpose of contingency planning is to restore businesses to the normal modes of operation with minimum cost and disruption to business activities after an unexpected event.

The main objective of a cyber security contingency plan is to protect data and assets after a security breach or disaster has occurred. Hence, a cyber security contingency plan will include the following:

- Steps on protective measures
- Steps on ways to prevent future attacks, breaches or losses
- Approaches on how to collect or preserve evidence
- Approaches on how to develop root cause analysis

3.2 Components of Contingency Planning

Essentially, contingency planning entails a business impact analysis which comprises of three planning processes namely:

- Incident Response Planning (IRP)
- Disaster Recovery Planning (DRP)
- Business Continuity Planning (BCP)

These three elements can be hierarchically represented as depicted in Figure 3.2

To ensure continuity across all of the CP processes during the planning process, contingency planners should:

- Identify the mission-or business-critical functions.
- Identify the resources that support critical functions.
- Anticipate potential
- Select contingency planning strategies.
- Implement the selected strategy
- Test and revise contingency plans

Four teams of individuals are involved in contingency planning and contingency operations:

- The CP team
- The incident recovery (IR) team.
- The disaster recovery (DR) team.
- The business continuity plan (BC) team

Now that we have identified the key components of contingency planning will take a closer look at each of these elements to understand how they relate to each other.

3.2.1 Relationship among the Components of Contingency Planning

In the previous section, we learned that there are three components to contingency planning. Now we will consider these components and their specific roles and how they relate to each other.

The three components of contingency planning and their corresponding roles are as follows:

- Incidence Response Planning (IRP)
  Focuses on the response to an incident

- Disaster Recovery Planning (DRP)
  Focuses on recovering operations

- Business Continuity Planning (BCP)
  Focuses on a backup plan establish alternatives until the system is stabilized.

  So how do these three components, IRP, DRP, and BCP, relate to each other?
- IRP: The IRP is a detailed set of processes and procedures that anticipate, detect and mitigate the impact of unexpected events (contingencies), that might compromise information assets

- DRP: The DRP is a preparation from recovery from a disaster. An incident can be classified as a disaster when an organisation is unable to contain or control the impact of an incident and is unable to recover quickly

- BCP: The BCP is a plan for continuity of critical business functions when a disaster occurs. A good number of BCP are executed parallel to DRP when a disaster is long term and requires the complex restoration of security information assets.
  On the whole, all three components entail planning for the unexpected, which in turn is contingency planning.

3.3 Overview of Data Backup

What do you understand by data backup in Information Technology? Within the context of Information Technology, data backup is simply a copy of computer data taken and stored elsewhere so that it may be used to restore the original after a data loss event. Therefore, backups can be used to

recover data after its loss through data deletion or corruption or to recover data from an earlier time.

Generally, data backup describes the process of creating and storing copies of data that can be used to protect organisations against data loss.

The main purpose of data backup is to create a copy of data that can be recovered in the event of a primary failure.

3.3 Techniques used for Data Backup

Even though data has become one of the most valuable resources of the Century, yet data loss can occur at any time and for all kinds of reasons such as crashes, malware, physical damage, theft, or basic user error. Therefore, data backup is a practical thing to get into the habit of doing. Besides, data backup is vital to the protection and success of businesses. Whether your data is stored on-premises or in the cloud, it is important to protect it.

Although, there are several options available for those seeking to back up their data, yet each option has its peculiar pros and cons. In this section, we will consider some of three common methods of backing up data namely:

- Full Backup
- Differential Backup
- Incremental Backup

We will now consider each of these techniques for data backup.

3.4.1 Full Backup

In the full backup technique, data is backed up to a target drive or disk each time data is backed up. In other words, all documents and files are stored in one file.

Merit:

- It is easier and faster to create full backups than differential or incremental backups
- In the full backup strategy, only one file needs to be restored. For this reason, it is easier to manage full backups.

Demerit:

The main drawback of the full backup strategy is that it requires more space than a differential or incremental backup

3.4.2 Differential Backup

In the differential backup technique, only the changed or new data since the last full backup is backed up. Hence, the initial full backup is required to clearly identify both the new as well as the modified documents.

Merit:
A regular differential backup requires less space than a full backup.

Demerit:

- The restoration of a differential backup is much slower than a full backup
- A differential backup requires two files. Therefore, managing a differential backup is more difficult than managing a full backup.

3.4.3 Incremental Backup

An incremental backup backs up new or changed documents as well as a prior incremental backup as opposed to the initial full backup. Only the first ever incremental backup is based on the initial 'base' backup.

Merit:
The main merit of this backup technique is that it requires much less space than a full backup or differential backup.

Demerit:

- The main drawback of the incremental backup is that it is slower than a full backup or differential backup
- Managing the incremental backup is more complex as all files from a backup 'chain' are required for a restoration.

3.4 Repository for Backup Operations

Generally, a backup technique requires an information repository that aggregates backups of data sources. The backup strategy actually determines how and when each piece of removable storage is used for backup operation and how long it is retained once it has backup data stored on it.

In this section, we'd consider the common repositories for backup operations namely:

- Printing
- USB Stick
- External hard drive
- Cloud storage.

Now let's take a closer look at each of the storages for data backup.

.

3.4.1 Printing

Printing is the data storage technique that provides a hard copy of documents. Figure 1 depicts the printing technique.

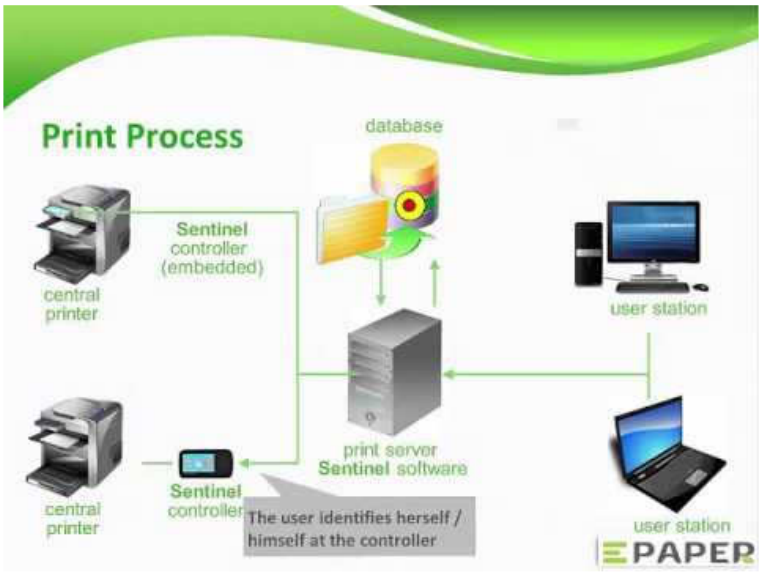


Figure 2.1: The Print Process

We will now consider the benefits and drawbacks of backing up data through printing.

S/N	Device for Data Storage	Benefits	Drawbacks
1	Printing	i. This sort of backup is not affected by hardware outages ii. It is impossible for hackers to access data on print.	i. It is not possible to store some files through printing ii. It is awkward to manage files stored in this mode iii. It is not practical for large documents iv. It is less environmentally

3.4.2 USB Sticks

USB sticks are small, cheap, portable, and convenient devices for data storage.

Figure 2.2 shows a USB stick

Figure 2.2: USB stick

Can you state at any benefit and drawback of the USB stick?

S/N	Device for data storage	Benefits	Drawbacks
1	USB Stick	i. Extremely portable ii. Very cheap. iii. Data can easily be transferred to other sources	i. USB sticks can easily be lost because of their size ii. There are concerns over the longevity of the read/write cycle of USB sticks

3.4.3 External Hard Drive

These are hard drives that reside outside your computer, meaning they can be plugged into other sources documents.

Figure 3 depicts the external hard drive

Figure 2.3: An External Hard Drive

We will now consider the benefits and drawbacks of backing up data in an external hard drive:

S/N	Device for Data Storage	Benefits	Drawbacks
1	External Hard Drive	.It is relatively cheap .It has plenty of storage space for larger files.	.Files stored in external hard drives are more prone to being lost.

3.4.4 Cloud Storage

There are several third party cloud storage options around that are free, paid for, namely: iCloud, Dropbox, Google Drive, OneDrive etc.

Figure 4 depicts a form of cloud storage: Dropbox

Welivesecurity.com/2015/03/31/6/-ways-to-backup-your-data

Figure 2.4: Dropbox

We will now consider the benefits and drawbacks of backing up data in a cloud.

S/N	Device for Data Storage	Benefits	Drawbacks
1	Cloud	.It can be done automatically .It usually has a certain volume of space free	.It requires an internet connection to work .It is difficult to account for security breaches in the cloud . The third-party offering the service is not obliged to provide the service forever

 Discussion **Scenario**

Skyline hotels is an international hotel that has a wide range of both local and foreign guests. On Saturday, December 7, 2019, one of the foreign guests, arriving from New York is trailed by armed bandits from the airport to Skyline hotel. Prior to their arrival, an accomplice cuts off power supply and disables the server that records video surveillance at the gate. The bandits successfully stop the guest at the gate and make away with his briefcase containing 4000 dollars, passport, etc. The police arrive after this incident and request for the video surveillance but unfortunately discovered that it was disabled during the operation,

What sort of contingency plan should have been put in place to ensure that surveillance at the Skyline gate is not interrupted?

Answer:

i. An alternative plan should be made, such that the surveillance is powered by solar panels thus ensuring that not disabled due to loss of power or other failures,

ii. The area should be monitored by assigned personnel until the backup analog camera and recorder can be put into service. The backup equipment is stored in room enter room identification.

4.0 Self-Assessment Exercise(s)

1. Identify the three main components of Contingency Planning

a) Incidence Response Planning
b) Data Recovery Planning
c) Disaster Recovery Planning
d) Business Continuity Planning

Answer: b

2. One of the drawbacks of using cloud storage is

b. It is difficult to account for security breaches in the cloud
c. It is relatively cheap
d. It cannot be done automatically
e. It has plenty of storage space for larger files.

5.0 Conclusion

Contingency planning entails preparing for, detecting, reacting to, and recovering from events that threaten the security of information resources and assets. Those that have adequately developed, maintained, and exercised their contingency plans will survive. Taking a proactive approach to security is the best means of countering security breaches. Every organisation should develop a nces/proactive security program to ensure that when an incident occurs, it is handled efficiently.

6.0 Summary

In this unit, you have learned about contingency planning, the components of contingency planning, and the relationship amongst these components. You have equally learned about the techniques used for data and application storage and recovery.

7.0 RefereFurther Readings

Diane Chinn (2019). The purpose of contingency planning. Retrieved from smallbusiness.chron.com/

Hotchkiss, Stuart. Business Continuity Management : In Practice, British Informatics Society Limited, 2010. ProQuest Ebook Central, https://ebookcentral.proquest.com/lib/pensu/detail.action?docID=634527.

Jason T. Luttgens and Matthew Pepe, Incident Response & Computer Forensics,(3rd Edition), McGraw-Hill.

^ *"The Disaster Recovery Plan". Sans Institute. Retrieved 7 February 2012.*

Study.Com, Cybersecurity Contingency Plans: Purpose, Development & Implementation. Chapter 13, Lesson 2.

Unit 2: Incidence Response

Contents

1.0 Introduction

To respond to the numerous security breaches, effective incidence response plans are required. Although security breaches are nearly always unavoidable, yet approaches and methods may be employed to minimise the impact and consequence.

2.0 Intended Learning Outcomes (ILOs)

By the end of this unit, you will be able to:

- describe an incident response
- develop an incident response plan
- plan for an incidence response that will solve a real-life problem.

3.0 Main Content

3.1 Incident Response (IR)

Once an actual incident has been confirmed and properly classified, the IR team moves from the detection phase to the reaction phase.

Thus, in the incident response phase, several action steps taken by the IR team and others must occur quickly and may occur concurrently.

An Incident Response comprises of some steps, Identify some of these steps.

Steps of Incident Response (IR)
These steps include notification of key personnel, the assignment of tasks, and documentation of the incident.

Notification of key Personnel
As soon as the IR team determines that an incident is in progress, the right people must be immediately notified in the right order.
An alert roster is a document containing contact information on the individuals to be notified in the event of an actual incident.
As soon as an incident has been confirmed and the notification process is underway, the team should begin to document it.
The documentation should record the who, what, when, why, and how of each action taken, and if they were effective.
It can also prove the organisaation did everything possible to deter the spread of the incident.

3.2 Incident Response Planning

The incident response plan (IRP) is a detailed set of processes and procedures that anticipate, detect, and mitigate the impact of an unexpected event that might compromise information resources and assets.

An incident occurs when an attack (natural or human-made) impacts information resources and assets. Whether through actual damage or the act of successfully attacking.

The IRP is usually activated when an incident causes minimal damage-according to criteria set in advance by the organisation-with little or no disruption to business operations.

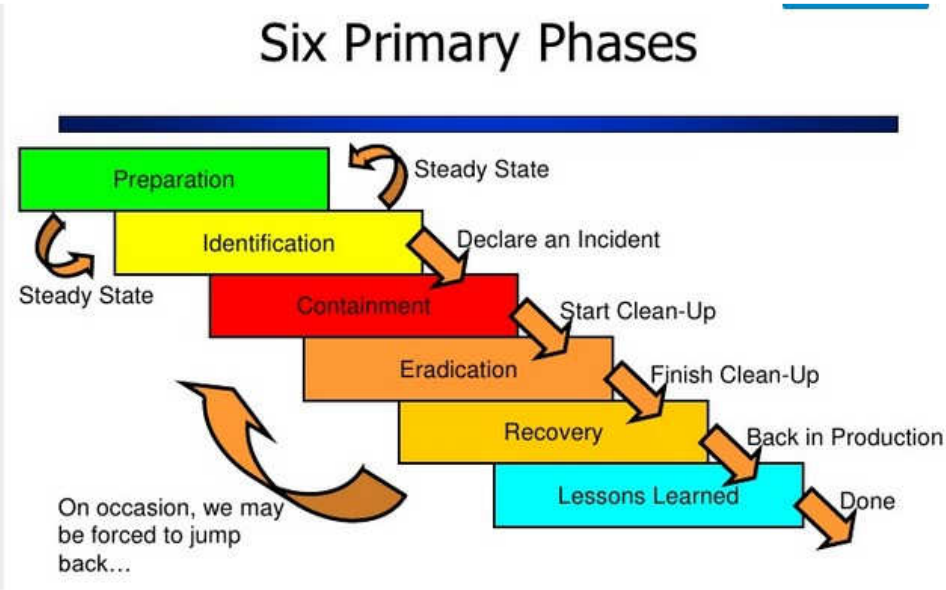


Figure 2.5: Incident Response Plan
https://3.bp.blogspot.com/-sixe4viwJGo/WeCA4q_OjBI/AAAAAAAACWo/O67brIpalK0qf2jwhGMw82J1TmGtb9m5QCK4BGAYYCw/s1600/AAEAAQAAAAAAAAYOAAAAJGQ2OGFlNjYyLTg3YjMtNDZiZi1hN2I0LTA2MTY1NGQ5ZWNlMw.jpg

When a threat becomes a valid attack, it is classified as an information security incident if:

- It is directed against information assets
- It has a realistic chance of success
- It threatens the confidentiality, integrity, or availability of information resources and assets

It is important to understand that IR is a reactive measure, not a preventative one.

3.2.1 Steps in Creating an Incident Response Plan

The steps for creating a useful Incident Response Plan – 'are as follows:

1. Planning
2. Testing (a) Simulation
3. Testing (a) Parallel
4. Testing (a) Full Interruption.

Now let us take a closer look at each of the steps.

1. Planning

1. Distribute the Incident Response Plan to each team member
2. Allow time for each member to evaluate the plan based on their role

3. Walk-through each member's steps at a joint conference following a 'round-table' style of discussion of actions at each juncture.

2. Testing (a) – Simulation

1. Put team members in isolation and allow them to simulate their steps.
2. Stop testing in places where testing would affect normal business operations (for example take down server X).

3. Testing (b) – Parallel

1. Team members simulate their steps in tandem as if a real incident is on-going
2. Stop testing in places where testing would affect normal business operations (for example take down server X).

4. Testing (c) – Full Interruption

1. Team members simulate their steps in tandem as if a real incident is on-going
2. Keep testing and simulate all procedures including those with denial/interruption of service
3. Attempt to restore data from previous backups.

Clearly, the third method of testing is the most realistic and effective approach. However, this may be too risky of a method for some businesses, or testing time may be a deciding factor.

 Discussion

Based on the lessons learned from the unit on Incidence Response, can you deliberate on the statement, "Incident Response is a reactive measure?" Comment on at least one post of your colleagues, justifying your answer.

 Case Studies Click on the following link on an incidence response plan.
https://www.cmu.edu/iso/governance/procedures/docs/incidentresponseplan1.0.pdf

Identify with the aid of an illustrative diagram, all the phases for a typical incident process

4.0 Self-Assessment Exercise(s)

1. Incident Response (IR) comprises of the following steps except:
a) notification of key personnel
b) assignment of tasks
c) prevention of the incident
d) documentation of the incident
Answer: c

2. Distributing the Incident Response Plan to each team member is the characteristic of which of the steps of creating a useful Incident Recovery Plan?

a) Testing (a) Parallel
b) Planning
c) Testing (a) Full Interruption
d) Testing (a) Simulation
Answer: b

5.0 Conclusion

In order to respond to the numerous security breaches, experienced and capable computer security incidence responders are highly sought after, and computer incidence response career paths have matured over time. Nevertheless, security breaches may be inevitable, but approaches and methods may be employed to minimise the impact and consequence

6.0 Summary

In this unit, you have learned about the incident response plan and the processes involved in incidence response planning. You have equally learned how to prepare an incident response plan for resolving a real-life scenario.

7.0 References/Further Reading

Angelos Chritidis (2018). How to mitigate the Risk of Cyber security through Contingency Planning. Retrieved from: http://metin-mitchell.com/how-to-mitigate-the-risks-of-cyber-security-through-contingency-planning/

Baybutt. P. (2003) A Scenario-based Approach for Industrial Cyber Security Vulnerability Analysis. A paper downlaoded from: http://www.primatech.com/images/docs/paper_a_scenario_based_approach_for_industrial_cyber_security_vulnerability_analysis.pdf

kouchakji, J. (2016) Pentesting vs Vulnerability in Typical Application Scenarios, An Article Published by Cybrary, downloaded from https://www.cybrary.it/0p3n/pentesting-vs-vulnerability-assessment-typical-application-scenarios/

Leighton R. Johnson III, Computer Incident Response and Forensics Team Management*, 2014.*

Proffitt. T. (2007). Creating and Managing an Incident Response Team for a Large Company. A Paper from the Information Security Reading Room, SANS organisation. Accessed from https://www.sans.org/reading-room/whitepapers/incident/creating-managing-incident-response-team-large-company-1821

Unit 3: Disaster Recovery

Contents

1.0 Introduction

Basically, most business processes are built on technologies that rely heavily on data to function. Organisations often consider such data their vital assets that must not be lost in any circumstance. Serious organisations must, therefore, be aware of incidents that have the potential to cause damage to their data to make robust plans to recover from the impacts of such disastrous incidents if and when they occur.

In this unit, you will learn how to perform the data recovery plans for lost data of an organisation after any type of disaster. To achieve this, this unit will take you through the techniques, guiding principles, and best practices in disaster recovery planning.

2.0 Intended Learning Outcomes (ILOs)

By the end of this unit, you will be able to:

- describe Disaster Recovery Concepts
- explain the principles of Disaster Recovery
- create techniques for disaster recovery.

3.0 Main Content

3.1 Overview of Disaster Recovery Concepts

Based on what you have learned in the last two units, how would you describe disaster recovery in the context of an organisation?

A disaster to an organisational can be defined as a sudden incident that disrupts all or part of its business operations and leading to loss of financial, infrastructural, and at times, human resources. The cause of a disaster can be natural occurrences such as flooding and fire outbreak or human actions like vandalism and cyber-attacks. Thus, Disaster Recovery (DR) is a systematic approach to restore the business systems and infrastructure of an organisation to their normal operations after a disaster. Figure 1 gives a generic overview of the stages in a typical DR process.

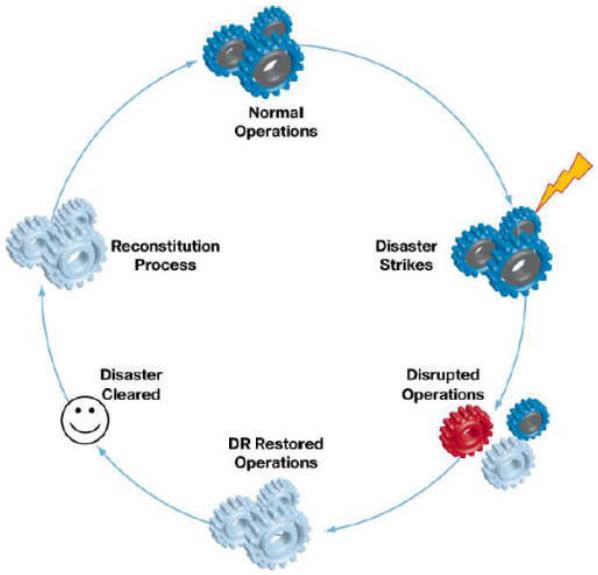


Figure 2.6: Disaster recovery operation cycle [Cisco 2008]

As Figure 1 depicts, when a disaster strikes and disrupts the normal business operations, the management of the organisation will quickly activate the procedure defined in the DRP (disaster recovery plan), which will normally involve switching to some alternative temporary facility while the normal process is being recovered and restored. We have discussed DR planning in the previous unit.

3.1.1 Recovery Scope

The recovery scope is a definition of the software and hardware resources to be backed up for the DR process. Such resources can include servers,

business software applications and their configurations and runtime data, database files, customer data, etc.

3.1.2 Recovery Point Objective (RPO)

RPO is a specification of the upper limit of the data loss between the original and restored operation environments, which a business process can tolerate. That is, a higher RPO implies that the system can tolerate higher data loss after recovery. Thus, a low RPO system requires a frequent backup to ensure it is as close as possible to the original data.

3.1.3 Recovery Time Objective (RTO)

RTO is a specification of the maximum wait time that the business process can tolerate before the restored environment commences normal processing.

3.1.4 Consistency

This is a specification of the requirement that after the completion of recovery from a disaster and subsequent restoration of the business systems, the recovered data should be as consistent as they were in the original system. That is, the crash due to the disaster should not leave inconsistent behind in the recovered systems.

3.2 Disaster Recovery Replication Techniques

What do you consider as the first concrete action in planning for DR?

You must first identify the critical resources for which there must be replicas as backups to support the business continuity and DR process. Then, data replicas are produced through regular backup processes on a secondary site, which becomes operational whenever the primary site is unavailable.

Note that DR replicas are usually kept in secondary sites mainly for security reasons. Incidents such as fire, flooding, vandalism, etc. can consume both the replica and original in the same site, thereby defeating the purpose of the replication.

Can you mention any DR technique for creating these replicas?

The following are the main DR replication techniques:

- Synchronous replication technique
- Asynchronous replication technique
- Mixed replication technique

You will now learn about the strengths and weaknesses of each technique.

3.2.1 Synchronous Replication Technique

This involves the creation of replicas of data and infrastructure at the primary and secondary sites simultaneously. This technique promotes very low RTO and RPO to guarantee little or no service downtime. It is very suitable for recovering high-end transactional applications that need instant failover whenever the primary site fails. However, this technique performs effectively only when the primary and secondary sites are not more than 100 - 300 kilometres apart.

3.2.2 Asynchronous Replication Technique

With this technique, replication occurs first as a backup at the primary site. This backup transaction is logged in a disk journal for subsequent transmission to the secondary site either at a scheduled time or during off-peak period. This technique solves the geographical problem associated with the synchronous technique. However, you cannot guarantee very low RPO since backups at the primary and secondary sites are not done simultaneously.

3.2.3 Mixed Technique

The mixed replication technique combines the features of both synchronous and asynchronous techniques to create replicas at two secondary sites. Hence, it gives near-zero RTO and very low RPO.

3.3 Disaster Recovery Principles and Best Practices

These are some best practices and precautions that need to be taken to ensure effective DR in organisation. The following is a list (not exhaustive) of some of these principles:

- **Keep your DR plan up-to-date with current and emerging threats**
  DRPs are usually developed based on subsisting assumptions at the time of development. The risks you identified in your DRP can become obsolete with time; always update it with current threats in your business environment. For example, cyber-attacks are common nowadays, you may want to analyse the vulnerability of your business operations to any kind of cyber-attack and prepare for it in your DRP.
- **Give consideration also to human resources**
  Let your DRP not focus only on the recovery of data and infrastructural resources. Since a disaster can as well inflict injury on human resources, your DRP should also consider the recovery of the productivity of your human resources after a disaster.

- **Identify your priorities**
  Give more priority to the resources that support critical business processes.
- **Maintain a culture of regular practice and training**
  It is not enough to have a comprehensive DRP in place, since the implementation is not a regular occurrence and can come suddenly; there is a need to sensitise and retrain the employees regularly in preparation for eventualities.
- **Be proactive**
  Do not wait until a disaster strikes before starting your preparation; DR decisions taken during an emergency can be faulty.
- **Do regular update of you Inventory in the DRP**
  On a regular schedule, update the inventory of your resources in the DRP. You may have recently acquired some critical infrastructure whose risks and vulnerabilities are not covered in the existing DRP.
- **Distribute and clarify DR roles and responsibilities in advance.**
  For effective and efficient DRP, everyone in an organisation should be assigned responsibilities in the DRP and be adequately informed of its importance.
- **Respect timely dissemination of accurate information when disaster strikes**
  As soon as a disaster strikes, pass adequate information to all stakeholders in good time and through all possible media.
- **Plan safe escape routes**
  Make an adequate plan for the safe movement of personnel and infrastructure to safe sites during a disaster
- **Pay attention to service level agreements (SLAs)**
  Ensure those disaster contingencies are clearly defined in all SLAs with and contractual obligations with partners of your organisation.
- **Do schedule and thorough testing**
  Conduct scheduled testing of your DRP, with due consideration to your RTO and RPO objectives to avert unexpected failure of the DRP when disaster strikes.

4.0 Self-Assessment Exercise(s)

1. Which of the following specifies the maximum data loss a process can tolerate after a disaster recovery between the original and the restored environments?
   a. Recovery Time Objective
   b. Recovery difference
   c. Recovery Point Objective
   d. Restoration tolerance
   Answers: c

2. Which disaster recovery technique involves the creation of replicas of data and infrastructure at the primary and secondary sites simultaneously?
   a. Asynchronous replication
   b. Synchronous replication
   c. Duplicate replication
   d. Recovery replication

   Answers: b

3. What is the first concrete activity involving all operational units of an organisation in recovery planning?
   a. Testing and exercise
   b. Risk assessment
   c. Identification of critical infrastructure
   d. Control procedure

   Answers: c

5.0 Conclusion

Organisations and businesses are confronted with disasters of varying degrees. The level of damage a disaster will do to an organisation depends on factors such as the recovery point and recovery time objectives of the business processes of the organisation. Hence, the recovery manager must be up to date with the recovery techniques that are most appropriate for its business processes to minimise the impacts of disasters on operations and ensure adequate restoration of data and infrastructure. Only organisations that have adequately developed, maintained, and implemented their contingency plans will survive.

6.0 Summary

You have learned from this unit that disaster recovery is the process of restoring the critical business data and IT infrastructure of an organisation after a disaster. You also learned the key terms that describe the tolerance of a business process to data and time loss. Also, you learned the main disaster recovery techniques and the principles and best practices for the effective implementation of disaster recovery plans for an organisation.

7.0 Refeences/Further Reading

Burgess, D., Dilworth, L., Reed, L., & Walt, M. V. D. (2018). *A Practical Guide to Business Continuity & Disaster Recovery with VMware Infrastructure*. Palo Alto, California 94304: VMware, Inc.

Cisco. (2008). Disaster Recovery: Best Practices.

DREWITT, T. (2013). *A Manager's Guide to ISO22301: A practical guide to developing and implementing a business continuity management system*. United Kingdom: IT Governance Publishing.

ISO. (2012). *ISO 22301: 2012. Societal security — Business continuity management systems — Requirements*. Switzerland: ISO.

Unit 4: Business Continuity

Contents

1.0 Introduction

Importance of business continuity: The process of business continuity is essential Organisations must keep technology and business in line with current threats.

2.0 Intended Learning Outcomes (ILOs)

By the end of this unit, you will be able to:

- describe Business Continuity Management
- derive a Business Continuity Plan
- differentiate between Business Continuity Planning and Disaster Recovery Planning.

3.0 Main Content

The process of business continuity entails arrangements aimed at protecting an organisations critical business functions from interruptions due to incidents or at least minimise the effects of such incidents.

This unit presents the process of business continuity and its significance as well as the strategies for business sustainability

3.1 Overview of Business Continuity

What do you understand by Business Continuity? Business continuity (BC) simply refers to the ability of an organisation to continue delivering its products and services to the clients/customers as previously agreed, even in the face of disruptive incidents.

Such disruptive incidents can be classified as:

- **Human related (human-made) incidents**: This comprises disruptive human actions like terrorist attacks, banditry, robbery, burglary, theft, protests, strike actions, etc.
- **Natural and environmental incidents**: This category covers all kinds of natural and environmental disasters that can disrupt your business activities. Examples include flooding, fire outbreak, earthquake, drought, etc.
- **IT Systems related incidents**: This comprises all forms of disruptive incidents that can arise through the IT infrastructure. It includes critical systems failure, virus attacks and other forms of cyber-attacks.
- **Others**: This encompasses incidents like a power outage, business competition, Client BC contractual requirements, etc.

Can you state any international standard for practicing business continuity?

The ISO 22313/22301:2012 standard offers directions, which can be adopted by organisations in any industry to ensure BC. According to the standard, BC is the capability of an organisation to continue the delivery of products and services at acceptable predefined levels following a disruptive incident. A disruptive incident in this case refers to any event, including natural and human-made disaster, which is capable of interrupting the activities of the organisation. It ranges from relatively simple events like power outage to more complicated ones like fire outbreak, flooding, epidemic, civil unrest, banditry, etc. Depending on its environment of operation, an organisation may be vulnerable to any of these disruptive events. Thus, the ability of the organisation to keep delivering its expected outputs, at satisfactory levels in the face of such events, while trying to recover fully from their impacts, is known as business continuity.

3.2 Business Continuity Management

Business Continuity Management (BCM) is defined as the holistic management process, which comprise the:

- Identification of risks to an organisation and their potential impacts on business operations
- Definition of a framework to effectively respond to such risks to safeguard the interests of key stakeholders, organisational reputation and brand, etc.

Recall from the organisational risk you learned in the previous unit, can you think of any two consequences of not having a business continuity management system?

A Business Continuity Management System (BCMS) is a component of the overall organisational management system. It is charged with the responsibility of the establishment, implementation, operation, monitoring, review, maintenance, and improvement of the business continuity of an organisation. It is an essential tool to keep you in business regardless of the industry; failure to consider having it in place poses the following consequences and many more for your organisation:

- A disruptive incident, not well managed, can adversely affect the reputation and brand of your organisation.
- Your organisation can incur a huge financial loss due to a disruption of critical business activities.
- A disruptive incident can prevent your organisation from meeting critical contractual or legislated obligations, and hence expose you to avoidable litigations.
- You can lose valuable clients/customers to your competitors due to service disruptions.
- Unmanaged disruption can cause even cause low employee satisfaction, and hence, excessive turnover for your organisation.

3.2.1. General Principle of Business Continuity Management

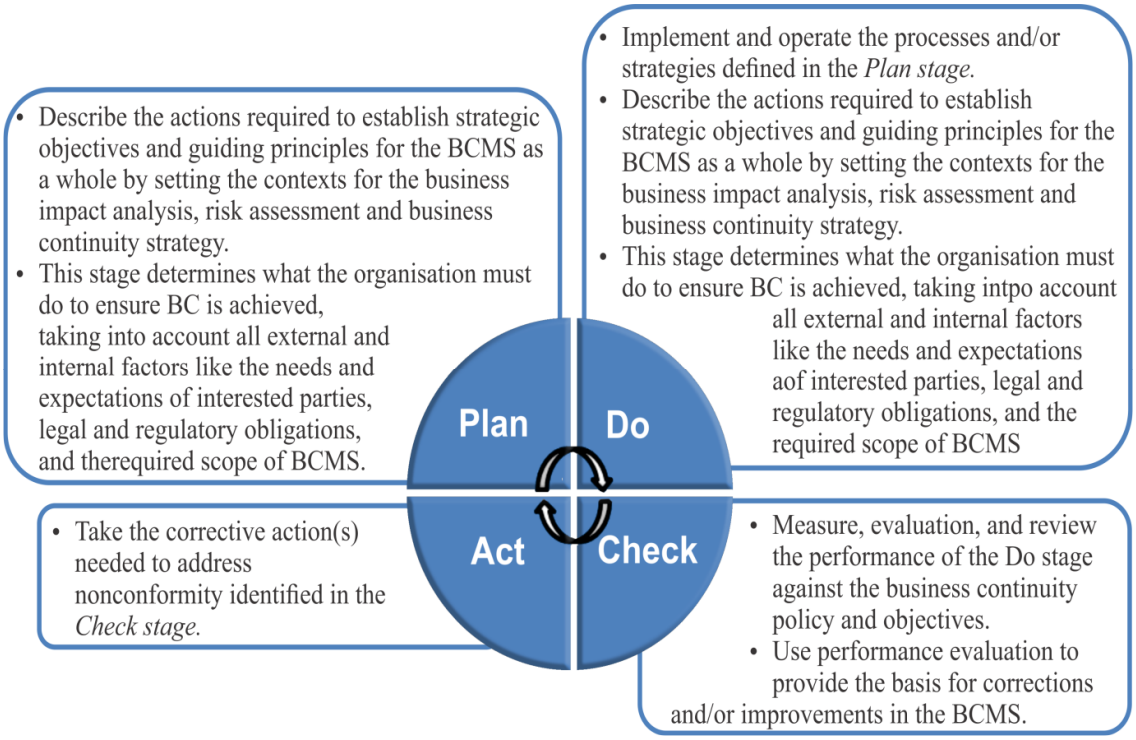


Figure 2.7: The Plan-Do-Check-Act cycle of BCM

The ISO 22301/22313 strongly recommends a 4-stage cycle known as "Plan-Do-Check-Act" (PDCA) for effective BCM as summarised in Figure 1. The PDCA cycle initially starts with the *Plan* stage and moves round the quadrants in a clockwise direction. The information box attached to each quadrant gives an overview of the activities of the respective stage.

3.2.2. Business Continuity Management Lifecycle

Based on the main clauses of ISO 22313/22301:2012, Figure 2.7 presents the various stages of the BCM lifecycle and their corresponding quadrants in the PDCA methodology.

Figure 2.8: Business Continuity Management Lifecycle

3.2.2.1 Operational Planning and Control

This element sits at the very core of BCMS to drive the BCM lifecycle. It is anchored by a BC manager appointed by the top management of an organisation to coordinate the activities in the four stages of the BCM lifecycle.

So if you are appointed the BC manager, what would be your mandate?

You have a general mandate to ensure that the BCMS does not fail to maintain the uninterrupted delivery of critical products and services. Specifically, you will control the monitoring of planned and unexpected changes in the BCM lifecycle and initiate the necessary actions to mitigate the adverse effects of such changes.

3.2.2.2 Business Impact Analysis (BIA) and Risk Assessment (RA):

BIA and RA make the first stage in the BCM lifecycle. BIA is the process of analysing an organisational system to identify the processes that are most critical to the delivery of products and services, the interdependencies between such processes, and the resources needed to execute them at an acceptable level of satisfaction. In other words, BIA will enable you, as a BC manager, to recognise how important is a system to the business activity and how much effect its outage can have on your business.

Risk Assessment (RA) is here again in the BCM lifecycle, can you remember the RA process we discussed in the previous unit?

RA, in this context, is a systematic identification, analysis, and evaluation of the risk posed by disruptive incidents to a business process. It will help you to understand the possible adverse effects of disruptive incidents on prioritised business processes and their dependencies. Having RA documentation during BIA will enhance your ability to identify, evaluate, and treat risks that may lead to disruptive situations. RA also enriches the knowledge of an organisation for the selection of appropriate BC strategy; you will learn BC strategies later in this unit.

wAt the end of this stage, you will have identified the critical risks to your various business activities, their likelihoods of occurrence, and severity levels. You will then move to the next stage in the BCM lifecycle with this information to make adequate plans and strategies to handle such incidents if and when they eventually occur.

3.2.2.3 Selection of BC Strategy

This stage follows immediately after BIA and RA to identify, evaluate, and choose suitable BC strategies ways to:

a. Prevent the disruption of critical business activities, and
b. Ensure the resumption of disrupted business processes to a satisfactory level of operation and within acceptable time limits.

How would you relate this with the risk treatment component of the risk management process we discussed in unit 1?

This stage offers you alternative approaches to keep critical business processes running when a disruptive incident occurs. The following are some possible options:

- **Plan to mitigate the risk:** by reducing the probability of occurrence of the disruptive incident and the severity of its impact on business processes.
- **Plan substitute procedures:** Plan other ways of continuing the affected business activity with less or no impact from the disruptive incident.
- **Insure the business process:** Take out insurance cover for the business process against the anticipated disruptive incidents.
- **Outsource the business activity:** Get a third party to perform the activity probably at a different location.
- **Do nothing/Ignore the risk**: Accept the risk of having the affected business activity disrupted if the incident occurs.

Your choice of BC strategy at this point may be determined by factors such as:

- Size of your organisation
- Spread of your organisation
- Your BC budget
- Cost versus benefit of maintaining the continuity of certain business activities.

3.2.2.4 Establishment and Implementation of BC Procedures:

At this stage, you implement the BC plans and strategies you have put in place in the previous stage. It involves the creation of incident response structures to help the organisation detect and promptly respond to disruptive incidents and return to business as usual. You respond to disruptive incidents by activating the appropriate continuity procedures and strategies, which you have defined in the previous stage. Depending on the BC strategy chosen, the response procedure may only involve people and processes within your organisation or require communications to relevant external parties. The following are some recommendations for effectively implementing the BC procedures to minimize the impacts of the disruption:

- Initiate appropriate communications with internal and external parties
- State the immediate steps to be taken at this critical moment.
- Be flexible in responding to unforeseen threats and to change internal and external conditions;
- Pay attention to the impacts of the disruptive incident on your business processes.
- Pay attention to previously stated assumptions and interdependencies between business activities.

3.2.2.5 Exercising and Testing BC Plans:

This stage involves the validation of the BC plans and procedures established in the previous stages against expected outcomes to:

- Measure the extent to which the chosen BC strategies can adequately respond to incidents and ensure recovery within acceptable delays.
- Ensure that established BC procedures are consistent with the BC objectives.
- Ensure that established BC procedures are complete and current.
- Identify the needs for improvement in the BC plans and procedure.

Can you think of a way to do this exercising and testing?

To initiate a testing exercise, you may take actions such as shutting down critical infrastructure, when it is safe to do so, and then run the implementation procedure to check its effectiveness.

3.3 Business Continuity Planning (BCP)

BCP is the process of documenting the set of procedures to guide an organisation to respond to a disruptive incident, accelerate the recovery from its adverse impact, and eventually restore normal business activities.

Where would you place the BCP in the PDCA methodology and the BCM lifecycle, both of which you have learned previously in this unit?

BCP activities fall in the *Plan* quadrant of the PDCA framework and spread across stages 1 and 2 of the BCM lifecycle. That is, it encompasses BIA and RA as well as the selection of suitable BC strategies to respond to disruptive incidents.

The general goal of BCP is to prevent loss and property as well as to minimise the undesired impacts of unavoidable disruptive incidents on the overall business process. Specifically, the objective is to analyse the business processes and operation environments to deduce the necessary information and procedures to help an organisation to:

- Respond rapidly and appropriately to disruptive incidents
- Communicate with appropriate personnel in the event of a disruptive incident
- Accelerate the restoration of normal business activities.

3.4 Business Continuity Planning Vs. Disaster Recovery Planning

Though BCP and DRP are closely related and you can apply the PDCA lifecycle frameworks we discussed in Section 3.3 to both be tempted to assume them to be precisely the same because they both work towards safeguarding business processes, they are not the same thing. They differ in their scopes and specific mandates. We can itemise some of the key differences as:

- While BCP outlines the strategies and procedures to keep critical business processes running, albeit with an acceptable level of downtimes, during and after a disastrous incident, DRP is concerned with the restoration of lost data and failed IT infrastructure and components after the disaster.

- While your BCP provides an answer to the question "*What can I do to keep the most critical processes of my business running even during the occurrence of a disaster?*", DRP will answer the question, "*Now that the disastrous event is over, how can I restore the lost business data and failed IT infrastructure, and how soon can I do that*?"

- Disaster recovery is usually considered a subset of BC; its focus is mainly on the restoration of the information technology infrastructure that drives the critical business processes after a disaster while BC aims at keeping all essential elements of the business running continuously despite the occurrence of disruptive incidents.

Case Study

Click on this link to see a hypothetical disaster recovery and business continuity plan that demonstrates the implementation of the concepts you have learned in this unit.

Discussion

Generally, the ability to maintain BC offers several benefits not only to an organisation but also to a lot of other stakeholders. In a discussion session, brainstorm to identify at least five concrete benefits you can think of. Also, identify at least three possible consequences of not being able to maintain BC to an organisation.

4.0 Self-Assessment Exercise(s)

1. Which of the following do you think is not one of the main objectives of BCM?
   a. To identify in advance the problematic points in performing business process within a business environment.
   b. To prevent the occurrence of events that can disrupt the business activities of an organisation
   c. To be able to endure the impacts of disruptive incidents on business processes.
   d. To prevent disruptive incidents from having any effects whatsoever o business processes if they eventually occur.

   Answers: b and d

2. Recall that we discussed the BCM methodology in Section 3.2.1, in which quadrant of the PDCA framework would you place BCP?
   a) Plan
   b) Do
   c) check
   d) Act

   Answers: a

Mini project
Develop a business continuity plan for the National Open University of Nigeria, and submit it to your tutor.

5.0 Conclusion

Most businesses nowadays are technology-driven with automated processes. A disruption of such processes even for a short duration can have grave consequences on the survival of such organisation. Therefore, the management of such organisation must be aware of potential threats to continuity in the business environment and develop a plan to minimise disruptions of critical processes and recover operations after any incident.

6.0 Summary

In this unit, you have learned the process of business continuity and its significance. You have equally learned how to derive effective strategies for business sustainability. You also learned the various stages in the business continuity lifecycle, as well as the steps in business continuity and disaster recovery planning.

7.0 References/Further Reading

Burgess, D., Dilworth, L., Reed, L., & Walt, M. V. D. (2018). *A Practical Guide to Business Continuity & Disaster Recovery with VMware Infrastructure*. Palo Alto, California 94304: VMware, Inc.

DREWITT, T. (2013). *A Manager's Guide to ISO22301: A practical guide to developing and implementing a business continuity management system*. United Kingdom: IT Governance Publishing.

ISO. (2012). *ISO 22301: 2012. Societal security — Business continuity management systems — Requirements*. Switzerland: ISO.

NIST Special Publication (SP) 800-61 – Computer Security Incident Handling Guide

https://bcmmetrics.com/benefits-business-continuity-planning/

https://www.continuitysa.com/six-benefits-of-business-continuity-management/

Module 3: Incidence Response - Organising And Preparing The Csirt

Introduction of Module

This module covers all needed to know with respect to

Unit 1 CSIRT Actions
Unit 2 CSIRT Design
Unit 3 CSIRT Development

Unit 1 Computer Security Incidence Response Team (CSIRT) Actions

Contents

1.0 Introduction

Many individuals, companies, and organisations have suffered from Information Technology security breaches, threats, and cyber intrusions, thus leaving a negative effect on their overall performance. Hackers work with little risks or repercussions while they compromise systems to fraudulently buy goods, steal identities, and make profits from stolen cardholder data or accounts.

Experienced and capable computer security incidence responders are highly sought after in response to the numerous security breahes, and computer incidence response career paths have matured over time. However, security incidences may be inevitable, but approaches and methods may be employed to minimize the impact and consequence.

2.0 Intended Learning Outcomes (ILOs)

By the end of this unit, you will be able to:

- categorise the activities performed by the personnel in the CSIRT
- identify the actions to take when a vulnerability is detected
- analyse the actions taken by CSIRT.

3.0 Computer Security Incidence Response Team Actions

3.1 Computer Security Incidence Response Team (CSIRT)

The effectiveness of any IT organisation depends greatly on the composition of its team. The Computer Incidence Response Team (CSIRT) is a cross-functional team that will coordinate actions during computer security incidence. CSIRT comprises IT professionals that provide an organisation with services and support regarding prevention, management, and coordination of potential cybersecurity-related emergencies. The overarching goals of a CSIRT are

- active response to computer security incidents to regain control and minimize damage,
- assisting with effective incident response and recovery, and
- inhibiting computer security incidents from reoccurring.

In your terms, how would you define Computer Security Incidence?

An assumption of this definition is: a CSIRT is an organised entity with a defined mission, structure, roles, and responsibilities. This assumption excludes any ad hoc or informal incident response activity that does not have a defined constituency and documented roles and responsibilities. This assumption is driven by the belief that without a formalized incident response capability, it is not possible to deliver effectively.

The Forum of Incident Response and Security Teams (FIRST), which is the international confederation of CSIRTs that cooperates on handling computer security incidents, has released the "FIRST CSIRT Framework". The framework builds upon and expands the CERT/CC CSIRT services list that has been in use since the late 1980s. It also outlines seven service areas that CSIRTs might want to consider offering its constituents, including incident management, incident analysis, information assurance, situational awareness, and research and development.

Individual CSIRTs are personalized and unique. Every CSIRT has three attributes different from other incident response teams, which include the mission statement, list of services, and the constituency.

Mission

The mission of a CSIRT is a statement of purpose or its reason for existence. A CSIRTs mission defines its area of responsibility and serves to set expectations with its constituency.

An example of a CSIRT mission statement may be:

"It is the mission of XYZ CSIRT to protect XYZ Corp. by creating and maintaining the capability of detecting, responding, and resolving computer and information security incidents."

Services

The delivery of CSIRT services to its constituency details on how the CSIRT mission is carried out. There are many services that a CSIRT may offer, but there are fundamental services. A CSIRT must offer to be considered a formal incident response organisaation. At its most basic level, a CSIRT must be able to do the following:

1. **Receive an incident report from a constituent**
   To receive an incident report from the CSIRT constituency, the constituency needs to know that the CSIRT exists, what it does, how services are accessed, and the service and quality levels that they can expect. This requires that the CSIRT has developed a definition of its mission and services, has announced itself to its constituency, and published guidance on how incident services are requested. This includes publishing the incident response policy, processes, procedures, forms, and resources necessary to inform and enable the constituency to file an incident report.

2. **Analyse an incident report to validate and understand the incident**
   Once an incident report has been received, the CSIRT must analyse the report to validate that an incident, or other types of activity that falls under the CSIRT mission, has occurred. They then must determine if they understand the report and the incident well enough to create an initial response strategy that fulfills the goal of regaining control and minimizing damage. Part of being able to analyse an incident report and respond efficiently is having a sufficient number of appropriately trained staff that can perform a variety of tasks. Each member of the CSIRT staff should have written plans, policies, and procedures that document the roles and responsibilities of the CSIRT technical staff and management.

3. **Provide incident response support**

This entails providing support for the constituent making the report. Depending upon how the CSIRT is organised and the service levels offered, a CSIRT may provide incident response support in one of several ways:

- On-site incident response services delivered directly to the constituent.
- Incident response services delivered virtually, over email, or the phone.
- Coordinated incident response services that combine and allocate the efforts of multiple incident response teams across multiple constituents.

In some situations, an organisation's CSIRT simply develops and oversees the incident response strategies and services rather than implement them. Other groups or departments like network engineers, information technology professionals, or system and data owners carry out the response strategy with the CSIRT managing the effort and ensuring that it is effective.

Constituency

Lastly, a CSIRT must have clearly defined constituency. A constituency is the CSIRT's customer base or recipients of the incident response services. The constituency is assumed to be unique to a given CSIRT and is often the parent organisation.

3.2.1 The Computer Security Incidence Response Team (CSIRT) Actions

The call of Computer Security Incidence Response Team (CSIRT) to actions are necessitated through notifications or request to help desks, email notifications, help desks, legal representatives, etc. for certain actions.

Actions performed by the CSIRT can be grouped into three, namely:

i. Active Service
ii. Passive Services
iii. Management Services.

i. Active Services

Services rendered by the CSIRT during computer incidences are termed active services. These services are meant to eradicate, recover, or report an incident. They include:

a. Incidence Handling: Its major goal is in the identification, documentation, and handling of computer security incidences.
b. Vulnerability Handling: Hardware, data, and application vulnerabilities are examined with a plan to provide proper response

to vulnerability and inform others about the strategies for its mitigation.

c. Evidence Handling: The CSIRT is also involved in handling evidence. Pieces of evidence are objects that could be responsible for attacking the information system. Examples include toolkits, log files, viruses, or exploit scripts.

ii. Passive Services

These are services engaged by the CSIRT in protecting an organisaation's information system against future malicious activity. These services include:

a. Vulnerability Assessment

b. Intrusion Detection Service

c. Announcements and Information Disclosure

iii. Management services provided by the CSIRT include Compliance Certifications, Awareness Training, and Risk Assessments.

A flowchart to depict the actions performed by the CSIRT at the occurrence of a computer security incidence is shown in Figure 3.1.

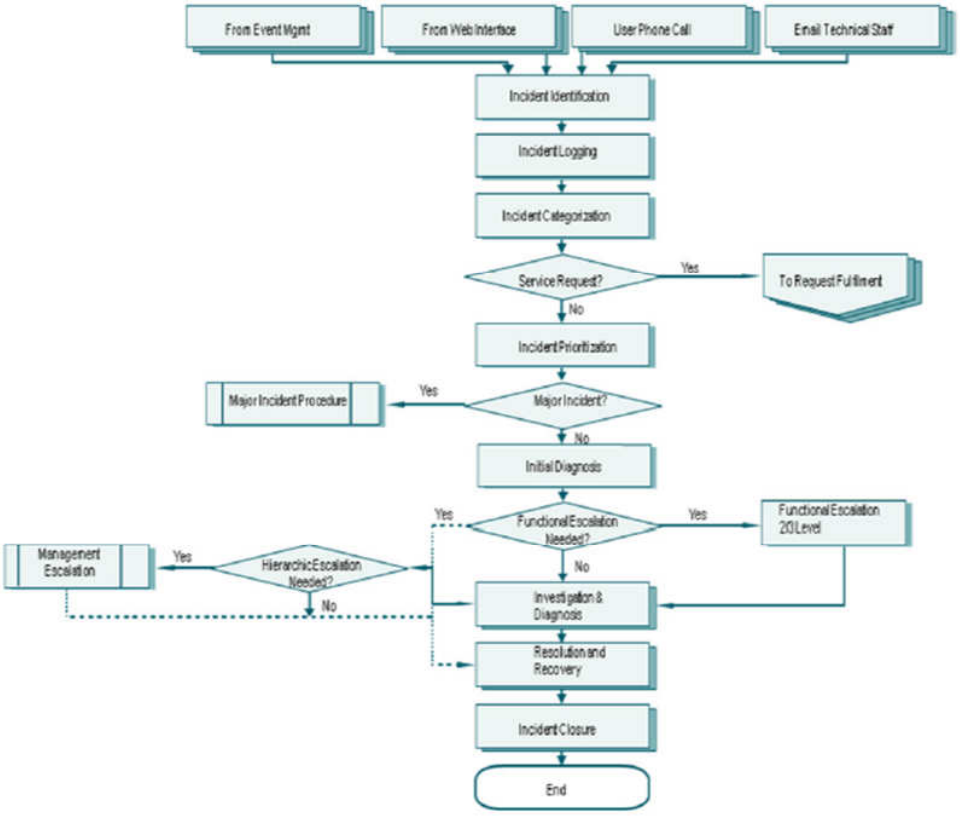


Figure 3.1: CSIRT Action flowchart for Computer Security Incidence Response

3.2.1.1 Conducting a Computer System Vulnerability Assessment (CSVA)

Computer systems vulnerabilities allow easy cyber or physical access by unauthorized users which makes them more susceptible to attack. Computer systems comprises hardware, software, and peopleware (the people who use them), and all these may contain vulnerabilities. Vulnerabilities of computer systems have been categorised as providing access or facilitating access, or misuse. Hackers and assailants use a variety of techniques and tools to exploit these vulnerabilities, including hacking software, reconnaissance, social engineering, password crackers, scanning, war dialing, sniffing, spoofing, and the use of zombies.
Performance of a cyber security analysis requires:

a. Identification and assessment of cyber security threats.
b. Identification and assessment of cyber security vulnerabilities.
c. Formulation of recommendations for cyber security measures.

i. Cyber Security Threat Analysis

Typically, threat analysis involves:

a. Identifying the source of threats, i.e. potential adversaries with the desire to cause harm.
b. Identifying the types of threats, i.e., deciding on the potential objectives of adversaries.
c. Assessing the probability of threat's occurrence (likelihood).
d. Developing an initial risk estimate using c above and estimates of the consequences of the threats.

The combination of the threat source and type defines specific threats that can be analysed using vulnerability analysis. Threat likelihood and risk can be used to decide to what extent vulnerability analysis is needed. Formal threat analysis approaches have been developed for process facilities, and these can be adapted to cyber threats. However, in many cases, it is probably appropriate simply to assume the threats described earlier exist and focus resources on the vulnerability analysis. The likelihood of the threats can be incorporated into the vulnerability analysis.

ii. Cyber Security Vulnerability Analysis

Vulnerability analysis is the identification of flaws or weaknesses that expose a cyber system to attack. In a scenario-based analysis, it includes identifying ways in which vulnerabilities could be exploited. Cyber security vulnerability analysis can focus on a computer system or the process or facility that contains the system. It identifies ways specific threats can be

realized (called cyber threat scenarios) in a similar way to identifying hazard scenarios in a Process Hazard Analysis (PHA). A threat scenario is a specific sequence of events that has an undesirable consequence resulting from the realization of a threat. It is the security equivalent of a hazard scenario.

Elements of a cyber threat scenario are shown in Figure 3.2.

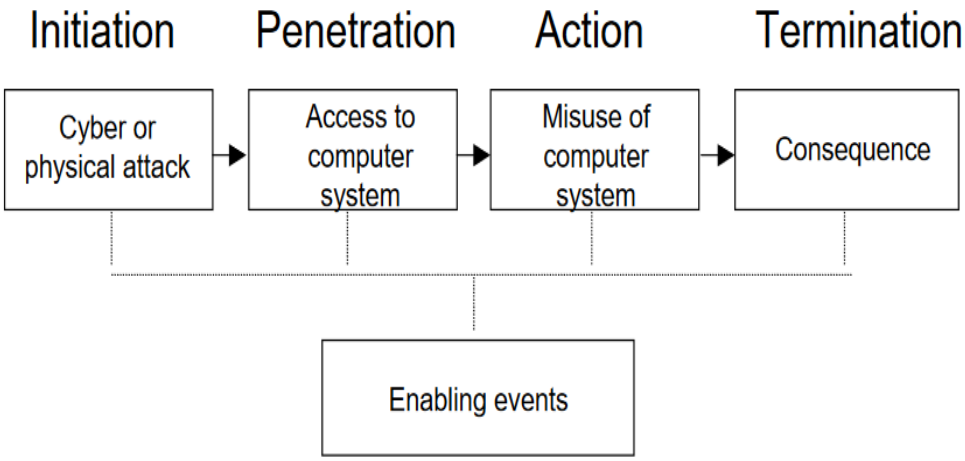


Figure 3.2: Elements of a Cyber Threat Scenario

A CSVA is accomplished in seven steps:

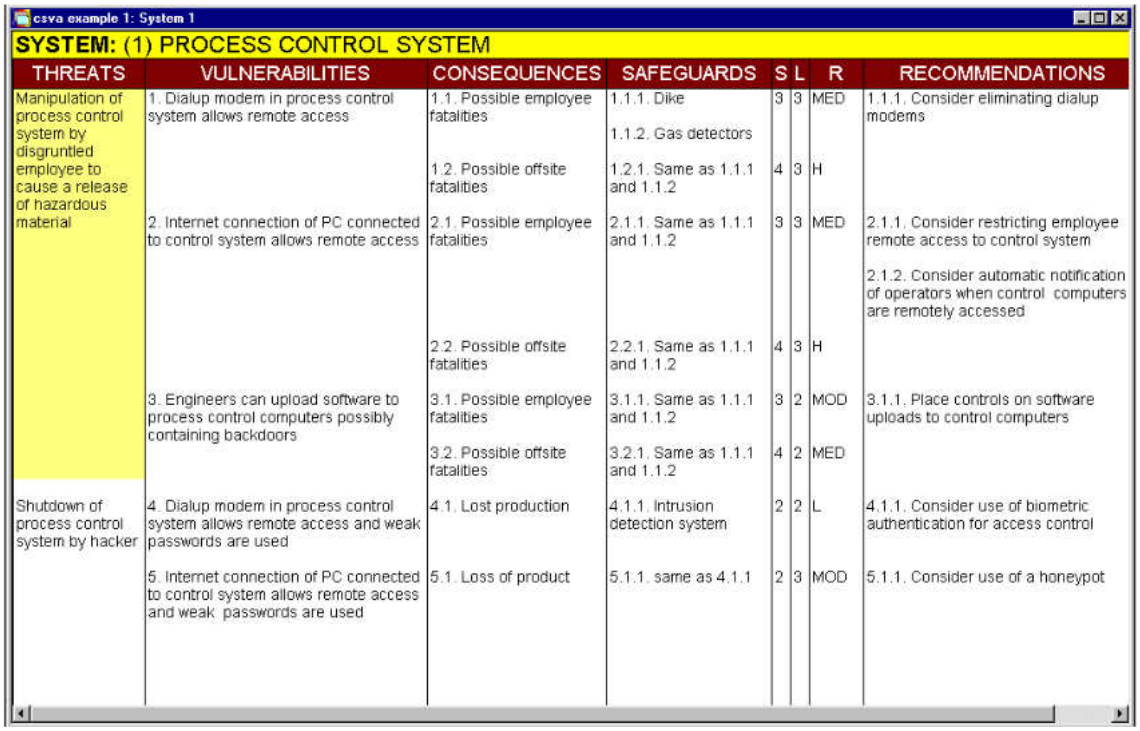
1) Divide computer system/process/facility into systems/subsystems
2) Consider each credible threat within each system/subsystem
3) Identify vulnerabilities within each system/subsystem
4) List worst possible consequences
5) List existing security measures and safeguards
6) Risk rank scenarios (optional)
7) Identify any recommendations.

Each step is described in the following steps:

Step 1. Divide computer system/process/facility into systems/subsystems.

CSVAs can be performed exclusively on the computer control system, and only useful when an SVA has already been performed to look at other aspects of security, such as physical security. For more detailed analysis, computer system can be examined as a single system, or it can be broken into subsystems. The latter approach is preferred for situations involving complex and multiple networks. Alternatively, cyber security can be considered together with other aspects of security and a single SVA conducted for a process or an entire facility. The process or facility can be

considered as a single system, or it may be subdivided into systems and subsystems for more detailed analysis. Whenever subdivision is employed, a global system should also be used to account for formal events that arise within multiple systems/subsystems and affect the entire facility/process. Subdivision helps to focus on the analysis and provides a suitable level of detail. It parallels the use of nodes and systems/subsystems in PHA, although they are typically larger in SVA than in PHA. For example, they may be a tank farm, production unit, or product storage area. Figure 3.3 describes a worksheet used in performing SVA and CSVA for each system/subsystem.



csva example 1: System 1

SYSTEM: (1) PROCESS CONTROL SYSTEM

THREATS	VULNERABILITIES	CONSEQUENCES	SAFEGUARDS	S	L	R	RECOMMENDATIONS
Manipulation of process control system by disgruntled employee to cause a release of hazardous material	1. Dialup modem in process control system allows remote access	1.1. Possible employee fatalities	1.1.1. Dike 1.1.2. Gas detectors	3	3	MED	1.1.1. Consider eliminating dialup modems
		1.2. Possible offsite fatalities	1.2.1. Same as 1.1.1 and 1.1.2	4	3	H	
	2. Internet connection of PC connected to control system allows remote access	2.1. Possible employee fatalities	2.1.1. Same as 1.1.1 and 1.1.2	3	3	MED	2.1.1. Consider restricting employee remote access to control system 2.1.2. Consider automatic notification of operators when control computers are remotely accessed
		2.2. Possible offsite fatalities	2.2.1. Same as 1.1.1 and 1.1.2	4	3	H	
	3. Engineers can upload software to process control computers possibly containing backdoors	3.1. Possible employee fatalities	3.1.1. Same as 1.1.1 and 1.1.2	3	2	MOD	3.1.1. Place controls on software uploads to control computers
		3.2. Possible offsite fatalities	3.2.1. Same as 1.1.1 and 1.1.2	4	2	MED	
Shutdown of process control system by hacker	4. Dialup modem in process control system allows remote access and weak passwords are used	4.1. Lost production	4.1.1. Intrusion detection system	2	2	L	4.1.1. Consider use of biometric authentication for access control
	5. Internet connection of PC connected to control system allows remote access and weak passwords are used	5.1. Loss of product	5.1.1. same as 4.1.1	2	3	MOD	5.1.1. Consider use of a honeypot

Figure 3.3: Worksheet for Separate Cyber Security Vulnerability on a Computer System (Baybutt, 2003)

Step 2. Consider each credible threat within each system/subsystem

Specific threats from the cyber threat analysis are considered in each system/subsystem, as applicable. Figure 3.3 shows a simple CSVA example of the threats of process shut down by a hacker and hazardous material released by a disgruntled employee.

Step 3. Identify vulnerabilities within each system/subsystem.

In scenario-based SVA, ways in which specific threats could be realized are usually identified by a team of people brainstorming similarly to performing a Process Hazard Analysis (PHA), except that threat scenarios are identified

instead of hazard scenarios. This can also be done in CSVA (see Figure 3.3). The column labeled "Vulnerabilities" on the worksheet is used to record threat scenario information. This could also be labeled "Scenario." Knowledge of cyber vulnerabilities enables specific vulnerabilities to be identified. Brainstorming focuses on the penetration and action elements of threat scenarios (Figure 3.2). Teams identify how the computer system can be penetrated and what malicious actions can be taken once access has been gained.

It is also possible to work at a higher level and simply consider ways in which a computer system can be penetrated using cyber or physical means. If measures can be implemented to reduce the likelihood of penetration, the remaining risk may be accepted depending on the type and magnitude of consequences possible. An alternative approach is to study the computer control system using techniques such as fault tree analysis or sneak path analysis. In PHA, the central reference documents are process drawings and procedures. In SVA, plot plans and process drawings are used. In CSVA network diagrams that describe the architecture of the computer control systems and other computer systems and support systems with which they interface are needed together with supporting information on system design and operation. Information on the logic and operation of the computer control software is also needed for a detailed analysis.

Step 4. List worst possible consequences

Usually, a range of consequences will be possible for each threat/vulnerability. Conservatively, the worst consequence must be assumed. Both the type of impact and severity of the event should be identified and recorded in the worksheet, e.g. release of hazardous material that could result in fatalities or process shut down (see Figure 3.3).

Step 5. List existing security measures and safeguards.

Security measures and safeguards may address prevention, detection, control, and mitigation of cyber-attacks. Applicable security measures and safeguards are recorded in the SVA worksheet (see Figure 3.2).

Step 6. Risk rank scenarios

The severity and likelihood of each threat scenario can be estimated using severity and likelihood levels such as those in Tables 3.1 and 3.2 and a risk matrix such as that in Table 3.3 (see Figure 3.2). The estimated risk levels can be used to determine if recommendations for risk reduction are needed or to prioritise recommendations.

Table 3.1: Example of Threat Likelihood Levels

Likelihood Level	Meaning
1	Remote
2	Unlikely
3	Possible, could occur in the plant lifetime
4	Probable, expected to occur in the plant lifetime

Table 3.2: Example of Threat Severity Level

Severity Level	Meaning
1	Injuries treatable by first aid
2	Injuries requiring hospitalization
3	Fatalities on-site
4	Fatalities extending off-site

Table 3.3: Example of Threat Risk Matrix

Threat Severity

Threat Likelihood

	1	2	3	4
1	Negligible	Very Low	Low	Moderate
2	Very Low	Low	Moderate	Medium
3	Low	Moderate	Medium	High
4	Moderate	Medium	High	Very High

Step 7. Identify any recommendations

Safeguards established for process safety management to protect against accidental releases may help protect against cyber threats but likely will not be sufficient. Additional and strengthened safeguards may be needed. Cyber security measures will also be needed. Various measures are possible such as authentication, encryption, firewalls, and intrusion detection systems.

iii. Recommendations for cyber security measures

Once vulnerabilities have been determined, recommendations may be made for consideration by management based on the nature of the threat, vulnerabilities, possible consequences, and existing security measures and safeguards (see Figure 3.2).

Programs for cyber security have been described that can be used as reference points in decision making. It is also possible to facilitate decisions on the implementation of recommendations by performing a Rings of Protection Analysis (ROPA) as an extension of the SVA. It must be recognised that actions to enhance cyber security could adversely impact safety, operability, etc.

Tradeoffs must be examined carefully in making decisions. For example, enhanced password protection using lockout after several logon attempts may not be possible for computer control systems for safety and operability reasons.

3.3 Roles of CSIRT Personnel in Incidence Response

An experienced incident manager, usually the Chief Information Security Officer (CISO) leads the investigation team during an incidence response event, supported by a member of the IT department and other ancillary staff whose role is task-oriented. A list of people involved in the computer security incidence response includes:

- Representatives from internal and external counsel
- Business line managers
- Industry compliance officers
- Security Professionals
- Desktop and server IT support team members
- Network infrastructure team members
- Human resource personnel and other employees who may find themselves involved in responding to a computer security incidence.

The diagram in Figure 3.4 shows the composition of the Computer Security Incidence Response Team (CSIRT). The team is expected to hold meetings to

review past incidences and make recommendations on changes to policy, training, and technology.

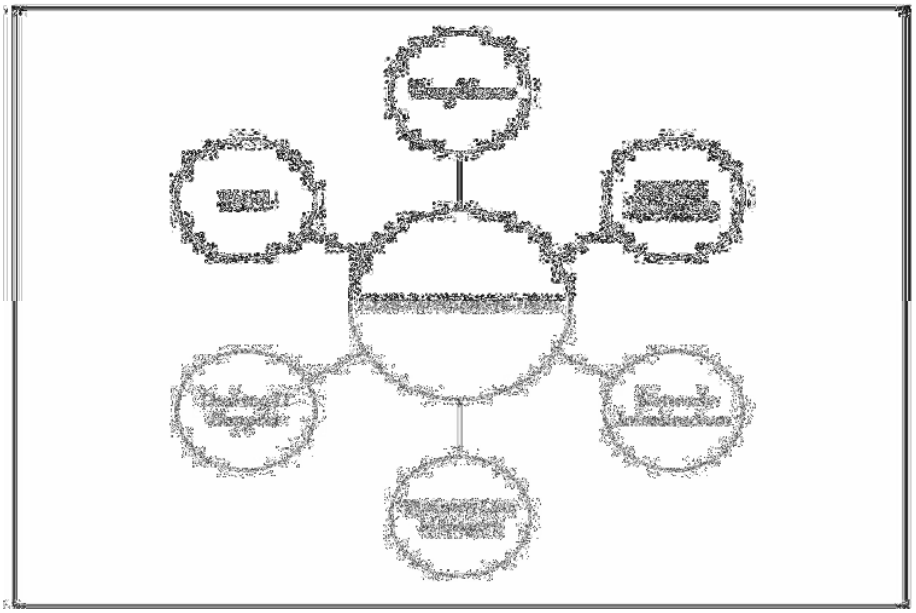


Figure 3.4: Composition of Computer Security Incidence Response Team

i. The User/Client

A person or group of persons who use the I.T services provided by the organisation are generally referred to as the users or clients. These people may request a change or report a computer security incidence. Their main roles in the incidence response process include:

a. Reporting computer security incidences when they occur.
b. Using the self-service portal or email or call your area's Support Desk
c. Providing complete and correct information about the computer security incidence itself and the circumstances under which it occurred.
d. Provides the input into the Computer Security Incidence Management Process.

ii. The Computer Security Incidence Response Manager

The Computer Security Incidence Manager (or Chief Information Officer, CISO) is the single individual responsible for the incidence management process across all of IT departments in an organisation. His responsibilities include:

a. Ensures that all IT departments follow the computer security incidence management process.
b. Represents the Computer Security Incidence Management Team in top-level management meetings

c. Communicates process information or changes, as appropriate, to ensure awareness.
d. Analyse Computer Security Incidence metrics.
e. Sponsor improvements to the process or tool(s).
f. Supervise, coordinate, communicate, and prioritise all recovery activities with all other internal/external agencies.
g. Oversee and monitor the consolidated IT Disaster Recovery plan
h. Interface with the organisation management; ensuring that the process receives the needed staff resources
i. Identify and acquire additional supplies necessary to support the overall disaster recovery effort.
j. Makes final determination and assessment as to recovery status, and determine when IT services can resume at a sufficient level.

iii. The Computer Security Incidence Response Coordinators

The coordinators are contact people between the different departments who are responsible for the planning and monitoring of a specific computer security incidence process and may be responsible for the design of processes within their departments. Their roles are not limited to, the following:

a. Using the process, procedures, policies, work instructions, required documentation, and tools as designed.
b. Determining whether a computer security incidence record requires special reporting.
c. Closing all assigned and resolved computer security incidences.
d. Analysing computer security incidence metrics.
e. Managing ownership of computer security incidence records while providing monitoring and tracking of incidence for their department.
f. Validating and assigning computer security incidence records to incidence response. Technicians.

iv. The Computer Security Incidence Technicians

This set of people are the initial contact between users and the IT organisaation. They are experts in different fields who help to resolve computer security incidence problem for their functional organisaation and specific technology platform. The technicians' roles are:

a. Performing first-line investigation and diagnosis of computer security incidences reported.
b. Communicating with users and keeping them informed of computer security incidence response progress, notifying them of impending changes or agreed outages, etc.
c. Log, categorise and prioritise computer security incidences.
d. Take ownership of assigned computer security incidences.
e. Resolve those computer security incidences they can and escalate incidence that cannot be resolved within agreed timescales.

3.4 Discussion

Within the context of Computer Incidence Response, can you discuss the actions that could be taken concerning the identification of vulnerabilities on your mobile phones?

3.5 Case Studies

A Routine Incidence in a Large Company

1 Jim checks the daily antivirus report and finds that workstation BOSTON0094 has been infected with a virus. He starts a ticket, copies details into it, establishes a remote connection to the workstation's network port, and puts it into quarantine. On carrying out some researches, he finds that the virus does not have any remote control or data export features, so there is no need to escalate the level of the incident. He thereafter dispatches a local technician to re-image the workstation. The local technician talks to the workstation owner, picks it up, verifies that critical data has been saved, and re-installs the standard company builds on it. The workstation is returned to the owner, and the ticket is closed. Can you identify the personnel to make up a Computer Security Incidence Response Team in this case?

4.0 Self-Assessment Exercise(s)

1. The role of a Computer Security Incidence Response Coordinator includes:
   a. Log, categorise and prioritise computer security incidences.
   b. Take ownership of assigned computer security incidences.
   c. Analysing computer security incidence metrics.
   d. Identify and acquire additional resources necessary to support the overall disaster recovery effort.

   Answer: c

2. Chief Information Officer (CISO) is also refered to as _____
   a. The Computer Security Incidence Manager
   b. The Computer Security Incidence Response Coordinators
   c. The Computer Security Incidence Technicians.
   d. The Computer Security Incidence Officer

   Answer: b

5.0 Conclusion

The most valuable and highest priority for safety an organisation can adopt is the formation and inclusion of Computer Security Incidence Response Team in its organisation. A proper computer security incidence response requires dedication to standard procedures and attention to great detail, which can only be provided by the Computer Security Incidence Response Team (CSIRT) to yield great satisfaction.

Most organisations now use internet facilities to enhance their operations, such as using e-mail or transacting business online and, as a result, may be subjected to malicious/virus attacks on their networks and infrastructures, which, if not properly addressed, may cause a major setback or harm to the organisation.

6.0 Summary

A Computer Security Incidence Response employs a varied and dynamic approach to respond and compensate for the multiple sources of potential computer security threats or incidences an organisation may encounter. This unit discussed different roles played by the personnel involved in CSIRT. Also, necessary tools to improve visibility, alerting, actionability, evaluate, and security incidences were clearly enumerated with a link to sample report to aid in decision making.

7.0 References/Further Reading

Baybutt. P. (2003). A Scenario-based Approach for Industrial Cyber Security Vulnerability Analysis. A paper downloaded from:

http://www.primatech.com/images/docs/paper_a_scenario_based_approach_for_industrial_cyber_security_vulnerability_analysis.pdf

Jason T. Luttgens and Matthew Pepe, Incident Response & Computer Forensics,(3rd Edition), McGraw-Hill

Kouchakji, J. (2016). Pentesting vs. Vulnerability in Typical Application Scenarios, An Article Published by Cybrary, downloaded from https://www.cybrary.it/0p3n/pentesting-vs-vulnerability-assessment-typical-application-scenarios/

Leighton R. Johnson III, Computer Incident Response and Forensics Team Management*, 2014*

Marcus K. G. Adomey, Introduction to Computer Security Incident Response Team(CSIRT)

Michael E. Whitman, Herbert J. Mattord, and Andrew Green, Principles of Incident Response and Disaster Recovery

Timothy Proffitt, Creating and Managing and Incident Response Team for a Large Company.

Unit 2: Computer Security Incidence Response Team (CSIRT) Design

Contents

1.0 Introduction

A Computer Security Incident Response Team (CSIRT) helps in mitigating the impact of security threats to any organisation. As cyber threats grow in number and sophistication, building a security team dedicated to Incident Response (IR) is a necessary reality. This unit discusses how to create. organise and manage a CSIRT and offer tips to make the incidence response team more effective.

2.0 Intended Learning Outcomes (ILOs)

By the end of this unit, you will be able to:

- describe different models involved in building CSIRT
- describe the Key responsibilities of a CSIRT
- differentiate between Community Emergency Response Team (CERT), Computer Security Incident Response Team (CSIRT), and Security Operations Center (SOC).

3.0 Main Content

3.1 Computer Security Incidence Response Team (CSIRT) Design

A CSIRT is a group that responds to security incidents when they occur. Key responsibilities of a CSIRT include:

- Creation and maintainenance of an Incident Response Plan (IRP)
- Investigation and analysis of incidents
- Management of an internal communications and updates during or immediately after incidents
- Communicating with employees, shareholders, customers, and the press about incidents as needed
- Remediating incidents
- Recommending technology, policy, governance, and training changes after security incidents.

From your last lesson, can you recall the actions taken when a vulnerability is identified in a system?

3.1.1 Emergency Response Teams

In general, a CSIRT analyses incident data discusses observations and shares information across the company. There are, however, overlapping responsibilities between a Community Emergency Response Team (CERT), Computer Security Incident Response Team (CSIRT), and Security Operations Center (SOC). The roles and background of their origination give clarity to their differences.

A facility where an organisation's network, applications, and endpoints are monitored and defended is termed Security Operations Center (SOC). The term was adapted from Network Operations Centers (NOC), where large telecommunication or corporate networks are monitored. When network security became more of a concern, security teams were formed within the NOCs and eventually were spun off into larger organisations as the responsibilities of security teams became more complex and specialized. SOC team are the security staff working in a security operations center.

The term "Computer Emergency Response Team" was coined in 1988. In response to the Morris worm attack that impacted thousands of servers on the Internet, DARPA funded the formation of the Computer Emergency Response Team Coordination Center (CERT-CC) at Carnegie Mellon University. The goal of CERT-CC was to help protect theff Internet by

collecting and disseminating information on critical security vulnerabilities. Several other countries formed similar centres using the same acronym (despite threats of legal action by Carnegie Mellon for trademark infringement). Now the term CERT applies to any emergency response team dealing with cyber threats. Many people use CERT-CC interchangeably with CSIRT, though the charter of a CERT is information sharing to help other response teams respond to threats against their infrastructure.

A CSIRT is responsible for responding to security incidents. A comprehensive response includes both technical actions taken to remediate the incident and recommended changes to systems to protect against future incidents. There are several nontechnical aspects to a response, including employee communications, responding to press inquiries, dealing with legal issues, and any personnel issues in the event of insider action. (Other names for CSIRT include Computer Incident Response Team (CIRT) and Incident Response Team (IRT).)

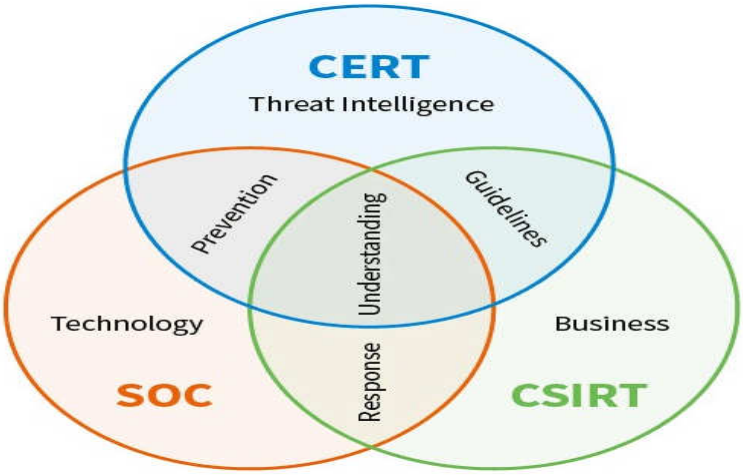


Figure 3.5: Relationship between CERT, CSIRT and SOC

Summarily, using strict definitions, a CERT collects and disseminates security information, typically for the benefit of a country or industry. A CSIRT is a cross-functional team that responds to incidents on behalf of a country or organisation. A SOC is where a country or organisation monitors and defends its network, servers, applications, and endpoint computers. Figure 3.5 displays the primary roles and characteristics of CERT, CSIRT, and SOC.

3.2 Structures of CSIRT

There are a number of organisational models that a CSIRT can follow. Some considerations for how a CSIRT may be structured include a need for 24/7 coverage, availability of trained employees, full or part-time

team members, and cost. Following are different structures that could be adopted in designing CSIRT:

i. Centralized CSIRT

In a centralized CSIRT, a single incident response team serves the entire organisation, and all incident response resources are contained within the dedicated unit. This kind of CSIRT is good for small organisations or organisations with limited geographic scope.

ii. Distributed CSIRT

Several independent incident response teams exist in a distributed CSIRT,. The distribution of CSIRT resources may depend upon the wide geographic scope of the organisation or the location of major facilities. Other attributes that may influence the distribution of CSIRT include a company organised by a business unit structure or simply by the distribution of employees and information assets. Most distributed CSIRT models also require CSIRT coordination.

iii. Coordinating CSIRT

A coordinating CSIRT is a CSIRT that manages other, often subordinate, CSIRTs. This CSIRT model coordinates incident response activities, information flow, and workflow among the distributed teams. It may not provide any independent incident response services itself but focuses on the efficient and effective use of the resources in the distributed teams as its value-add. CERT/CC is an example of a coordinating CSIRT that orchestrates activities among national, governmental, and regional CSIRTs.

iv. Hybrid CSIRT

A hybrid CSIRT is one that combines some of the attributes of centralized and distributed CSIRTs. Often, the central CSIRT component is full-time, and the distributed component is composed of subject matter experts that may not be attached to the incident response activity except as needed during computer security incident response. In this model, when the central CSIRT component detects an incident, it analyses the incident and determines what kind of specialized help it needs. The appropriate experts can then be called up to assist in response activities.

It must be noted that even though the hybrid CSIRT relies upon subject matter experts that are not full-time CSIRT members. The hybrid CSIRT is a formal incident response organisaation with distributed units of experts designated as incident response professionals. These professionals have defined roles and responsibilities, receive formal incident response training, and may be required to obtain and maintain certification as an incident handler.

v. CSIRT/SOC Hybrid

There is another hybrid CSIRT model that is driven largely by the increase in the number of Security Operations Centres (SOC). In this hybrid model, the SOC is responsible for receiving all alerts, alarms, or user security reports that may be indicative of an incident. As the SOC clears the volume of alerts at tiers 1 and 2, there are some indicators of compromise that rise through the SOC levels that require additional analyses to understand if they represent a computer security incident or not. For those alerts and indicators that are, in fact, security incidents, the CSIRT is activated. In this model, the SOC acts as a front-end for the CSIRT, performing incident detection and passing incidents to the CSIRT.

vi. Outsourced CSIRT

The last CSIRT model is the outsourced CSIRT. There are many reasons to outsource CSIRT activities with cost and the time to build an internal CSIRT as the predominant reasons to outsource. Other factors include the ability to find and train enough incident responders or the need to provide 24/7 service, which also puts a strain on finding sufficient numbers of trained incident responders.

Variations to the outsourced CSIRT model include staffing an internal CSIRT with contractors rather than employees or outsourcing specialized services that may be only occasionally needed, like digital forensics.

3.2.1 How to build a CSIRT

Developing an effective incident response means an organisation can detect and respond to a computer or information security incident in a way that limits the damage done and keeps the cost of recovery as low as possible. While the organisation should have a multi-layer approach to protecting business operations, one strategy to accomplish this is building a CSIRT.

The creation of an effective incident response team is supported by the following strategies:

a. Deciding what types of technical backgrounds, roles, and responsibilities are required on the CSIRT.
b. Assigning a team leader to oversee CSIRT efforts and communicate incidents and progress to the executive staff.
c. Determining the best suited CSIRT organisational model and required functioning hours for the company.
d. Creating security plans, policies, and procedures for a variety of potential threats and incidents.
e. Providing team members with routine cybersecurity education and awareness training.
f. Conducting system risk assessments.

g. Identifying critical incident response assets, including information, business processes, technology, and people.
h. Having a well-documented asset management
i. Implementing a configuration management program that ensures all software is patched and updates are tested and applied on time.
j. Executing a defensive network architecture using routers, firewalls, intrusion detection and prevention systems, network monitors, and security operations.

Some of the mechanisms for creating CSIRT include:

- Provide early warning
- Detect & Identify the activity
- Develop mitigation & response strategies
- Establish a trusted communication channel
- Share data and information about the activity
- Track and monitor information
- Determine Trends & Long Term Remediation plans.

3.2.2 Best Practices for Creating an Effective CSIRT

In many organisations, a Computer Security Incident Response Team (CSIRT) has become essential to deal with the growing number and increasing sophistication of cyber threats. Unlike a Security Operations Center (SOC); a dedicated group with the tools to defend networks, servers, and other IT infrastructure, a CSIRT is a cross-functional team that bands together to respond to security incidents. Some members may be full-time, while others are only called in as needed.

Unlike a SOC, the comprehensive response provided by an incident response team reaches beyond the technical actions taken to remediate an incident. It includes recommending changes to systems or organisational practices to protect against future incidents. It also includes non-technical responsibilities, such as managing internal communications, status reporting, assisting counsel, and handling personnel issues in the event an incident resulted from insider actions.

Creating an effective incident response team involves different processes and talent compared to establishing a SOC. In this lesson, we will review five effective best practices, leveraging the latest techniques and technologies.

a. Build a Friendly Team

Part of building an effective CSIRT is educating your entire organisation about its critical, cross-functional nature. Every team member needs to understand the value of complementary skills and

roles. This helps eliminate friction between, for example, technical members in the SOC and nontechnical CSIRT members.

b. Recruit an Effective Advocate or Executive Sponsor

This should be a staff member at the level of a CISO or executive staff member, who can effectively communicate the impact of an incident to other executives, as well as to board members. This person is also responsible for ensuring that the incident response team receives appropriate attention, a workable budget, and retains the authority to act swiftly during a crisis.

c. Define Key Roles and Recruit from across the Organisation

The cross-functional team members should include:

- An Incident Manager who can work across the organisation, call meetings, and hold team members accountable for their action items. This person rolls up findings before communicating incidents to the company.
- A Lead Investigator, such as a security analyst or dedicated SOC incident responder who takes charge of investigating a security incident.
- A Communication and Public Relations specialist who handles everything from fielding press enquiries to communicating to employees and monitoring social media.
- A Lead Legal/Privacy expert such as your general counsel or a deputy legal team member, who advises on issues. An example is the need to disclose a breach or deal with potential legal impacts of a security incident.

d. Create a Deep Bench based on Realistic IT Budgets

Since security incidents can occur at any time, you will need to have CSIRT staff geographically dispersed to ensure someone will be available 24/7. If you can not "follow the sun," then the next-best option is to implement shifts comprised of those who are trained and qualified to lead an incident. You should also have redundancy through cross-training for each CSIRT member and their role.

However, few IT organisations have the budget to staff to this ideal level. So, as part of this best practice, plan for real-world staffing limitations before an incident occurs. Job shadowing and cross-training also help.

e. Insulate Team Members from Distractions

Security incidents can be intense; the effort required for breach response could take years. CSIRT members may experience burnout from responding

to an ongoing deluge of audits, legal needs, HR requests, various daily fires to put out, and so on. So, while your incident response team needs to be "friendly," they should also practice distraction avoidance. This requires isolation from unplanned external requests as well as establishing a process for work intake.

Using these capabilities enables CSIRT to define a preapproved set of actions or playbooks to deal with an attack or other incident. And since CSIRT actions are cross-functional, they should include all aspects of negative event response—from locking down an impacted system to inbox cleanup, and rapid communication to impacted stakeholders. This makes the response much friendlier—or eliminating the "scary" aspect of automated responses.

3.3 CSIRT Management

Since incidents cannot always be predicted, it is important to have a dispersed but well-managed CSIRT. Most CSIRTs are structured to have enough staff to maintain 24/7 monitoring. This is done by dividing operating hours into three shifts, each with a designated shift lead. Additionally, larger companies will not only separate employees by time but also geographic location. Smaller companies may want to accomplish this by outsourcing CSIRT processes for after hours.

Due to this distributed nature, emphasis should be placed on management. Shift leads should communicate with each other to determine what was, or was not, resolved during their timeframe. This should then be relayed to the overall CSIRT team leader or executive staff representative so as to maintain transparency to the rest of the organisation.

The four-step process for organising and managing CSIRT is depicted in Figure 3.6

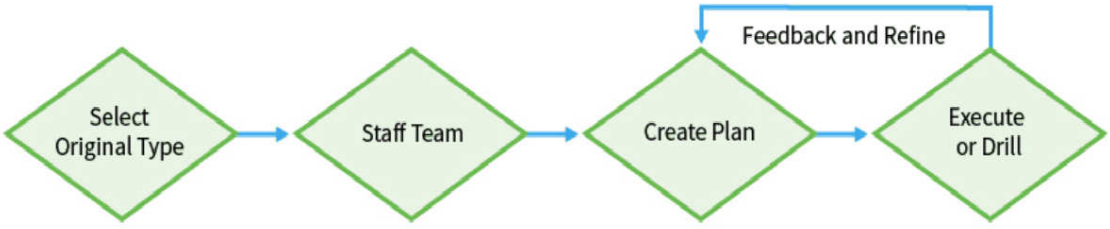


Figure 3.6: Process for managing a Computer Security Incident Response Team (CSIRT)

Selecting Original Type

Using the strict definitions in 3.1 of this unit, the choice between a CSIRT and CERT is straightforward. Unless your goal is to collect and disseminate information on security vulnerabilities on behalf of a country (which probably is already covered) or industry (which likely already exists), then your choice is narrowed down to either a CSIRT or SOC.

If your incident response team roles include monitoring and defending your organisation against cyber-attacks, you are looking at building and staffing a SOC. If your organisation is too small to afford a SOC, or you have outsourced your SOC (which is common for smaller organisations), then you will want a CSIRT to deal with security incidents as they occur. Again, the response may not be technical, but the response requires legal or PR expertise.

Organising a CSIRT

Organising your CSIRT involves determining who will be on the team, their roles and responsibilities, which functions to outsource, and where your team members will be located.

As mentioned, the CSIRT is a cross-functional team that will coordinate during incidents. The CSIRT should also hold quarterly meetings to review past incidents and make recommendations on changes to policy, training, and technology. Lastly, the team should participate in drills at least twice a year. These drills are considered "table-top incidents," where CSIRT members act out what they would do in the case of an incident so that the team stays sharp and works out any issues.

To build your CSIRT team, here is a list of the talent you will need, along with the different CSIRT roles and responsibilities:

i. **Team Leader or Executive Sponsor:** Typically, this is the CISO or a member of the executive staff. The key role of the team leader is to communicate incidents to the executive staff and board and to assure that the CSIRT gets appropriate attention and budget.
ii. **Incident Manager:** This manager or executive can work across the organisation and is responsible for calling meetings and holding team members accountable for their action items. The incident manager also summarizes findings and any impacts on communication throughout the company before escalating issues up to higher levels.
iii. **Lead Investigator:** This technical resource, such as a security analyst or dedicated incident responder in the SOC, is responsible for investigating the occurrences during a security incident. The lead investigator may work with an extended team of security analysts and forensic investigators.

iv. **Communication and Public Relations:** Ideally, this is an individual on the marketing team responsible for public relations, fielding any press inquiries or statements, as needed, and drafting communications to be sent to employees, partners, and customers. This individual should also handle the monitoring of social media.

v. **Legal:** The general council or a deputy member of the legal team, this individual advises on the need to disclose incidents, such as a breach, and deals with any of the fallout resulting from the security incident, such as shareholder or employee lawsuits.

vi. **Human Resource Representative:** This position is typically filled by the head of HR, who can manage any personnel-related issues that occur, especially if they involve insider theft. The HR representative also gives suggestions for how incidents are communicated to employees.

3.5 Developing an Incident Response Plan

Creating an IR plan is the first thing a CSIRT should do. Organisations that lack experience can hire a consultant to help draft the plan. It is essential that the team be fully staffed and participate in the plan creation–even if it's done with an external consultant—so that the CISRT team has fa miliarity and a sense of ownership.

Here are the critical steps in developing an Incident Response Plan (IRP). (It doesn't matter if these are slides or documents or spreadsheets.) The most important thing is that the plan is easy to find during the panic of a potential crisis, and simple to understand for by someone who is overwhelmed.

i. Gain executive buy-in: Your team leader will be the one to spearhead gaining executive buy-in. If this individual is a member of the executive team such as the CIO or CISO, then this step will be easier. Make sure the CEO, CFO (who may deal with investors), chief counsel, and other key members of the executive team are informed and in agreement on the charter. The CSIRT will be looking at sensitive information and communicating delicate details, so the team must be trusted and supported at the executive level.

ii. Confirm roles and responsibilities: Based on the staffing guidelines above, confirm what all the role is and ensure that everyone agrees. Establish a backup for each role in case someone is on vacation or otherwise unreachable. Importantly, get agreement from your CEO or other executives when executive approval is needed, and decide on what situations the CSIRT can act on its charter.

iii. Document critical assets: Map out your critical systems and intellectual property. Understand the value of source code or web properties. Know the financial impact of a network going down. You want to know the impact on the business when something goes down or goes missing, such as critical data. One critical asset is your customer database. There may be breach notification requirements and even penalties. Examining reports from past audits may also be useful in this step.

iv. Establish a communications plan and protocol: Establish how the team will communicate. For example, we had a crisis where half the incident response team was waiting on a conference bridge, and the other half was waiting on Slack. In such a case, who would initiate the call? Who would initiate it if that person was not around? How often should you provide updates to the executive team? When would you need to get permission from an executive who was not on the team? Ideally, consider all scenarios and work out approvals in advance.

v. Draft core communications in advance: List all your potential incidents in advance, such as theft of customer data, critical system compromise, network or site down, cyberbullying by an employee, and so on. Then draft potential tweets for social media, short statements for the press, and even a press release for a serious incident that requires legal disclosure. Previously, these were called "drawer statements" as they were kept in the desk drawer for emergencies. Once drafted, have them vetted and approved by your legal team– that way, you don't need approvals in the middle of a fire drill.

vi. Prepare by conducting drills: Like the communications issues we mentioned above, many things can go wrong or fall through the cracks during a crisis. Have your team leader organise periodic drills and walk through your process. It will not only highlight potential issues, but drills also give the team more confidence.

vii. Socialize the CSIRT charter to the company: First, have your CEO and executive team review and approve the CSIRT's charter and draft plan. Once you have approval, let your company know about the CSIRT and its charter. Also, let the company know how you will be communicating with during a public security incident. The last thing you want is every salesperson in the company emailing your PR person (or worse, your CEO) asking about what is happening. Lastly, make it clear that only members of the CSIRT will be writing and disseminating communications to customers and partners.

Ultimately, you will learn from experience that it is essential that you continually collect feedback and refine your process. This may involve making some adjustments, such as adding or changing team members and changing how you communicate.

Security incidents will happen that are outside of your control. How you build a CSIRT team dedicated to dealing with these incidents will depend on you.

3.6 Discussion

Assuming you're short-staffed in your organisation, discuss the best way to implement an incident response process.

3.7 Case Study

During routine maintenance of the database server, Jim noticed a new administrator account that had been created a week ago. It didn't belong to anyone in the database team and could be a sign of a security breach. He starts a ticket and calls his CISO. The CISO evaluates the situation and decides to contact a specialized cyber-crime consultant for assistance. Over the next few days, they find evidence that an attacker had compromised a workstation then moved laterally through the network. The attacker had uploaded 20 TB of sensitive data from the network. Many parties had to get involved: the IT department, the CISO, the CEO, the legal team, the outside cyber-crime consultant, the FBI, the state police, the cyber-insurance company, and the public relations team, to name a few. The incident took several months to resolve and caused an impact on the company's reputation and finances.

4.0 Self-Assessment Exercise(s)

1. To build your CSIRT team, there is a list of talents needed, choose some of those talents below:
   a) **Executive manager**
   b) Incident Manager
   c) Communication and Public Relations
   d) Human Resource Representative
   Answer: a

2. Some of the mechanisms for creating CSIRT include:
   a) Provide early warning
   b) Detect & Identify the activity
   c) Draft core communications in advance
   d) Develop mitigation & response strategies

   Answer: c

3. Following are different structures that could be adopted in designing CSIRT except:

   a) Centralized SOC
   b) Coordinating CSIRT
   c) CSIRT/SOC Hybrid
   d) Outsourced CSIRT

   Answer: a

5.0 Conclusion

A Computer Security Incident Response Team (CSIRT) is a group of IT professionals that provides an organisation with services and support surrounding the prevention, management, and coordination of potential cybersecurity-related emergencies. The overarching goals of a CSIRT include responding to computer security incidents to regain control and minimize damage, providing or assisting with effective incident response and recovery, and inhibiting computer security incidents from reoccurring. Security incidents will happen that are outside of your control. How you build a CSIRT team dedicated to dealing with these incidents will depend on you.

6.0 Summary

A CSIRT is an organised entity with a defined mission, structure, roles, and responsibilities. This assumption excludes any ad hoc or informal incident response activity that does not have a defined constituency and documented roles and responsibilities. This assumption is driven by the belief that without a formalized incident response capability, it is not possible to deliver an effective incident response. This unit, therefore, identified the structures in creating CSIRT. It illustrates different approaches and mechanisms for building CSIRT.

7.0 References/Further Reading

Baybutt. P., (2003). A Scenario-based Approach for Industrial Cyber Security Vulnerability Analysis. A paper downloaded from http://www.primatech.com/images/docs/paper_a_scenario_based_approach_for_industrial_cyber_security_vulnerability_analysis.pdf

CERT. Handbook for Computer Security Incident Response Teams (CSIRTs) CERT.

Defining Incident Management Processes for CSIRTs: A Work in Progress SANS.

Incident Handling Step-by-Step and Computer Crime Investigation: Book 1 CERT.

"CSIRT Code of Conduct." Materials from the course Managing Computer Security Incidence Response Teams(CSIRTS).

Kouchakji, J. (2016). Pentesting vs Vulnerability in Typical Application Scenarios, An Article Published by Cybrary, downloaded from https://www.cybrary.it/0p3n/pentesting-vs-vulnerability-assessment-typical-application-scenarios/

Leighton R. Johnson III, Computer Incident Response and Forensics Team Management*, 2014.*

Proffitt. T. (2007). Creating and Managing an Incident Response Team for a Large Company. A Paper from the Information Security Reading Room, SANS organisation. Accessed from https://www.sans.org/reading-room/whitepapers/incident/creating-managing-incident-response-team-large-company-1821

Unit 3: Computer Security Incidence Response Team (CSIRT) Development

Contents

1.0 Introduction

A CSIRT is a team of incident handlers, built to be more cross-functional and aid all departments with all types of incidents. This could include handling legal issues, communicating with the press, or working with human resources on behalf of the organisation as a whole. The Computer Security Incident Response Team's (CSIRT) function is to react in a timely fashion to intrusions, types of theft, denial of service attacks, and many other events that have yet to be executed or considered against their company. The CSIRT will be responsible for investigating and reporting malicious insider activity, internet spam, human resource violations, and copyright infringements. With these functions, there is a need to have a basic understanding of the development of plans, procedures, and policies. Can you give a literal definition of Policy and Procedure?

2.0 Intended Learning Outcomes (ILOs)

By the end of this unit, you will be able to:

- define and create essential policies to guide the CSIRT
- describe the essentials of developing IR
- describe the basic infrastructure needed for coordinating responses.

3.0 CSIRT Development

3.1 CSIRT Policies and Standards

Policies are documented principles adopted by the management team. The entire workforce should clearly understand the policies of an organisation and the knowledge of the incident response policy will allow the CSIRT to act on their responsibilities.

Incident Response Policy

Building an incident response policy involves several objectives. First, an Incident Response Policy cannot be enforced unless it has management approval. Endorsement by management is critical. Without this approval, the team will be destined to encounter business road bocks that will hinder a timely incident response. In some cases, it may not even be allowed. Second, the policy must be clear. Any employee should be able to understand what the policy is about easily. If a non-technology oriented employee is confused by the policy, then the policy should be rewritten.

Third, the policy must be to the point. A long-winded policy will either be a bad policy or one that would include sections that should be in a procedure document instead. Fourth, the policy must be usable and implementable. Avoid statements that sound appropriate but will be open to interpretation. At the same time, the policy should not include objectives that the CSIRT will not be able to execute due to business processes or corporate culture. Once the policy has been created, it is essential to make regular checks against its effect on the workforce. When changes occur in the business direction or new technology systems are implemented, update the policy to match the new processes.

From what we have learned about Incident Response Policy, how does it differ from Incident Response Standards and Procedures?

A successful CSIRT is a team that has documented standards and procedures. Standards should be written from how the CSIRT will begin its investigations and report the findings to standards written for how the CSIRT will be trained and what authority the members will be granted. A good standard will define when the CSIRT will contain and clean up incidents and when the team will watch and gather information for litigation. Having proper recovery procedures are essential. It is very rare to find a CSIRT member that has mastered every operating system and application in your environment. Having procedures to follow on how to correctly down and restore a system can help prevent time-consuming efforts and alleviate some of the stress of the incident. These written procedures will aide the CSIRT in formalizing how investigations are carried

out, how evidence is handled, what organisations are notified at what times, how post mortem reporting is conducted, how malicious software is to be eradicated, and how to perform a recovery of an information system.

Code of Conduct

The code of conduct policy for the CSIRT is a set of rules outlining how a team member will behave in a way that supports the goals of the incident response team and the mission statement of the company. The code of conduct will be used when no other policy or procedure applies. It should reflect the natural behaviour of a professional incident handler.

Disclosure Policy

It is important to define the CSIRT disclosure policy. Without the policy, the team will have no guidance on who to disclose to, what to disclose, and when to disclose the information. Traditionally, CSIRT staff treated all information reported to them as confidential, and information around security incidents was not distributed to other organisations. In some cases, law enforcement or other response teams were included when coordinating the response to the incident. The policy should outline the information disclosure restrictions placed on the CSIRT staff.

What will be reported to law enforcement?

If the incident involved the disclosure of personally identifiable information, when do you disclose to the affected individuals? Personal information includes, but is not limited to, information regarding a person's home or other personal address, driver's license, marital status, financial information, credit card numbers, bank accounts, parental status, sex, race, religion, political affiliation, personal assets, home or other personal phone numbers, and so on.

Did the incident involve the disclosure of electronically protected healthcare information as defined in HIPAA?

Did the incident involve social security numbers?

If the CSIRT is to engage law enforcement, can the business afford to have equipment confiscated?

The disclosure policy will specify (sometimes legal) limitations that outline how or when law enforcement is notified; customers are notified, external CSIRTs, and upper management.

The timing of a disclosure event is imperative. It is important to perform incident investigations and be as certain as possible about the disclosure events. At the same time, the CSIRT should be notifying the victims as soon as possible. If the duration between the identification and the notification

is too great, the company can face litigation and even greater loss of public opinion. The CSIRT must utilize the legal counsel when drafting a disclosure communication to anyone as this notification can have enormous consequences to the company's reputation. `

Disclosure Procedures to External CSIRT

There will be times where the company CSIRT will want to notify external CSIRT, such as the CERT/CC, FIRST, or private Managed Security Solutions Partners (MSSP). To be successful, coordination must occur among law enforcement, National CSIRTs, and the research community who have experience in responding to security incidents. External CSIRTs can play an important role by helping their constituents protect their systems, detect, identify, and analyse compromises to the security of those systems and effectively coordinate the response to the attack. External CSIRT teams can also be evangelists in promoting and helping other organisations build effective incident management capabilities.

The details for sharing of information will change depending on the incident and how the external CSIRT will benefit from the information. Information is typically disclosed to:

- Inform other CSIRT of a large attack.
- Inform other teams about a new vulnerability or attack vector.
- Contact other sites that are the target of an incident to help coordinate the remediation.

Procedures should be clearly written for the internal CSIRT to follow when submitting an incident outside the organisation. When reporting intruder activity, it is important to ensure that you provide enough information for the external CSIRT to be able to understand and respond to your report, but still, filter any information that would be considered sensitive to the company.

Evidence Handling Procedures

During the CSIRT's active services, it is important to track information about the incident. This tracking of information should be at a level of detail that can be useful for recalling the event years later. Handling procedures should record information in logically organised methods to provide historical records and actions taken by the team. In many cases, this information can be used for statistical reporting purposes in management reports.

For every incident, best practices capture and track, at a minimum, the following set of information:

- Local Tracking Number/External CSIRT Tracking Number
- Category of Incident
- Disclosure, Hacking Attempt, Worm Outbreak, Malicious Insider, etc.
- Brief Description
- Contacts for all Parties Involved
- Subjective Priority
- Critical, High, Medium, Low, Informational
- Evidence Gathered
- who, what, where, why, how, when
- History of Actions
- Record all actions by the team.

This will be important if litigation is an optional outcome.

- Current Status of the Incident
- Active, On Hold, Complete, etc.

CSIRT should utilize electronic collaboration tools such as a Microsoft SharePoint Server.

Team members should have a single point to deposit, search, and update data on incident activities. Additionally, incidents should be archived for some predetermined period, using the collaboration tool. The SharePoint tool allows for a repository of electronic data, online workflow capabilities, versioning, automatic alerting, and very flexible role-based access for team members and additional stakeholders outside the team.

Physical evidence should be maintained in a designated "war room." An empty office or conference room can be converted into a CSIRT war room with the understanding that the team will have sole access to a physically secured room. Locking cabinets for hard drives, tapes, and notes on the tracking of the equipment are a must.

3.2 Primary Phases of the CSIRT

The functions that the CSIRT performs during active services are going to be considered the heart of the CSIRT mission. These primary functions are the preparation, identification, containment, eradication, recovery, and lessons learned.

a) Identification

How does the company detect an event? What triggers the CSIRT into action? The answer for most is a mixed one.

– Technology departments deploy intrusion prevention sensors, monitor firewall logs, review honeypot activity, analyse antivirus alerts, review vulnerability assessment reports, examine authentication events, etc.
- Business units will typically educate and raise awareness about security risks to make the workforce use their eyes and ears to identify suspicious activity.

When either of these groups detects an event, the CSIRT should be notified.

i) Triage Role

The goal of the triage role is to ensure that information about an event is gathered from a single point of contact. The triage role is the primary contact for the CSIRT for the business. Contacted by email, fax, telephone, anonymous form, or hallway conversation, the triage role will kick off the incident procedures by calling into action the correct team members to start the investigation. The company should be trained on how to report information to the CSIRT. The triage role should be clearly defined; contact methods should be easily accessible, simple and defined procedures for reporting and clear guidelines on types of events to be reported.

ii) Identification Tasks

The CSIRT should have a member of the management team as its sponsor. This is typically the CSO, CIO, or VP over the technology department. Notify your sponsor that an investigation has started. If additional resources are needed outside the CSIRT, the sponsor will help with obtaining what is needed. It is in the identification function that a primary incident handler should be assigned. The responsibility of the primary handler is to ensure coordination, documentation, and communication with the CSIRT and any other departments or organisations directly involved. The primary handler will be responsible for the quality of the incident handling procedures for the assigned event.

The information gathered in this identification phase is critical. The first goal of the team is to determine whether the incident reported is actually an incident. The team will be asking assessment questions such as, what are the affected systems, if a vulnerability is present, the value of the system to the business (i.e., mission-critical), can the vulnerability be exploited remotely, was this incident user error, was data exposed to unauthorized individuals, does this incident affect companies outside our own? Be sure to establish a good chain of custody scenarios. Document the "who, what, where, when", whenever possible. Each piece of evidence must be under the control of a CSIRT member at all times and document the storage of evidence

if it is secured. The chain of custody will be important for law enforcement if the evidence is going to be used in litigation.

b) Containment

The containment function is designed to prevent the attack from affecting systems, people, or organisations any more than it has already. The CSIRT is now trying to keep the scenario from getting worse. A decision must be made when entering the containment phase. If evidence collected is going to be used for litigation, care must be taken to keep the system(s) from becoming contaminated by the containment efforts. Drives should be imaged, backups performed, original copies secured, etc. Always use a backup or a copy to perform the incident handling procedures. The CISRT should perform multiple backups as soon as it is practical. The backups can be used for forensics or in the off chance that containment procedures render the system(s) inoperable. In most cases, original media will be catalogued and secured, while a backup copy will be used to restore the system for eradication and recovery. The containment phase can involve many tasks: Patching systems, password changes, firewall rule changes, account management, stopping of services, and RootKit/Antivirus system scans. On the employee side, the CSIRT may place phone calls to halt a business process, obtain paper materials or printouts that contain false information or send a corporate-wide communication to alert the workforce.

c) Eradication

The eradication phase involves the removal of any malicious activity or artefacts left by the intrusion. Typically eradication engages in removing virus infections, backdoor software, data left by the intruder, and uninstalling attack tools. If the system was hit with any flavour of a rootkit, formatting hard drives, reloading the system, patching, and restoration from backup is highly recommended. Vulnerability assessment and analysis is typically performed during the eradication phase. Initiating system and network-level vulnerability scans will help the team find open vulnerabilities. In many cases, attackers often use the same vulnerability across the entire network. A quality scanner such as Qualys or Foundscan can go a long way in providing your CSIRT will vulnerability data. The CSIRT should research the vulnerability against the known information repositories such as CERT or BugTraq to understand the impact of the exploit against the company. Improving the defences of the systems or business processes affected is vital. New firewall rules, host-based intrusion prevention technologies, upgrades to more secure applications, and patching are good techniques for improving the defences. If the vulnerability is not removed, the system can become compromised all over. A business process can be

strengthened by objectives such as implementing the least access principles, encryption mechanisms, and social engineering awareness.

d) Recovery
The recovery phase is used to bring the restored system(s) back into production. Recovery will typically take place, according to the system owner, after business unit testing has been conducted. Monitoring is an important objective during this phase. When the incident system(s) are brought back into production use, monitoring must be conducted to validate the eradication was successful. Auditing the operating system logs, intrusion detection or prevention logs, checking for backdoor ports, reviewing firewall logs, and searching for any new vulnerabilities are standard procedures.

e) Lessons Learned
The best way to improve on a company's defence is to learn from the mistakes made. The goal of the lessons learned reporting is to finalize the CSIRT documentation and create a post mortem report for review. In most cases, a meeting is scheduled within a week to review the report. The report should focus on events leading up to the incident, generally what occurred, what was done to contain and eradicate, and what can be done to mitigate the vulnerability in the future. The reporting phase is a good time to note organisational problems that conflicted with the CSIRT's procedures and suggest improvements. Invite the correct management, stakeholders, and information technology individuals to expose the CSIRT's efforts better. The lessons learned meetings could be a good place to obtain approval to fix business processes, obtain newer technologies, update incident handling procedures, and educate the business. It is important to have the CSIRT members involved in the incident complete the lessons learned documentation as close to completing the incident as possible. These post mortem reports should be short but professional and designed for executive consumption.

3.3 Communication among CSIRT Members

Operational principles must ensure that CSIRTs can operate independently from other actors' vested political and commercial interests. CSIRTs need to assess reported vulnerabilities and threats as a neutral party without a hidden or specific political agenda.

A major challenge that the CSIRT community faces is ensuring that existing relationships among its practitioners will continue to scale as more and more users and devices connect to the global network. Another challenge is to manage and integrate the growing number of government-driven CSIRTs into the existing governance system.

It is only a matter of time until news breaks of the next big cyber incident. In recent years, the steady drumbeat of incidents has shown that cyberspace has become an environment rife with competition and conflict, but many cybersecurity threats, such as common viruses or botnets, affect just about everyone. The work of CSIRTs is an effective reminder that we should leverage common interests in keeping cyberspace safe and create a strong foundation for cooperative structures to emerge.

It is necessary to build relationships and establish means of communication within the incident response team, with other groups within the organisation (e.g., human resources, legal departments) and with external stakeholders (e.g., other incident response teams, law enforcement, IT-department of the customer organisation, software vendors). In practice, many informal networks exist, in which, for instance, members responsible for the technical details of incident response share strategies and methods for mitigating attacks. During attacks, these networks enable team members to coordinate an incident response with operational colleagues at partner organisations. Moreover, during the same incident, team managers may seek advice and additional resources for successfully responding to the incident at the government level.

3.3.1 Communication Techniques

Attackers may seek to read or listen to IR team and executive team communications to learn about your company's tailored tactical responses, your investigation and your efforts to stop their attack. Reduce the risk that this may happen. A robust IR plan should include communication techniques that operate outside regular company communication methods (so-called "off-band" communications methods). Information about off-band communication methods must not be included in your IR plan, in case of attackers get hold of the plan. Prepare an ancillary document for a very limited team; do not widely publicise it in your organisation or to an entire IR team. Types of off-band communications: email, internet, computers, phones and messaging.

i. EMAIL

Attackers may have access to email from several vectors, including direct access to email accounts on a company email server, or by having control over computers or other devices on which employees access company email accounts.

- IR team and executive team members should have non-company email accounts with multi-factor authentication activated.
- Many well-regarded free email service providers offer *two-factor authentication* at no cost.

- *Do not use regular personal email accounts* - use accounts created solely for this limited purpose and discontinue use after a major security incident.
- *Do not circulate a list of off-band email accounts via company email*. Store copies in a location that attackers are less likely to access (e.g., a hard copy at home).
- Be cautious when writing emails.
- Off-band email communication could still be compromised if attackers have control over computers; always use caution about what you write in emails – this is especially the case for IR team and executive team members. *Before you click send*, assume an attacker will read the email.
-
- Even this imperfect solution significantly decreases company risk during an IR.

ii. INTERNET

Attackers may intercept network traffic via wireless or wired networks. IR team and executive team members (or the company as a whole) should access off-band email accounts other than from regular company wired or wireless Internet access.

- Consider MiFi hotspots, a DSL line, or mobile phone hotspots that are *not on regular company ISP service accounts*.
- Consult with technical security experts about the safest method.
- Do not use an insecure wireless network at a public location, such as a library or a coffee shop.
- Assume executives' or IR team members' home networks may also be compromised.

iii. COMPUTERS

Attackers may have compromised your laptops, desktops, or other devices in addition to your systems and network. Even if an employee uses off-band email via an off-band Internet connection if the employee's laptop is compromised, an attacker could still potentially monitor the employee's communications on that compromised laptop.

- IR team and executive team members as well as critical IT and IS staff should have separate hardware (laptops or tablets) that can be used during a security incident and then decommissioned.
  - Many relatively low-cost options exist for purchasing barebones laptops or tablets that can be used to access off-band email via off-band Internet connections.
  - Don't use this hardware for other purposes to reduce the likelihood that attackers could compromise it.

- Store the hardware in a safe place and bring it out only in the event of a security incident
- Assume that personal laptops or tablets that were used to access company email, company networks, or by the executive team for personal use may have been compromised.

iv. *PHONES*

Attackers may have compromised a company's phone systems and mobile devices.

- IR team and executive team members should have spare phones that can be used during a security incident.
- Inexpensive non-smart phones with prepaid service are one solution; also available are well-reputed phone-call apps with encrypted phone call options.
- Consult with technical security experts about the best option for you based on your company's landline phone system and employees' mobile phone devices.

v. *TEXT MESSAGING AND INSTANT MESSAGING*

Attackers may have access to messages from several vectors, including mobile phones, computers, or other devices on which employees send text messages or instant messages. Consult with technical security experts about these and other communications options.

3.3.2 Rules Guiding the Communication by CSIRT

i. Have Off-Band Communication Methods on Standby

Companies should have off-band communication methods on standby for possible use during an actual or suspected security incident. Again: do *not* list the off-band email addresses in your IR plan in case attackers get hold of the plan. Prepare an ancillary document for a small subset of people; do not widely publicize it in your organisation or to an entire IR team.

ii. Select The Right Off-Band Communication Methods In Advance

Technical security experts who understand your company's regular communication methods should advise you in determining the right off-band communication methods for your company. The examples listed below serve as a guide, but may not necessarily be right for each company. Off-band communication method choices should be both safe and *usable*. An extremely secure communications method is *not* an effective option if it is difficult to activate.

iii. Not All Your Off-Band Communication Methods are Necessary in Every Incident

During an actual or suspected security incident, technical security experts should determine which off-band communication methods to use based on the characteristics of the specific security incident at hand. Not all off-band communication methods will be required every time.

iv. Continue Using Your Regular Communication Methods

Keep using regular communication methods, such as your conventional email and instant messages. This will help you avoid tipping off attackers to the fact that your executives or IR team are using off-band communication methods.

As in any situation where litigation is possible, counsel will advise the company on litigation hold requirements (i.e., not to destroy potential evidence) according to established protocols. Off-band communications would be subject to the same litigation hold requirements as regular company communication methods.

3.4 Discussion

Information about off-band communication methods must not be included in your IR plan. Discuss extensively.

3.5 Case Studies

Your company is in crisis mode in the throes of a security incident response (IR). But you are calmly executing your well-honed IR plan – a plan you developed and tested during mock exercises over the past year. You are confident in your team's ability to triage the incident and your technical security experts' ability to stop the attack. You know you will return your company to its fully operational state as soon as possible.

One of the first steps in your IR plan is to convene an IR team meeting. You have an IR team email distribution list at the ready, which saves valuable time. You send a calendar invite to your IR Team for 2:00 – 3:00 PM ET with the dial-in conference number, code, and – because you are prepared – a single-use password just for this call.

Your executive team, IT and Information Security leads and other IR team members convene in your board room and dial into your conference line from different locations.

Scenario

As you get ready for the meeting, here are some questions to ponder.

Do you mind if the attackers dial into the conference call too?

If attackers have infiltrated your network, they may have access to company email and other communication methods, including your IR Team

Do you mind if the attackers launch secondary attacks during the meeting?

If attackers know your best IT/IS staff are in a meeting, they may seize the opportunity to launch a second wave of attacks while your systems are not being monitored closely.

Do you mind if the attackers follow along with your IR Plan playbook?

If attackers have obtained a copy of your IR plan playbook, they will know where you are looking and – perhaps more importantly – where you aren't *looking.*

4.0 Self-Assessment Exercise(s)

1. The following objectives are required in building an incident response policy except:
   a) it cannot be enforced unless it has management approval.
   b) It must be unambiguous.
   c) It must be usable and implementable.
   d) It must be complete
   Answer: d

2. One of the following is not the type of off-band communications

   a) email
   b) router
   c) computers
   d) messaging

   Answers: b

5.0 Conclusion

Computer security incident response teams (CSIRTs) play an important role in responding to incidents and achieving its benefits. Incident response teams can be formalized, such that performing incident response is its major function. These teams can also be more *ad hoc* in nature, in that members are called together to respond to an incident when the need arises. Usually, these members work in IT-departments within the organisations themselves. After an incident has been detected, one or more team members, depending on the familiarity and magnitude of the incident and availability of personnel, will initially handle the incident. Ideally, the team analyses the incident data determines the impact of the incident and acts appropriately to limit the damage and restore normal services

6.0 Summary

This unit presents comprehensive details on policies that guide CSIRT on their assigned roles and responsibilities. It enlightens students om the different types of standards and procedures to follow in developing the CSIRT. Basically, all essentials needed in organising and preparing the CSIRT were clearly identified.

7.0 References/Further Reading

Cybersecurity Law Alert (2015). Plan now to use off-band communications during an incident response: key points. Published by By: DLA PIPER Publications, 27 OCT 2015 https://www.dlapiper.com/en/us/insights/ publications/2015/10/plan-now-to-use-offband-communications/

Tim Matthews (2018). The Complete Guide to CSIRT Organisation: How to Build an Incident Response Team. Downloaded from https://www.exabeam .com/incident-response/csirt/

Module 4: Crisis Management and International Standards for IR/DR/BC

Module Introduction

With increasing incidents of hacked websites, breached networks, and ransomware and denial-of-service attacks, cybersecurity is transforming from an operational challenge into a business challenge. It is not possible to completely shield a business from cyberattacks, but you can create a crisis management plan to deal with them in unfortunate times. Having a cybersecurity crisis management plan will help you respond more quickly to cyberattacks, deliver coherent and consistent internal and external communications, and take timely remedial action.

Crisis management is a critical organisational function, of which its failure can result in serious harm to stakeholders, losses for an organisation, or end its very existence. Public relations practitioners are an integral part of crisis management teams. So, a set of best practices and lessons gleaned from our knowledge of crisis management would be a beneficial resource for those in public relations and those in the research world. The study of crisis management originated with large-scale industrial and environmental disasters in the 1980s. It is considered to be the most important process in public relations.

This module shall be considering the key roles played by the stakeholders in Information Technology and cyberspace. It will also examine the different stages for managing and responding to the crisis. This lesson will critically look to study the standards that guide all plans for managing crisis in organisations. The study shall, however, be restricted to crisis management related to cybersecurity and information technology.

The module is broken into the following units:

Unit 1 Role of Crisis Management
Unit 2 Element of Plan to prepare for Crisis Response
Unit 3 International Standards for IR/DR/BC

Unit 1 Role of Crisis Management

Contents

1.0 Introduction

A crisis is a situation that poses a threat to the organisation's very existence. If the situation is not resolved, the results could be catastrophic to the enterprise. In today's dynamic cyberspace, crises can arise fast and snowball even faster, driven by a set of multimedia, the presence of social media, and access to information and opinion that may not be accurate or relevant.

A crisis can as well be defined as a significant threat to operations that can have negative consequences if not handled properly. A crisis can create three related threats: (1) public safety, (2) financial loss, and (3) reputation loss. A crisis can create financial loss by disrupting operations, creating a loss of market share/purchase intentions, or spawning lawsuits related to the crisis. A crisis reflects poorly on an organisation and will damage a reputation to some degree. Clearly, these three threats are interrelated. Injuries or deaths will result in financial and reputation loss, while reputations have a financial impact on organisations.

In crisis management, the threat is the potential damage a crisis can inflict on an organisation, its stakeholders, and an industry.

A crisis can arise in an organisation due to any of the following reasons:

- Technological failure and Breakdown of machines lead to crisis. Problems in the internet, corruption in the software, errors in passwords all result in a crisis.
- Violence, thefts, and terrorism at the workplace result in organisation crisis.

- Neglecting minor issues, in the beginning, can lead to major crises and a situation of uncertainty at the workplace. The management must have complete control over its employees and should not adopt a casual attitude at work.
- Illegal behaviours such as accepting bribes, frauds, data, or information istampering all lead to organisation crisis.
- A crisis arises when an organisation fails to pay its creditors and declares itself a bankrupt organisation.

Managing a crisis means being proactive and fast, focusing on rapid resolution and recovery that is effective. It also means clear, effective communication that is sent to stakeholders, shareholders, regulators, the general public, and employees via multiple media and messengers.

2.0 Intended Learning Outcomes (ILOs)

By the end of this unit, you will be able to:

- explain the crisis and its management concerning cybersecurity
- describe the benefits of crisis management to business and organisation in general
- describe the role of the Crisis Management Team in comparison with other Emergency Response Teams.

3.0 Overview of Crisis Management

3.1 Definition

Crisis management is the process by which an organisation deals with a disruptive and unexpected event that threatens to harm the organisation or its stakeholders. In contrast to risk management and Incident management, crisis management involves dealing with threats before, during, and after they have occurred. It is a discipline within the broader context of management, which consists of skills and techniques required to identify, assess, understand, and cope with a serious situation, especially from the moment it first occurs to the point that recovery procedures start.

Crisis management is a situation-based management system that includes clear roles and responsibilities and process related to organisational requirements company-wide. The response shall consist of action in the following areas: Crisis prevention, crisis assessment, crisis handling, and crisis termination. The aim of crisis management is to be well prepared for a crisis, ensure a rapid and adequate response to the crisis, maintaining

clear lines of reporting and communication in the event of crisis and agreeing with rules for crisis termination.

The techniques of crisis management include a number of consequent steps from the understanding of the influence of the crisis on the corporation to preventing, alleviating, and overcoming the different types of crises. Crisis management consists of different aspects, including:

- Methods used to respond to both the reality and perception of crisis.
- Establishing metrics to define what scenarios constitute a crisis and should consequently trigger the necessary response mechanisms.
- Communication that occurs within the response phase of emergency-management scenarios.

Can you differentiate between Incident Management and Risk Management?

3.2 Stages Involved in Crisis Management

According to Gonzalez-Herrero and Pratt, crisis management includes the following three stages:

i. Diagnosis of Crisis

The first stage involves detecting the early indicators of crisis. It is for the leaders and managers to sense the warning signals of a crisis and prepare the employees to face the same with courage and determination. Superiors must review the performance of their subordinates from time to time to know what they are doing.

The role of a manager is not just to sit in closed cabins and shout on his subordinates. He must know what is happening around him. Monitoring the performance of the employee helps the managers to foresee the crisis and warn the employees against the negative consequences of the same. One should not ignore the alarming signals of crisis but take necessary actions to prevent it. Take the initiative on your own. Don't wait for others.

ii. Planning

Once a crisis is being detected, the crisis management team must immediately jump into action. Ask the employees not to panic. Devise relevant strategies to avoid an emergency situation. Sit and discuss with the related members to come out with a solution that would work best at times of crisis. It is essential to make quick decisions. One needs to be alert and, most importantly, patient. Make sure your facts and figures are correct. Don't rely on mere guess works and assumptions. It will cost you later.

iii. Adjusting to Changes

Employees must adjust well to new situations and changes for the effective functioning of organisation in the near future. It is important to analyse the causes, which led to a crisis at the workplace. Mistakes should not be repeated, and new plans and processes must be incorporated into the system.

Following are the needs for Crisis Management:

- Crisis Management prepares individuals to face unexpected developments and adverse conditions in the organisation with courage and determination.
- Employees adjust well to the sudden changes in the organisation.
- Employees can understand and analyse the causes of the crisis and cope with it in the best possible way.
- Crisis Management helps the managers to devise strategies to come out of uncertain conditions and also decide on the future course of action.
- Crisis Management helps the managers to feel the early signs of crisis, warn the employees against the aftermaths, and take necessary precautions for the same.

3.3 Crisis Management Team: Roles

A Crisis Management Team (CMT) is formed to protect an organisation against the adverse effects of the crisis.CMT prepares an organisation for inevitable threats, where a decision is made on the future course of action and devises strategies to help organisation come out of difficult times as soon as possible. The Team is formed to respond immediately to warning signals of crisis and execute relevant plans to overcome emergency situations.

Crisis Management team primarily focuses on:

- Detecting the early signs of crisis.
- Identifying the problem areas
- Sit with employees face to face and discuss the identified areas of concern
- Prepare crisis management plan which works best during emergency situations
- Encourage the employees to face problems with courage, determination, and smile. Motivate them not to lose hope and deliver their level best.
- Help the organisation come out of tough times and also prepare it for the future.

The main role of the team (CMT) is to support the regional, site, and the associated emergency management teams. This high-level corporate team should manage human impacts (both employees and the community), company reputation, share values, and corporate assets. Depending on the assigned responsibilities, the CMT should be empowered to make strategic decisions to advance the response and provide direction and guidance to response teams and the rest of the organisation.

The role of the Crisis Management Team is to analyse the situation and formulate a crisis management plan to save the organisation's reputation and standing in the industry.

Other roles include:

- People on the CMT need to have a global view of the organisation as well as a good understanding of the potential impacts and needs of their specific area.
- Apart from the leader, people on the CMT act as advocates for their area; they gather information on that area and make sure the impacts to it are understood and given due priority. They lead or direct the recovery or actions for the area.
- In large organisations, each of the areas would likely be filled by one person. In medium and small organisations, the roles might be doubled or tripled up. The important thing is making sure that each area has someone assigned to look after it.
- CMT members are not expected to have all the information for their area of responsibility in their heads. However, they should know where to get their hands on it quickly should the need arise.
- Each CMT member is an advocate – the one who ensures each area's risk and impacts are addressed and considered. They must also be able to consider the overall impacts and understand when other areas or issues take priority.

3.3.1 Functionality of the *Crisis Management Team*

A Team Leader is appointed to take charge of the situation immediately and encourage the employees to work as a single unit. The first step is to understand the main areas of concern during emergency situations.

Crisis Management Team then works on the various problems and shortcomings that led to a crisis in the workplace. The team members must understand where things went wrong and how current processes can be improved and made better for the smooth functioning of the organisation.

It is important to prioritise the issues. Rank the problems as per their effect on the employees as well as the organisation. Know which problems must be resolved immediately.

A single brain cannot take all decisions alone. Crisis Management Team should sit with the rest of the employees on a common platform, discuss prevailing issues, take each other's suggestions and reach plans acceptable to all.

One of the major roles of the Crisis management team is to stay in touch with external clients as well as media. The team must handle critical situations well.

Develop alternate plans and strategies for the tough times. Make sure you have accurate information. Double-check your information before finalizing the plan.

Implement the plans immediately for results. Proper feedback must be taken from time to time.

Crisis Management team helps the organisation to take the right step at the right time and help the organisation overcome critical situations.

Crisis Management Team includes:

- ✓ Head of Departments
- ✓ Chief Executive Officer
- ✓ Board of Directors
- ✓ Media Advisors
- ✓ Human Resource Representatives

3.4 Case Studies

DOMINO'S PIZZA

One of the world's largest pizza chains found itself in a public relations crisis when two employees began posting prank videos on YouTube in 2009. Initially, the company responded according to its previously established crisis management protocol: They posted a response video from the company president on their website. Unfortunately, the video garnered very few views, and the crisis continued to spread. That's when Domino's realized they needed to utilize the same technology platform that had started the incident. If people were viewing the prank video on YouTube, they realised, the response should also leverage the power of YouTube.

The PR team crafted a new, edgier version of the response video and posted it to YouTube. And this new approach worked: Simply by using a different technology that is more widely used by consumers, Domino's was able to reach millions of customers with a clever "viral" video of their own, and the crisis subsided.

Considering this case study, can you describe what could have been done to save the situation from escalating?

For Videos on Crisis Management, visit Developing a Crisis Management Plan in Cybersecurity

http://go.everbridge.com/demorequest.html?utm_expid=.DMjxVVsiRR2o13y06i8DiQ.0&utm

4.0 Self-Assessment Exercise(s)

1. Crisis Management Team consists of:

- Head of Departments
- Executive Directors
- Board of Directors
- Team Leader

a) i and ii

b) i and iii

c) i, ii and iii

d) i, iii, and iv

Answer: b

2. How many stages are involved in Crisis Management?

a) 2
b) 3
c) 4
d) 5

Answer: b

Assignment:
Identify at least two functions for each of the following Crisis Management Team:

1. Head of Departments
2. Chief Executive Officer
3. Board of Directors
4. Media Advisors
5. Human Resource Representatives

5.0 Conclusion

Cybersecurity is a high-risk crisis scenario that keeps many executives up at night, while it's not a crisis scenario that you can ever fully prevent, there are ways to mitigate the long-term impact that this type of crisis threatens to have on your organisation. Having the right IT structures and controls in place is the first step, but from there, you also want to think through and develop comprehensive crisis management strategies and protocols for managing this type of crisis.

6.0 Summary

This unit has provided students with a basic understanding of the crisis and its management concerning Cybersecurity. The general benefits that organisations gain from incorporating crisis management to business have been highlighted. More so, the roles played by the different crisis management teams have been discussed to assisting students in differentiating between crisis management and other management schemes that relate to life and infrastructure threatening.

7.0 References/Further Reading

Course note on Crisis Management Management Study Guide

Esbensen. L. H. and Krisciunas (2008) Crisis Management & Information Technology. Master Thesis, Submitted to Lund University, June 2008.

Gitanjali Maria (2019). How to Create a Cybersecurity Crisis Management Plan in 5 Steps. Published by GetApp, Jul 9, 2019. Downloaded from

https://lab.getapp.com/cybersecurity-crisis-management-plan/

https://www.managementstudyguide.com/crisis-management.htm

https://www.managementstudyguide.com/crisis-management-team.htm

Marcus K. G. Adomey (2016). Introduction to Computer Security Incident Response Team (CSIRT). An Article downloaded from

Richard Long (2018) CMT 101: Crisis Management Team Roles. Published by MHA Consulting

Scott E, Donaldson Stanley G., SiegelChris K. and WilliamsAbdul Aslam (2019) Managing a Cybersecurity Crisis. Published by Enterprise Cybersecurity pp 167-191

Downloaded from https://www.mha-it.com/2018/05/09/crisis-management-team-roles/

Case Study downloaded from https://www.rockdovesolutions.com/blog/3-crisis-management-case-studies-that-utilized-innovative-technology

Unit 2: Elements of Plan to Prepare for Crisis Response

Contents

1.0 Introduction

Crisis management is a process designed to prevent or lessen the damage a crisis can inflict on an organisation and its stakeholders. As a process, crisis management is not just one thing. Crisis management can be divided into three phases: (1) pre-crisis, (2) crisis response, and (3) post-crisis. The pre-crisis phase is concerned with prevention and preparation. The crisis response phase is when management must actually respond to a crisis. The post-crisis phase looks for ways to better prepare for the next crisis and fulfils commitments made during the crisis phase, including follow-up information. The tri-part view of crisis management serves as the organising framework for this entry.

This unit discusses the preparation guide to avert any form of crisis. It elaborates on different planning strategies to adopt for crisis management.

2.0 Intended Learning Outcomes (ILOs)

By the end of this unit, you will be able to:

- advise organisations on how to mitigate the crisis
- prepare a crisis management plan
- explain best practices for creating a cybersecurity crisis management plan.

3.0 Main Content

"Traditionally, "good" crisis management includes three elements: there must be a plan of action, the organisation must have early warning systems to signal potential crises, and the organisation must have a crisis management team in place with the power to act."

These elements are the minimal of crisis preparation. They are not enough when making detailed preparations, but they can be used as a backbone and have some important aspects.

3.1 Responding to a Crisis

Some strategies would be considered in responding to a crisis. The first response strategy is the first step within the crisis plan. When done properly, it can immediately help you begin to regain control of the situation, easing the flow of negative comments and complaints flooding your wall, Twitter feed, inbox, and wherever else the messages may be overflowing into.

The first response strategy is the first public response to the crisis. Where you implement your first response strategy is very important. When released on the right platform, you will begin to regain control of the situation. When released on the wrong platform, it will not affect whatsoever.

The first response to a crisis should always be directed to the platform where the attack or crisis was made. If the crisis first occurred on WhatsApp, then the first response will be posted on WhatsApp. You must keep your first response very brief, having the mind that it is only to cool the situation and buy time too look into the events of the crisis and develop your plan of action.

What to address

There are four main points that you need to address within your first response:

- *You are aware of the situation.* This will alleviate all of the "did you know/are you aware" messages flooding in.
- *You're looking into the situation.* This gives the public ease of mind that you're currently looking into the events of the crisis.
- *You will let the public know as soon as you know more.* You've already assured your customers and fans that you're looking into the situation. Next, you need to inform them that they can expect to hear from YOU as soon as you know more.

- *Thank the public for their understanding and patience.* No time is too soon to show your fans compassion and appreciation. Always end your first response by thanking them for their patience.

When you address each of these issues, there's nothing left for the public to do but settle down and wait for more answers – which you've promised will come from you. This is a big step in regaining control of the situation and giving you time to assess the damage and implement your full crisis plan properly.

An example of a good first response might look something like this:

"We understand that many of you have encountered problem X, and we would like you to know that we are presently looking into the situation and will get back to you with more information as soon as we know more. Thank you for your understanding and patience. – Sign Name."

Your first response must be released as soon as you're made aware of the crisis. The sooner you respond, the sooner you begin to regain control, and the sooner you will be able to overcome and resolve the situation.

Consider the case study in the last unit to know the importance of the highlighted strategies.
Did Domino follow the strategies, as discussed?

3.2 Prepare a Crisis Management Plan

The Crisis Response Plan (CRP) is a brief procedure used to reduce an individual's risk for suicidal behaviour. The CRP is created collaboratively between a suicidal individual and a trained individual and is typically handwritten on an index card for easy, convenient access during times of need. The CRP serves as a checklist to follow during periods of intense emotional distress. At its core, the CRP helps someone remember what to do when they feel emotionally overwhelmed.

The CRP is comprised of five key sections:

1. Personal warning signs: personal indicators of an emerging emotional crisis.
2. Self-management strategies: simple strategies that can be used to help reduce stress or serve as a distraction.
3. Reasons for living: things that provide a sense of purpose or meaning in life.
4. Social support: people who provide support or elevate one's mood during tough times (e.g., friends, family members).
5. Professional crisis support: contact information for health care providers, crisis hotlines, and emergency services.

The CRP usually takes less than 30 minutes to create. An important part of the CRP is helping individuals to cope with intense levels of distress when faced with problems that seem unsolvable and never-ending successfully.

Preparing a robust cybersecurity crisis management plan may take you weeks or months, and it requires the support and approval of top leadership.

Here are five steps to help you prepare your cybersecurity crisis management plan.

1. **Form an emergency cybersecurity incident response team**
   You need to state who will take charge and manage the "firefighting" in the event of a cybersecurity incident. In addition to leading the organisation as it follows the defined crisis management processes, this team will also be involved in creating and updating the crisis management plan.

2. **Define what a cybersecurity crisis means to your organisation**
   Not every security incident is a crisis. You must, therefore, define what qualifies a security incident as a crisis for your organisation. Loss of confidential data; adverse financial or reputation consequences for your business, partners, or customers; and regulatory breaches are some instances when a security incident becomes a crisis.

3. **Create an escalation process flowcharts for crisis situations**
   Visual representations such as flowcharts help employees quickly understand the steps they must take following an incident. Below is a sample flowchart depicting action items that need to be taken when a security incident is reported.

   Your escalation process flowchart must also cover the legal and regulatory aspects of the different security incidents. For example, Article 33 in GDPR requires you to notify the controller about any breach of customers' personally identifiable information within 72 hours.

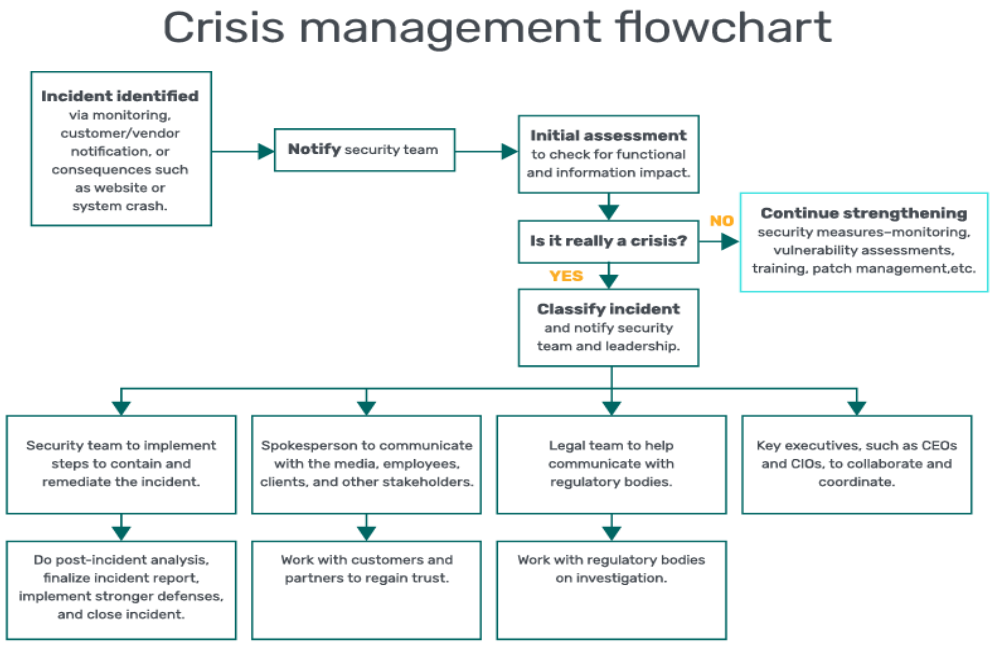


Figure 4.1: Crisis Management Flowchart

Having separate flowcharts to indicate how employees should respond to different types of incidents—phishing, DDoS attacks, malware, IoT attacks—helps create a faster and more targeted response.

4. Create cybersecurity crisis communication templates

You will need to issue communique about security incidents to internal as well as external stakeholders (media, clients, and partners, depending on the severity of the crisis).

Having crisis communication templates ready for different scenarios—serious data breach incidents, minor data breach incidents, etc. - helps save time and avoids incoherent communications. You must also designate spokespersons who are authorized to speak on behalf of your company about the incident. Here's a sample crisis communication template:

Our company, [Company name], has become aware of a potential network and systems breach. At this time, we are unable to confirm the extent of the breach and whether sensitive data is affected. We are working closely with federal authorities and cybersecurity experts to determine and contain the impact of the incident. We are committed to working through this investigation and addressing any concerns our clients or partners might have.

We will provide regular updates on our website, www.companyname.com, and will hold media briefings as necessary.

5. **Create RACI charts and list emergency contact details for speedy communication and collaboration**

Providing timely information to internal and external stakeholders about how the crisis is being handled is an important step. RACI charts help you quickly determine whom to contact or get approval from for different steps in the crisis management plan. Below, we discuss what each element in a RACI chart means:

Responsible: Person who is responsible for executing or doing the activity.

Accountable: Person who owns, approves, and is the final decision-maker for the activity.

Consulted: Person who can provide further information or feedback for performing the activity.

Informed: Person who only needs to be informed about the activity's progress or status.

Here is a downloadable template that you can customize for your incident response plan. We've added columns providing communication details for the relevant stakeholders in the template to help make communication easier and faster.

3.2.1 Best practices for creating a cybersecurity crisis management plan

A crisis management plan is a document that will be referred to under intense pressure and panic. It should not be complicated, forcing a reader to read a step multiple times to understand what to do. Here are some best practices you should follow when preparing your cybersecurity crisis management or incident response plan.

- **Keep it simple and short:** Use simple, actionable language to provide employees with enough details to initiate the correct response.

- **Ensure the plan addresses traditional and new security incident types:** Include distinct flowcharts that show how to tackle common
incidents such as malware or DDoS attacks, as well as listing out generic procedures for tackling new types of security incidents.

- **Keep copies of the plan in a secure yet easily accessible location:** Store physical as well as electronic copies of the crisis management plan with business unit heads or team leads or on cloud storage tools.

- **Test the plan regularly:** Conduct mock drills to check the preparedness of your team and the robustness of your cybersecurity

crisis management plan. This will also help train employees to act quickly and take immediate reactive steps.

3.3 Developing a Crisis Management Plan in Cybersecurity

Step 1: Define the parameters

The first step is to simply start at the beginning and define what a cybersecurity crisis is and means to your organisation. As a high-level starting point, a cybersecurity incident can be defined as "a breach, compromise, or disruption of the organisation's critical data and systems."

Once you have this risk defined, you'll need to determine how your organisation – and the law – defines "critical data and systems." For example, what types of data do you have access to and what are your most critical systems, whereby if either were breached, compromised or disrupted, it would present a crisis or potential crisis to your organisation?

Step 2: Develop your internal escalation process

Not every cybersecurity incident risks rising to crisis levels. Depending on the size and nature of your business, your information security team probably detects issues and potential threats regularly as part of their business as usual activities. So how do you determine whether or not a cybersecurity incident is a "business as usual issue" versus a potential crisis? Who will help your IT team make this determination, and at what point do they get called in to do so?

A good way to approach this, in my experience, is to provide your IT team with a set of questions that they can answer as part of their initial assessment of any given incident. These questions should aim to help them assess the potential business impact of each incident. From there, I usually devise a protocol stating that if the IT team can answer "yes" or "maybe" to X amount of these questions, they are to escalate the incident to a dedicated cybersecurity assessment group. This group should include members of different departments that, together, can assess the full potential impact of a given incident on the business and its stakeholders. From there, if this group deems the situation to be a potential crisis, the protocol should be to escalate the incident to senior management.

One of the main goals of this escalation process is to ensure that the right people have the tools they need to assess the full potential impact of a cybersecurity incident while ensuring that as few "false alarms" as possible get escalated all the way up to senior management. It's both an effective filtering process and a way to make sure that the right people are a part of the initial assessment process when needed.

Step 3: Understand the legal aspects of a cybersecurity crisis

One of the goals of crisis preparedness is to minimise the number of tasks needed to be undertaken in the event of a crisis. This means that if there is work that can be done now that will prove to be beneficial to the team in the heat of the moment, then that work should be outlined and completed.

As cybersecurity crises can come with a lot of legal obligations and ramifications, part of the preparedness process is to set out to understand your organisation's legal responsibilities in the event of a breach. Depending on the jurisdiction(s) of where the incident happens, the type of data that gets compromised and the potential impact on your stakeholders, your organisation will be subject to different legal requirements and timelines. It is your responsibility to understand and adhere to these requirements.

Even if you have a powerhouse of internal attorneys, it’s a good idea to consult with outside counsel on this one. One advantage of doing this is that many of the big legal firms that provide this type of service to their clients already have most of the work done. For example, you’ll find that many of them have created a matrix that details the different rules and laws within different jurisdictions, and that they’re committed to keeping this information current as laws change and evolve.

Equipping your team with the right third-party experts is an important part of being crisis-ready. In the event of a cybersecurity crisis, this list usually includes legal counsel, cyber forensic professionals, insurance providers, and a specialized crisis management consultant.

Step 4: Draft your playbook and crisis communications handbook

The goal is to think through the required tasks and considerations for each member of your crisis team within the first 24-48 hours of a cybersecurity crisis. This should include task considerations, action items, contact lists, timelines, and pre-approved crisis communications.

I find the best way to tackle drafting the pre-approved crisis communications for a complex crisis such as a cybersecurity incident, is to think through the most likely types of scenarios that pertain to your organisation and to draft talking points, stakeholder-specific written notifications, and an FAQ to the most extent possible.

However, one of the challenges with this type of crisis is that you will have two main focuses when it comes to your crisis communications: one focus will be on relationship maintaining (in other words, trying not to lose the trust of your stakeholders), and the second will be your legally required notifications which are very case-specific. With these two focuses in mind, you can draft an outline of the different notifications you would want to use,

including appropriate tone of voice and key message points, and then set parameters for guiding the flow and timelines for communicating with your stakeholders. This isn't an easy undertaking, but with the right help, it's well worth the effort.

Step 5: Put your plan – and your team – to the test

Once you have your crisis preparedness program developed, it's important to test it. Testing the plan with a tabletop – or better yet, a crisis simulation – allows you to detect gaps and strengthen the plan before you need to put it to use. It also helps your team develop muscle memory and crisis management instincts that everybody will be very grateful to have in the event of a real crisis.

Remember: your plan is not complete unless it has been adequately tested. And you certainly don't want to test it during a breaking crisis.

3.4 Discussion

Crisis Management is very important to an organisation. However, are there possible reasons or conditions for neglecting the usage of Crisis Management Plan?

The role of the Incident Response Team in an organisation is not only limited to incidence response, what other roles can the team perform in an organisation? Discuss?

3.5 Case Studies

Mercedes Benz Superdome.

As home to the New Orleans Saints and other big-name events throughout the year, the Superdome regularly hosts tens of thousands of people. Management wanted a better way to communicate with the crowd during a crisis while also improving exterior lighting to optimize safety. They turned to a product called Intellistreets to help solve both challenges.

Intellistreets is an audio and LED signage system that can be installed on streetlight poles in public parks, near stadiums, and around other busy areas. The wireless technology provides emergency response, homeland security, and public safety functions, all in one highly visible location.

At the Superdome, the Intellistreets systems also include a powerful sound system to enable officials to speak directly to the exiting or entering crowds. It also features LED signage that can display emergency messaging and community announcements as needed, creating a simple yet effective way to relay information about wayfinding, evacuation instructions, and more.

4.0 Self-Assessment Exercise(s)

1. One of the best practices for creating a cybersecurity crisis management plan is ensuring that the plan addresses only traditional and past security incident types, true/ false?
   Answer: false

2. The last element in a RACI chart indicates:
   a) intention
   b) information
   c) informed
   d) interest
   Answer: c

3. One of the main points that you need to address within your first response Responding to a Crisis

   a) You are aware of the situation
   b) Define the parameters
   c) Draft your playbook and crisis communications handbook
   d) Create cybersecurity crisis communication templates

   Answer: a

5.0 Conclusion

Responding to crises can be a very challenging process if the experienced team is not solely in charge of the process. The unqualified and inexperienced team may not know what to address or the plan of action to carry out in order to achieve outstanding success. However, if best practices and plans are followed; the team will not take a quite long time to achieve success in crisis management.

6.0 Summary

The three key elements for good crisis management are clearly identified with the main points needed to be identified when managing crises. Cybersecurity incidence teams are always on the increase due to numerous prevalent attacks recorded in the Information world. Also, a flow chart to depict the stages involved in crisis management is also depicted in this chapter.

7.0 References/Further Reading

For more case studies: https://www.rockdovesolutions.com/blog/3-crisis-management-case-studies-that-utilized-innovative-technology

https://lab.getapp.com/cybersecurity-crisis-management-plan/

https://en.wikipedia.org/wiki/Crisis_management

Incident Management for Operations by Rob Schnepp, Chris Hawley, Ron Vidal, Publisher(s): O'Reilly Media, Inc. ISBN: 9781491917619

The Essential Guide to ITIL Incident Management

Unit 3 International Standards for IR/DR/BC

Contents

1.0 Introduction

Standards are generally created by bringing together all interested parties such as manufacturers, consumers, and regulators of a particular material, product, process, or service. The *International* Organisation for Standardisation (*ISO*) is the most significant *standards*-developing and publishing body in the world. It is solely responsible for providing international standard regulating activities and services provided by different incidence response organisations.

International Standards (IS) is a document comprising of established and approved consensus for common and repeated use, rules, guidelines or characteristics for activities or their results, aimed at the achievement of the optimum degree of order in a given context.
This unit details the different aspects of International Standards Organisations Regulations relating to incidence response and management.

2.0 Intended Learning Outcomes (ILOs)

By the end of this unit, you will be able to:

i. describe the various standards provided for Incidence Response, Disaster Recovery and Business Continuity
ii. differentiate between Disaster Recovery and Business Continuity

iii. define and explain the Principles of a Business Continuity Management System
iv. explain and describe the **Plan-Do-Check-Act (PDCA**) model for evaluating a Business Continuity Management System.

3.0 Main Content

Managing incidents effectively involves processes such as detecting and correcting controls designed to recognise and respond to incidents, minimize adverse impacts, gather forensic evidence (where applicable) and in due course 'learn the lessons' in terms of prompting improvements to the ISMS, typically by improving the preventive controls or other risk treatments. The ISO standards on incidence response are contained in a document labelled ISO/IEC 27035, which was published in 2016. The summary of the publications will be discussed in different subsections under section 3.1.

3.1 Information Security Incident Management - Guidelines to Plan and Prepare for Incident Response

3.1.1 ISO/IEC 27035:2016 — Information technology — Security techniques — Information security incident management

This document describes incident management processes into five stages which are:

a. **Planning and preparing for Incidence Response:** Develop information security incident management policy, form an **I**ncident **R**esponse **T**eam, *etc.*
b. **Detection and reporting of Information and Security Incidents:** personnel must be solely in charge of detecting and reporting "events or actions " that might result in incidents;
c. **Assessment and decision on Incident Reports:** Designated team must assess the situation to determine whether it is, in fact, an incident;
d. **Actions and Responses to Combat Security Incidents:** contain, eradicate, recover from and forensically analyse the incident, where appropriate;
e. **Document Lessons learned:** Actions performed to avert incidence and improvements to the organisation's management must be properly documented

3.1.2 ISO/IEC 27035-2:2016 Information security incident management - Guidelines to plan and prepare for incident response

The document, though published in 2016, provides responses to how ready organisations are to respond to security incidents. It also covers the *Plan, Preparations,* and *Lessons Learned* phases of the process to improve incidents response through the following actions:

a. Establishing information security incident management policy
b. Updating of information security and risk management policies
c. Creating an information security incident management plan
d. Establishing an **I**ncident **R**esponse **T**eam [a.k.a. CERT or CSIRT] *etc.*
e. Defining technical and other support
f. Creating information security incident awareness and training
g. Testing (or rather exercising) the information security incident management plan
h. Documenting Lesson learned.

3.1.3 ISO/IEC 27035-3 Information security incident management - Guidelines for ICT incident response operations (draft)

This document is at the Draft **I**nternational **S**tandard stage and should be published *soon* (in 2020). Its scope reads (in part):

"This document provides the guidelines for ICT incident response operations. This document is not concerned with non-ICT incident response operations such as loss of paper-based documents. The guidelines are based on the "Detection and Reporting" phase, the "Assessment and Decision€" phase and the "Responses" phase of the "Information security incident management phases" model presented in ISO/IEC 27035-1:2016."

The document contains a sectionalized procedures to typical incident response process, *i.e*. incident detection; notification; triage; analysis; containment, eradication and recovery; and reporting.

Who provides the most accepted standard for incidence response?

3.2 Business Continuity and Disaster Recovery

The awareness and recognition that businesses and technology executives need to collaborate when planning for incident responses instead of developing schemes in isolation led to the combination of business continuity and recovery.

The main aim in Business continuity is to provide organisation with the ability to function in the event of a disruptive incident by ensuring the most critical business functions continue to operate (even if at reduced capacity) while attending to the disruption.

Similarly, disaster recovery plans are focused on returning an organisaation back to 'business as usual' after a disruptive incident and achieving total recovery.

Business continuity is a more proactive process involving more comprehensive planning geared toward long-term challenges to an organisation's success while Disaster recovery is more reactive consisting of recovery actions take place after the incident, and response times can range from seconds to days.

Figure 4.2: Business Continuity and Data Recovery Planning Stages

3.2.1 Benefits of Business Continuity Planning

Business continuity planning is a very critical issue that takes into consideration what will take the organisation up and running as soon as possible after a security incidence is experienced. However, an effective BCM plan based on international best practice will generate the following benefits:

a. Minimise the effect of a disruption on an organisation
b. Builds confidence among your customers and employees in the organisation's services
c. Reduce the risk of financial loss.

d. Protects valuable business and organisation data
e. Ensures compliance with industry standards
f. Retain company brand and image.
g. Mitigate the organisation's financial risk.
h. Enable the recovery of critical systems within an agreed timeframe.
i. Meet legal and statutory obligations.
j. Gives the organisation a competitive advantage

3.3 Implementing a Business Continuity Management System (BCMS) Plan

The international standard ISO 22301:2012 provides a best-practice framework for implementing an optimized BCMS (business continuity management system), enabling organisations to minimize business disruption and continue operating in the event of an incident.
A BCMS framework is provided for organisations to update, control, and deploy an effective BCM programme that helps them prepare for, respond to and recover from disruptive incidents.
However, multiple standards have emerged over the years, and many keep emerging from the International Organisation for Standardization (ISO) and the International Electrotechnical Commission (IEC). Examples of standards which have emerged include:

a. ISO 22301:2012: Business Continuity Management Systems -- Requirements
b. ISO 22313:2012: Business Continuity Management Systems -- Guidance
c. ISO 22320:2011: Emergency management -- Requirements for incident response
d. ISO/IEC 27031:2011: Information technology -- Security techniques -- Guidelines for information and communication technology readiness for business continuity
e. ISO/IEC 24762:2008: Information technology -- Security techniques -- Guidelines for information and communications technology disaster recovery services
f. National Institute of Standards and Technology Special Publication 800-34: IT contingency planning
g. American Society for Industrial Security (ASIS) SPC.1-2009: Organisational resilience guidance
h. ASIS SPC.4-2012: Organisational resilience management systems.

3.3.1 Principles of a Business Continuity Management System

ISO 22301 is founded on some core principles and activities. These include:

a. Securing Management Support

It consistently monitors the overall process, ensuring that necessary resources are available and supported throughout the process.

b. Risk assessment

The scenarios which might disrupt business functions are critically considered to determine the extent to which it may affect the organisation. Determining these is a key output of the risk assessment.

c. Business Impact Analysis (BIA)

Business impact analysis helps to identify an organisation's most important activities and resources. The extent of impact which the organisation will experience if those activities are affected is also analysed in this process. Recovery time objective (RTO) for each activity or resource is the outcome of a well-planned Business Impact Analysis.

d. Business Continuity Plans (BCPs)

The content of the BCP(s) is primarily developed on the basis of the risk assessment and BIA. Business continuity plans reflect an organisation's needs and specific circumstances. It is developed based on the risk assessment and BIA.

3.3.2 Evaluation and Continual Improvement of BCMS

Evaluating the BCMS for an organisation, the ISO 22301 especially recommends the **Plan-Do-Check-Act (PDCA**) model. The model proposes that a plan of actions be written down, then execute (or do) that plan. Afterwards, the performance is checked to determine if there is a need for improvement. Finally, actions are carried out on the decisions. Testing the BCP is also vital to ensure that the organisation's plan works effectively and that the employees know what to do if an incident occurs.

3.4 Discussion

Given the benefits of utilising international standards for incidence response and disaster recovery in an organisation, there may be possible challenges mitigating the proper implementation. Discuss.

4.0 Self-Assessment Exercise(s)

1. One of the following is not among the benefits of business continuity planning
   a) Reduce the risk of financial loss.
   b) Protects valuable business and organisation data
   c) Helps to onstruct incident management plan
   d) Ensures compliance with industry standards

   Answer: c

2. The principles of a Business Continuity Management System consist of
   i. Disaster Recovery Plan (DRP)
   ii. Business impact analysis (BIA)
   iii. Business continuity plans (BCPs)

   a) i and ii
   b) ii and iii
   c) i and iii

   Answer: b

5.0 Conclusion

International standards provide the generally acceptable ways and medium to which organisations respond to security incidence, disaster recovery, and ensure business continuity. Since awareness has also been initiated by the organisation managers and security personnel, then the need to collaborate on ensuring that organisations do not run out of businesses or fold up due to security incidences that have been experienced

6.0 Summary

This unit details more on international standards dealing with incidence response, disaster recovery and business continuity. The contents of different published standards have were discussed. The benefits of collaboration between business continuity plans with disaster recovery are also highlighted. Conclusively, the principles and evaluation model of business continuity management systems framework was explained in detail.

7.0 References/Further Reading

Federal Information Security Management Act

https://www.scu.edu/is/technology-policies-procedures-and-standards/incident-response-standard/

https://searchdisasterrecovery.techtarget.com/definition/Business-Continuity-and-Disaster-Recovery-BCDR

https://bcmmetrics.com/benefits-business-continuity-planning/

https://www.continuitysa.com/six-benefits-of-business-continuity-management/

NIST Special Publication (SP) 800-61 – Computer Security Incident Handling Guide

ISO/IEC 27035-1:2016 – Principles of incident management